Sociotechnika

Sociotechnika je ovlivňování a přesvědčovaní lidí s cílem oklamat je tak, aby uvěřili, že sociotechnik je osoba s totožností, kterou předstírá a kterou si vytvořil pro potřeby manipulace. Díky tomu je sociotechnik schopný využit lidi, se kterými hovoří, případně dodatečné technologické prostředky, aby získal hledané informace.

Obsah

Vstupní slovo

Všichni se rodíme s vnitřní potřebou poznávání podstaty svého okolí. V mládí jsme byli, Kevin i já, nesmírně zvědaví na okolní svět a toužili ukázat svou vlastní hodnotu. V dětství jsme byli odměňováni, když jsme se naučili něco nového, vyřešili hádanku nebo vyhráli nějakou hru. Ale ve stejnou dobu nám svět diktoval pravidla chování a spoutával naši vnitřní potřebu poznávání. Stejně jako u vynikajících vědců či technických vizionářů, tak i u lidí ražení Kevina Mitnicka způsobovalo následování této vnitřní potřeby největší možné vzrušení, které nám dovolilo dělat věci, které se jiným zdají neuskutečnitelné.

Kevin Mitnick je jedním z nejúžasnějších lidí, které znám. Zeptejte se ho a on vám upřímně odpoví, že sociotechnická metoda, kterou používal, spočívá v podvádění lidí. Kevin už však není sociotechnik a dokonce i v době, kdy jím byl, nikdy nebyla jeho motivací touha se obohatit nebo někomu ublížit. Neznamená to však, že neexistují nebezpeční a destruktivní zločinci, kteří používají sociotechniku, aby vám způsobili skutečnou škodu. Právě před nimi vás chce Kevin v této knize varovat.

Umění klamu ukazuje, jak moc jsou státní úřady, firmy i každý z nás bezbranné proti útoku sociotechnika. Dnes, kdy se hodně pozornosti věnuje bezpečnosti, vydávají se ohromné prostředky na ochranu počítačových sítí i dat, bychom si měli uvědomit, jak snadné je oklamat lidi “uvnitř" a obejít všechna možná technická zabezpečení. Právě to popisuje tato knížka.

Pokud pracujete ve firmě nebo státí instituci, je tato kniha neocenitelným pomocníkem, který umožňuje pochopit, jak sociotechnici fungují a co můžeme udělat, abychom jim zkřížili plány. Ve svých fabulovaných příbězích, jejichž četba nejenže otevírá očí, ale je zároveň dobrou zábavou, popisuje Kevin spolu se spoluautorem Billem Simonem techniky používané podvodníky. Po každém příběhu dostáváme rady, jak se v podobných situacích bránit.

V zabezpečeních zajišťovaných technologickými prostředky zeje velká díra, s jejímž utěsněním nám mohou pomoci lidé, jako je Kevin. Po přečtení této knihy si určitě uvědomíte, jak moc takovou pomoc potřebujete.

Steve Wozniak[1]

[1] Pozn. překl.: Steve Wozniak je spoluzakladatelem firmy Apple Computer.

Předmluva

Jsou na světě hackeři, kteří ničí cizí soubory nebo celé pevné disky -nazývají se *crackeři* nebo prostě *vandalové*. Existují rovněž nezkušení hackeři, kteří se neobtěžují tím, že by se učili technologie, ale stahují si z Internetu hackerské nástroje, s jejichž pomocí se vloupávají do počítačových systémů. Říká se jim *script kiddies*. Zkušenější hackeři sami vytvářejí hackerské programy, které posléze umisťují na Síti či v diskusních skupinách. Existují i takové osoby, které technologie vůbec nezajímají, a počítač využívají jen jako nástroj, který jim pomáhá krást peníze, zboží a bezplatně využívat různé služby.

Oproti mýtu Kevina Mitnicka, jak ho vytvořila média, nebyl jsem zákeřný hacker.

Ale to předbíhám.

Začátky

Dráha, na kterou jsem se vydal, měla svůj počátek již v dětství. Byl jsem bezstarostné, ale znuděné dítě. Máma, aby nás po rozchodu s otcem (byly mi tehdy tři roky) uživila, pracovala jako servírka. Jistě si dokážete představit jedináčka vychovávaného věčně rozlítanou matkou — kluka osamoceně trávícího celé dny. Byl jsem si svou vlastní chůvou.

Vyrůstal jsem v San Fernando Valley a měl jsem celé Los Angeles k průzkumům. Když mi bylo dvanáct let, našel jsem způsob, jak zadarmo cestovat po celé oblasti Los Angeles. Jednoho dne jsem při cestě autobusem objevil, že soustava dírek na jízdence označované řidičem představuje den, čas a autobusovou linku. Přátelsky naladěný řidič mi odpověděl na všechny moje důkladně promyšlené otázky a prozradil mi také, kde je možné koupit označovací strojek, který používá.

Tyto jízdenky umožňovaly přestupy i pokračování přerušené jízdy. Vymyslel jsem tehdy, jak je používat, aby se dalo jezdit všude zadarmo. Získat nepoužité lístky byla maličkost: odpadkové koše na autobusových nádražích byly plné zčásti vypotřebovaných bločků, které řidiči na konci směny vyhazovali. Když jsem měl nepoužité jízdenky i označovací strojek, mohl jsem si je sám označovat tak, abych se dostal na libovolné místo v Los Angeles. Brzy jsem znal celý systém autobusových linek zpaměti. To je jeden z prvních příkladů mé udivující schopnosti pamatovat si informace jistého druhu. Dodnes si pamatuji čísla telefonů, hesla a podobné detaily — dokonce i ty z dětství.

Jiný můj zájem, který se projevil poměrně brzy, byla fascinace kouzelnickými triky. Když jsem zjistil, v čem spočívá nějaký kousek, trénoval jsem ho tak dlouho, dokud jsem ho neovládl. V jistém smyslu jsem díky kouzelnictví objevil radost, jakou lze pociťovat při klamání lidí.

Od phreakera k hackerovi

Mé první setkám s něčím, co jsem se později naučil označovat slovem sociotechnika, bylo na střední škole. Poznal jsem tehdy kamaráda, kterého pohlcoval koníček nazývaný phreaking. Představovalo to pronikání do telefonních sítí díky využívám pracovníků telefonních služeb a znalostí fungování sítě. Předvedl mi kousky, jaké lze dělat pomocí telefonu: získat všechny informace o libovolném uživateli sítě, nebo využívat tajné testovací číslo na dlouhé meziměstské hovory (později se ukázalo, že číslo vůbec nebylo

testovací — hovory, které jsme uskutečnili, byly připsány na účet jedné nebohé firmy).

Takové byly moje začátky z oblasti sociotechniky — svým způsobem mateřská školka. Ten kamarád a ještě jeden phreaker, kterého jsem záhy poznal, mi dovolili poslouchat telefonní rozhovory, které vedli s pracovníky telekomunikační firmy- Všechno, co říkali, znělo velmi věrohodně. Dozvěděl jsem se, jak fungují různá oddělení firmy, naučil jsem se žargon a procedury, které jejich pracovníci používají. Ale tento výcvik netrval dlouho; nepotřeboval jsem to. Prohluboval jsem si své znalosti v praxi a brzy jsem sám dělal všechny ty věci lépe než mí učitelé. Takto byla má životní cesta určena na nejbližších patnáct let.

Teden z mých oblíbených kousků spočíval v tom, že jsem získal přístup do telefonní ústředny a změnil druh služby přiřazený číslu mého známého phreakera. Když se pak pokoušel z domova telefonovat, slyšel v sluchátku pokyn, aby vhodil minci — ústředna si myslela, že telefonuje z automatu.

Pohlcovalo mne všechno, co se týkalo telefonů. Nejen elektronika, ústředny a počítače, ale také organizace, procedury a terminologie. Po nějaké době jsem věděl o telefonní síti snad více, než kterýkoliv profesionál. Rozvinul jsem také své dovednosti v oblasti sociotechniky do té míry, že jsem v sedmnácti letech byl schopen namluvit většině pracovníků sítě skoro cokoliv, ať už telefonicky či osobně.

Moje všeobecně známá kariéra hackera začala na střední škole. Nemohu zde popisovat podrobnosti, stačí, když povím, že hlavním motivem mých prvních průniků byla touha být přijat skupinou mně podobných osob.

Tehdy jsme označení hacker používali pro ty, kteří trávili hodně času experimentováním s počítači a programy, psaním efektivnějších programů, či nalézáním lepších způsobů řešení nějakých problémů. Dneska má to označení hanlivý přídech a člověk si přitom vybavuje pojem „nebezpečný zločinec". Já ho tu však používám v tom smyslu, jak jsem ho používal vždycky — čili v tom dřívějším, jemnějším.

Po skončení střední školy jsem studoval informatiku v Computer Learning Center v Los Angeles. Po několika měsících odhalil správce školní sítě, že jsem našel díru v operačním systému a že jsem získal veškerá práva na počítačích IBM. Nejlepší odborníci z řad učitelů nedokázali zjistit, jak jsem toho dosáhl. Tehdy asi došlo k jednomu z prvních případů „zaměstnání hackera" — dostal jsem nabídku, jaká se neodmítá: bud v rámci zápočtové práce opravím zabezpečení školního počítačového systému, nebo budu vyloučený za vloupání do systému. Samozřejmě jsem si vybral to první a díky tomu jsem mohl ukončit školu s

vyznamenáním.

Sociotechnik

Někteří lidé vstávají ráno z postele s hrůznou představou dalšího rutinního dne opakovaných činností. Měl jsem to štěstí, že jsem vždycky měl rád svoji práci. Nejvíce výzev, úspěchů a uspokojení mi přinášela práce soukromého detektiva. Piloval jsem tehdy své dovednosti v umem zvaném sociotechnika — přesvědčování lidí, aby dělali věci, které se pro neznámé lidi obvykle nedělají. A byl jsem za to placený.

Stát se odborníkem v této branži pro mne nebylo těžké. Rodina z otcovy strany se po generace zabývala obchodem — možná je dovednost přemlouvat a ovlivňovat jiné dědičná. Když spojíte sklony k manipulaci s lidmi s dovednostmi a talentem v oblasti přesvědčování a ovlivňování lidí, dostanete vlastnosti ideálního sociotechnika.

Lze říci, že existují dvě specializace v povolání umělce-manipulátora. Ten, kdo mámí z lidí peníze, je obyčejný podvodník, a ten, kdo využívá manipulace a přesvědčování vůči firmám — obvykle se záměrem získání informací — je sociotechnik. Od doby mého prvního kousku s autobusovými bločky — kdy

jsem byl ještě příliš mladý na to, abych si přiznal, že dělám něco špatného – jsem u sebe začal rozeznávat dar dozvídat se věci, které bych neměl vědět. Rozvíjel jsem svůj talent, klamal jsem, oháněl se žargonem a vyvinutou dovedností manipulace.

Jeden ze způsobů, jak jsem rozvíjel dovednosti v mém řemesle (pokud to lze nazvat řemeslem), byly pokusy získat nějakou informaci, na které mi ani nezáleželo. Šlo o to, jestli jsem schopen přemluvit osobu na druhém konci drátu, aby mi ji řekla – jen tak v rámci tréninku. Stejně, jako jsem kdysi cvičil kouzelnické triky, jsem ted zdokonaloval umění vemlouvání. Díky tomu jsem brzy objevil, že mohu získat prakticky jakoukoliv informaci, kterou potřebuji.

Když jsem o mnoho let později vypovídal před senátory Liebermanem a Thompsonem, řekl jsem:

Podařilo se mi získat neautorizovaný přístup do počítačových systémů několika největších korporací na světě, prorazit nejlépe zabezpečené existující počítačové systémy. Používal jsem technologické nástroje i nástroje nesvázané s technikou, abych získal přístup ke zdrojovému kódu různých operačních systémů, telekomunikačních zařízení, a abych poznával, jak fungují a jaké mají slabé stránky.

Skutečně jsem tím uspokojoval pouze svou vlastní zvědavost, přesvědčoval jsem se o možnostech a vyhledával tajné informace o operačních systémech, mobilních telefonech a o všem ostatním, co vzbuzovalo můj zájem.

Shrnutí

Po zatčení jsem přiznal, že to, co jsem dělal, bylo v rozporu se zákony a že jsem se dopustil narušení soukromí.

Moje činnost byla způsobena zvědavostí – toužil jsem znát všechno, co se dalo, o fungování telefonní sítě a vstupů a výstupů počítačových bezpečnostních systémů. Z dítěte fascinovaného kouzelnickými kousky jsem se stal nejstrašnějším hackerem na světě, kterého se obávala vláda korporace. Když se probírám vzpomínkami posledních třiceti let mého života, musím přiznat, že jsem, vedený zvědavostí, touhou po poznávání technologií a uspokojování intelektuálních výzev, učinil několik velmi špatných rozhodnutí.

Změnil jsem se. Dnes využívám svůj talent a své znalosti o bezpečnosti informací a sociotechnice, které se mi podařilo osvojit, k tomu, abych pomáhal vládě, firmám i soukromým osobám při odhalování, prevenci a reakcích na ohrožení bezpečnosti informací.

Tato kniha je dalším ze způsobů, jak mohu uplatnit své zkušenosti ve prospěch jiných, tak, aby si dokázali poradit se zloději dat. Doufám, že zde popsané případy zaujmou, otevřou oči a poučí.

Kevin Mitnick

Úvod

Tato kniha obsahuje bohatou sbírku informací týkajících se sociotechniky a bezpečnosti dat. Zde je stručný přehled uspořádání knihy, které usnadní její použití.

V první části odhaluji Achillovu patu bezpečnostních systémů a ukazuji, proč jsme my a naše firma vystaveni nebezpečí sociotechnických útoků.

Druhá část popisuje, jak sociotechnici využívají naši důvěru, ochotu pomoci, soucit a naivitu, aby získali to, co chtějí. Fiktivní historky demonstrující typické útoky ukazují sociotechnika nasazujícího si stále nové masky. Jestliže se vám zdá, že jste se nikdy nesetkali se sociotechnikem, pravděpodobně jste na omylu. Nejeden z těch příběhů se nám může zdát nečekaně povědomý. Avšak po přečtení druhé až deváté kapitoly bychom měli mít potřebné znalosti k tomu, abychom se ubránili dalšímu útoku.

Ve třetí části se hraje o větší sázky. Vymyšlené příběhy ukazují, jak se může sociotechnik dostat do areálu firmy, ukrást tajemství, což muže zruinovat náš podnik, nebo zničit náš technologicky nejmodernější bezpečnostní systém. V této části nás ukázané scénáře seznamují s nebezpečími počínaje obyčejnou pomstou a kyberterorismem konče. Jestliže je pro nás důležité zabezpečení klíčových informací, které udržují v chodu naši firmu, měli bychom si přečíst od začátku do konce kapitoly deset až čtrnáct.

Je nutné si uvědomit, že pokud není napsáno jinak, jsou příběhy představené v této knize čirou fikcí.

Ve čtvrté části jsou popsány způsoby, jak v organizaci předcházet sociotechnickým útokům. Patnáctá kapitola obsahuje nástin účinného bezpečnostního školení a v šestnácté kapitole najdeme hotový vzor popisující bezpečnostní politiku firmy, který můžeme upravit podle našich potřeb a rovnou uvést v platnost, abychom zabezpečili naši informační bezpečnost.

V závěru se nachází část „Bezpečnost v kostce", která shrnuje klíčové infomace formou seznamů a tabulek. Mohou být pro naše zaměstnance jakýmsi tahákem, pomáhajícím vyhnout se sociotechnickým útokům.

Zde obsažené informace také mohou pomoci při vytváření firemního programu bezpečnostního školení.

V knize najdeme také poznámky týkající se žargonu, které obsahují definice termínů, používaných hackery a sociotechniky, a také doplňující poznámky Kevina Mitnicka obsahující shrnutí příslušného fragmentu — zlaté myšlenky, které pomáhají při formulaci bezpečnostní strategie. Ostatní poznámky a rámečky obsahují zajímavé doplňující informace nebo vysvětlují okolnosti konkrétní záležitosti.

I

Zákulisí

Achillova pata bezpečnostních systémů

1

Achillova pata bezpečnostních systémů

Firma si může pořídit ty nejlepší a nejdražší bezpečnostní technologie, vyškolit personál tak, aby byla každá důvěrná informace před odchodem domů pod zámkem, najmout si tu nejlepší firmu na noční ostrahu objektů, a přece bude ta organizace ještě zranitelná.

Soukromé osoby se mohou držet všech nejlepších zásad doporučovaných odborníky, mohou otrocky nainstalovat všechny nejnovější produkty vylepšující zabezpečení a odpovídajícím způsobem pozorně zkonfigurovat systém, mohou použít všechna jeho vylepšení či opravy, a přece jsou tyto osoby stále nechráněné.

Lidský faktor

Když jsem — ne tak dávno — vypovídal před Kongresem, vysvětlil jsem, jak jsem často získával od firem hesla a jiné citlivé informace. Predstavoval jsem se jako někdo jiný a prostě jsem o ně požádal. Touha po pocitu absolutní bezpečnosti je přirozená, ale vede mnoho krát k falešnému pocitu chybějícího ohrožení. Vezměme si za příklad zodpovědného a milujícího muže, který si pořídil do vstupních dveří systém Medico (cylindrický zámek proslulý tím, že jej nelze otevřít paklíčem), aby ochránil svou ženu, děti a domov. Po namontování toho zámku se cítí lépe, protože jeho rodina je ted ve větším bezpečí. Ale co se stane, když lupič rozbije sklo v okně nebo prorazí kód otevírající vrata do garáže? Nezávisle na drahých zámcích nejsou stále obyvatelé v bezpečí. A co když zavedeme kompletní bezpečnostní systém? To už je lepší, ale stále to nebude záruka bezpečí.

Proč? Protože Achillovou patou zabezpečení je *lidský faktor.*

Bezpečnost je až příliš často iluzorní. Pokud k tomu ještě připočteme lehkověrnost, naivitu a ignoranci, situace se dále zhoršuje. Nejuznávanější vědec 20. století, Albert Einstein, prý řekl: „Pouze dvě věci jsou nekonečné: vesmír a lidská hloupost. Ačkoli tím prvním si nejsem jist." Ve výsledku se atak sociotechnika často podaří, protože lidé bývají hloupí, Častěji jsou však takové útoky účinné proto, že lidé nerozumějí ověřeným zásadám bezpečnosti.

Podobný přístup, jako měl pán domu obeznámený se záležitostmi zabezpečení, má také mnoho pracovníků z oboru IT. Mívají chybný názor, že dostatečně zabezpečili své firmy proti útokům tím, že si nainstatovali standardní produkty jako *firewall* a taková ověřená vyspělá řešení, jako jsou například časově závislé kódy nebo biometrické karty. Každý, kdo si myslí, že produkty samotné zajišťují opravdové bezpečí, si vytváří pouze jeho *iluzi*. To je klasický případ života ve světě představ: takové osoby se mohou dříve či později stát oběťmi útoku.

Jak říká známý poradce pro otázky bezpečnosti Bruce Schneier: „Bezpečnost není výrobek, ale proces". Rozviňme tuto myšlenku: bezpečnost není technologický problém, ale je to problém lidí a řízení.

S postupem stále dokonalejších bezpečnostních technologií, které ztěžují nalézání technických děr v systému, se budou útočníci stále vícezaměřovat na lidské slabosti. Překonání „lidské bariéry" je o mnoho jednodušší a často vyžaduje investice v hodnotě nákladů na telefonní hovor, nemluvě o menším riziku.

Klasický případ podvodu

Kdo představuje největší ohrožení bezpečnosti firemního majetku? Odpověd je prostá: sociotechnik — kouzelník bez skrupulí, který, když sleduješ jeho levou ruku, tou pravou ti krade tvá tajemství. K tomu bývá často tak milý, hovorný a zdvořilý, že jsi opravdu potěšen, že jste se setkali.

Podívejme se na příklad užité sociotechniky. Dnes už si jen málokdo pamatuje mladého člověka, který se jmenoval Stanley Mark Rifkin, a jeho případ s dnes už neexistujícím ústavem Security Pacific National Rank v Los Angeles. Zprávy o jeho eskapádě se různí a sám Rifkin (podobně jako já) svoji verzi nikdy nevyprávěl, proto se popis zde uvedený opírá o publikované informace.

Lámání kódu

Jednoho dne roku 1978 se Rifkinovi podařilo dostat do místnosti určené pouze pro povolaný personál provádějící elektronické převody banky Security Pacific, kde pracovníci vysílali a přijímali převody o celkové částce miliard dolarů denně.

Rifkin tehdy pracoval pro firmu, která podepsala s bankou kontrakt na vytvoření záložního systému v místnosti převodů pro případ poruchy jejich hlavního počítače. To mu umožnilo přístup k transferovým procedurám včetně těch, které popisovaly, jakým způsobem pracovníci banky zadávají převody. Dozvěděl se, že osoby pověřené zadáváním převodů dostávaly každé ráno přísně chráněný kód, který používaly, když telefonovaly do místnosti převodů.

Úředníkům z místnosti se nechtělo si každodenní kódy pamatovat a tak si povinný kód zapisovali na list papíru a umísťovali si ho na viditelném místě. Toho listopadového dne měl Rifkin zvláštní důvod navštívit místnost. Chtěl se mrknout na ten lístek.

Když se objevil v místnosti, všímal si operačních procedur, zdánlivě proto, aby se ujistil, že zálohovací systém bude správně spolupracovat se základním systémem. Zároveň si koutkem oka přečetl bezpečnostní kód na lístku a zapamatoval si ho. Po několika minutách odešel. Jak později říkal, cítil se, jako by právě vyhrál v loterii.

Bylo jednou jedno švýcarské konto...

Po odchodu okolo 15. hodiny se odebral přímo k telefonnímu automatu mramorové hale budovy, vhodil minci a vytočil číslo místnosti převodů. Ze Stanleyho Rifkina, spolupracovníka banky, se stal Mike Hansen, pracovník mezinárodního odboru banky.

Podle jednoho ze zdrojů probíhal rozhovor následovně:

„Dobrý den, tady je Mike Hansen z mezinárodního," řekl mladé pracovnici, která zvedla telefon.

Děvče se zeptalo na číslo jeho kanceláře. Byla to standardní procedura, na kterou byl připraven.

„286," odvětil.

„Uvedte, prosím, kód," požádala potom pracovnice. Rifkin později přiznal, že se mu v tom okamžiku podařilo opanovat bušení srdce.

Bez zaváhání odpověděl: „4789".

Nato začal sdělovat detaily převodu: „Deset milionu dvě stě tisíc dolarů přesně" z Irving Trust Company v New Yorku do Wozchod Handels Bank of Zurich ve Švýcarsku, kde si předtím založil účet.

„V pořádku. Teď, prosím, uveďte mezikancelářský kód."

Rifkina polil pot. To byla otázka, kterou nečekal. Něco, co mu uteklo během pátrání. Zachoval však klid předstíraje, že se nic nestalo a bez sebemenšího zaváhání řekl: „Musím ho najít, zavolám za chvíli." Hned zatelefonoval na jiný odbor banky a tentokrát se představil jako pracovník místnosti převodů. Obdržel mezikancelářský kód a zavolal zpátky dívce do místnosti převodů.

Zeptala se na kód a řekla: „Děkuji". (Vezmeme-li v úvahu okolnosti, tak její poděkování můžeme brát velmi ironicky.)

Dokončení práce

O několik dní později odletěl Rifkin do Švýcarska, vybral hotovost a za více než 8 milionů dolarů nakoupil od jedné ruské agentury diamanty. Při návratu do Států měl diamanty v pásku na peníze. Uskutečnil největší bankovní podvod v historii bez použití pistole či počítače. Jeho případ se nakonec dostal do Guinessovy knihy rekordů v kategorii Největší počítačový podvod.

Stanley Rifkin využil umění manipulace – dovednosti a techniky, které se dnes nazývají sociotechnika. Vyžadovalo to pouze důkladný plán a dar řeči.

A o tom je vlastně tato kniha – o sociotechnických metodách, které sám ovládám a o způsobech, jak se proti nim jednotlivci i organizace mohou bránit.

Podstata ohrožení

Rifkinův příběh je důkazem, jak klamný může být náš pocit bezpečí. Podobné incidenty – třebas nedosahující deseti milionů dolarů, nicméně přesto škodlivé – se odehrávají *dennodenně*. Možná právě v této chvíli ztrácíš své peníze nebo někdo krade tvé plány na nový produkt a ani o tom nevíš. Jestli se něco takového ještě nestalo ve tvé firmě, otázka nezní, jestli se to stane, ale *kdy* se tak stane.

Rostoucí obava

Institut počítačové bezpečnosti ve svých výzkumech z roku 2001 zabývajících se počítačovými zločiny prohlásil, že během roku zaznamenalo 85 % dotázaných organizací narušení počítačového zabezpečení. Je to udivující procento: pouze patnáct firem ze sta mohlo říci, že s tím nemělo problémy. Stejně šokující je počet organizací, které ohlásily ztráty z důvodu počítačových vloupání – 64 %. Více než polovina firem utrpěla finanční ztráty – *za jediný rok*.

Moje vlastní zkušenost mě však vede k podezření, že čísla ve zprávách tohoto typu jsou přehnaná. Mám pochybnosti o způsobu provádění výzkumů, to však neznamená, že ztráty opravdu nejsou velké. Pokud takové situace nepředvídáme, odsuzujeme se předem k prohře.

Komerční bezpečnostní produkty dostupné na trhu, které většina firem používá, slouží hlavně na ochranu před útoky amatérů, například dětí nazývaných *script kiddies*. Tito mladíci si hrají na hackery, používají programy dostupné na síti a většinou jsou jen jakýmsi obtížným hmyzem. Největší ztráty a reálné ohrožení hrozí ze strany rafinovanějších hackerů, kteří mají jasně definovaný úkol, motivuje je zisk a soustřeďují se během útoku na konkrétní cíl, místo toho aby se infiltrovali do tolika systémů, kolik jen stihnou – jak to obvykle dělají amatéři. Průměrní hackeři se zaměřují na kvantitu, zatímco profesionálové se orientují na informace podstatné a cenné.

Takové technologie jako je ověřování a zjišťování totožnosti, kontrola přístupu (přístupová práva k souborům a systémovým zdrojům) a systémy detekce vetřelců (elektronická obdoba alarmů) jsou nezbytnou součástí systému ochrany firemních dat. Typická firma však dnes vydává více peněz na kávu než na prostředky chránící před napadením bezpečnostních systémů.

Stejně jako se kleptoman nemůže vzepřít pokušení, je i mozek hackera ovládnutý touhou obejít bezpečnostní systémy. Hackeři si tak dokazují své intelektuální schopnosti.

Metody klamu

Oblíbené rčení zní, že bezpečný počítač je vypnutý počítač. Vtipné, ale nepravdivé: podvodník prostě přemluví někoho, aby šel do kanceláře a ten počítač zapnul. Protivník, který potřebuje nějakou informaci, ji obvykle může získat několika odlišnými způsoby. Je to jen otázka času, trpělivosti, osobnosti a úsilí. V takové chvíli se hodí znalost umění manipulace.

Aby překonal zabezpečení, musí útočník, vetřelec nebo sociotechnik najít metodu na oklamání důvěryhodného pracovníka tak, aby prozradil nějakou informaci, trik nebo zdánlivě nedůležitou nápovědu, která by umožnila dostat se do systému. Pokud lze pracovníky oklamávat nebo jimi manipulovat, aby nám prozradili důvěrné informace, nebo když jejich činnost způsobuje vznik děr v zabezpečení, které umožní útočníkovi přístup do systému, pak neexistuje žádná technologie, která by mohla firmu ochránit. Tak jako jsou kryptologové občas schopni dešifrovat text zakódované zprávy tak, že najdou slabé stránky kódování, umožňující obejít šifrovací technologii, tak i sociotechnici používají lsti vůči pracovníkům firmy, aby obešli technologii zabezpečení.

Zneužití důvěry

Ve většině případů mají sociotechnici velké schopnosti působit na lidi. Dovedou být okouzlující, zdvořilí, je snadné si je oblíbit — to jsou vlastnosti potřebné k tomu, aby si získali porozumění a důvěru jiných. Zkušený sociotechnik, který používá strategii a taktiku patřící k jeho řemeslu, je schopný získat přístup prakticky ke každé informaci.

Důmyslní technologové vypracovali do posledního detailu systémy ochrany informací, aby zminimalizovali riziko spojené s používáním počítačů; zapomněli však na to nejdůležitější — na lidsky faktor. Přes naše intelektuální schopnosti zůstáváme my, lidé, největším nebezpečím pro svoji vlastní bezpečnost.

Americká mentalita

Neuvědomujeme si plně nebezpečí, zvláště v západním světě. V USA se lidé většinou neučí podezíravosti vůči druhému člověku. Jsou přivyklí zásadě „miluj bližního svého", a navzájem si důvěřují. Organizace sousedských hlídek mají často problémy přesvědčit lidi, aby si zamykali domy a auta. Tyto prostředky ochrany vypadají jako samozřejmé, ale mnoho Američanů je ignoruje a volí život ve světě snů — až do první lekce.

Uvědomujeme si, že ne všichni lidé jsou dobří a poctiví, ale příliš to se chováme, jako by právě takoví byli. Američané jsou toho zvláštní případem — jako národ si vytvořili koncepci svobody spočívající v tom, že nejlepší místo pro život je tam, kde nejsou potřeba ani zámky ani klíče.

Většina lidí vychází z přesvědčení, že nebudou podvedeni jinými, protože se takové případy stávají zřídka. Útočník si tento panující předsudek

uvědomuje a formuluje své žádosti velmi přesvědčivým způsobem, který nevzbuzuje žádná podezření. Tak využívá důvěry oběti.

Naivita organizací

Tato svérázná presumpce neviny, která je součástí americké mentality, se projevila zejména v počátcích existence počítačových sítí. ARPANET, předchůdce Internetu, byl vytvořen na výměnu informací mezi vládními a vědeckovýzkumnými institucemi. Cílem byla dostupnost informací a technologický pokrok. Mnoho vědeckých ústavů vytvářelo rané počítačové systémy jen s minimálním zabezpečením nebo úplné bez něj. Jeden ze známých hlasatelů volnosti programů, Richard Stallman, dokonce rezignoval z ochrany svého konta heslem. V době používání Internetu jako média elektronického obchodu drasticky vzrostlo ohrožení spojené se slabými stránkami jeho zabezpečení. Ani použití dodatečných bezpečnostních technologií však nikdy nevyřeší otázku lidského faktoru.

Podívejme se například na dnešní letiště. Jejich zabezpečení je důkladné, ale každou chvíli slyšíme o cestujících, kterým se podařilo obelstít ochranku a přenést zbraň přes kontrolní rámy. Jak je to možné v době, kdy jsou naše letiště prakticky v neustálém stavu pohotovosti? Problém obvykle nespočívá v zařízeních, ale v lidech, kteří je obsluhují. Vedení letišť se mohou opírat o Národní gardu, instalovat detektory kovů a systémy na rozpoznávání tváří, ale obvykle by lépe pomohlo školení pracovníků ochrany, které by podpořilo účinnost kontroly pasažérů.

Stejný problém mají vlády, firmy a vzdělávací instituce po celém svéte. Přes úsilí odborníků na bezpečnost jsou informace všude vystaveny nebezpečí útoku sociotechnika, pokud nebude posílen nejslabší clanek - lidský faktor

Dnes, více než kdy jindy, musíme přestat myslet způsobem, jakým bychom si přáli. Musíme si uvědomit, jaké techniky používají ti, kteří sa pokouší zaútočit na důvěrnost, integritu a dostupnost našich počítačových sítí. Už jsme se naučili řídit auta za použití zásady omezené duvěry. Je nejvyšší čas naučit se obdobným způsobem obsluhovat počítače.

Hrozba narušení soukromí, osobních údajů nebo firemních systémových informací se zdá málo reálná, dokud se skutečně něco nestane. Abychom se vyhnuli takové srážce s realitou, musíme byt všichni připraveni a ve střehu. Musíme také intenzivně chránit naše data, osobní údaje, a také, a to v každé oblasti, kritické prvky infrastruktury, a co nejrychleji začít používat popsaná bezpečnostní opatření.

Teroristé a klam

Podvod samozřejmě není nástrojem používaným výhradně sociotechniky. Popisy teroristických činů představují významnou část agenturních zpráv a museli jsme si uvědomit jako nikdy dříve, že svět není bezpečným místem. Civilizace je koneckonců jen tenké pozlátko.

Útoky na New York a Washington v září 2001 naplnily smutkem a strachem srdce nejen Američanů, ale všech civilizovaných lidí po celé planetě. Byli jsme zaskočeni faktem, že po celém světě jsou rozeseti posedlostí ovládnutí teroristé, kteří jsou dobře vycvičení a čekají na možnost nového útoku.

Současná zintenzivněná snaha vlády zlepšila úroveň povědomí o bezpečnostních záležitostech. Musíme zůstat ve stavu pohotovosti vůči projevům terorismu. Musíme si uvědomit, jak teroristé vytvářejí své falešné totožnosti, hrají role studentů či sousedů, vnořují se do davu. Maskují své pravé záměry, kují proti nám pikle, přičemž si pomáhají triky podobnými těm, které jsou popsané v této knize.

Podle mých informací se zdá, že teroristé zatím ještě nepoužívají sociotechnické triky, aby infiltrovali do korporací, do vodáren, elektráren a dalších základních prvků státní infrastruktury. Každou chvíli tak ale mohou učinit – protože je to prostě velmi jednoduché. Doufám, že díky této knize zavedou vedení firem odpovídající bezpečnostní politiku, dokud nebude pozdě.

0 čem je tato knížka?

Bezpečnost firmy je otázkou rovnováhy. Příliš slabé zabezpečení ponechává firmu v ohrožení, příliš silné zase překáží v činnosti, brzdí růst a prosperitu firmy. Úloha spočívá v nalezení rovnováhy mezi bezpečnosti a produktivitou. Jiné knížky zabývající se bezpečností firem se soustředují na zařízení a programy a nevěnují patřičnou pozornost nejvážnějšímu nebezpečí podvodu. Cílem této knihy je pro změnu pomoci pochopit, jakým způsobem mohou být lidé v organizacích zmanipulováni a jaké bariéry mají vytvořit, aby se tomu předešlo. Kniha se soustřeďuje zejména na metody netechnologické, které vetřelci používají s cílem získat informaci, narušit integritu dat, která zdaleka nejsou tak bezpečná, jak se zdá, nebo přímo zničit výsledky práce firmy.

Má úloha je však ztížená z jednoho prostého důvodu: každý čtenář už byl zmanipulován největšími sociotechnickými experty – svými rodiči. Ti našli způsoby jak zařídit, abychom „ve svém vlastním zájmu" dělali to, co je podle nich nejlepší. Rodiče jsou schopní všechno vysvětlit, stejně jako sociotechnici šikovně vymýšlejí věrohodné historky, důvody a argumenty, jen aby dosáhli svého.

V důsledku takových zkušeností jsme se všichni stali náchylnými podlehnout manipulaci. Náš život by byl těžký, kdybychom museli být pořád ve střehu, nedůvěřovat jiným, brát v úvahu možnost, že nás někdo využívá. V ideálním světě by bylo možné bezstarostně důvěřovat jiným a mít jistotu, že lidé, se kterými se setkáváme, jsou poctiví a hodni důvěry. Nežijeme však v takovém světě, a proto si musíme vytrénovat návyk bdělosti, abychom mohli odhalit lidi, kteří se nás pokoušejí oklamat.

Většina této knihy (druhá a třetí část) se skládá z příběhů ukazujících sociotechnika v akci. Popsána jsou taková témata jako:

- Rafinovaná metoda, jak získat od telekomunikační firmy nezveřejněná telefonní čísla – phreakery to napadlo už před drahnými lety.
- Několik metod, které používají útočníci k přemlouvání i těch nejpodezíravějších pracovníků, aby prozradili svá uživatelská jména a hesla.
- Krádež nejlépe střežených údajů o výrobku, ke které dopomohl manažer z operačního střediska.
- Metoda, pomocí které hacker přesvědčil jistou paní, aby si stáhla a nainstalovala program, který sleduje všechno její počínání a posílá e-maily s informacemi.
- Jak soukromí detektivové získávají informace o firmách i o soukromých osobách. Garantuji během četby husí kůži.

Po přečtení některých příběhů ze druhé a třetí části může leckdo dojít k názoru, že se to nikdy nemohlo stát, že by se pomocí lstí a metod zde popsaných nikomu nepodařilo nic získat. Tyto příběhy však jsou potenciálně pravdivé – ukazují události, které se mohou stát a stávají se. Mnoho z nich se někde na světě odehrává den co den, možná dokonce ve vaší firmě, zatímco ty čteš tuto knihu.

Zde uvedený materiál nám též může otevřít oči, když na nás přijde řada setkat se s dovednostmi sociotechnika a chránit před ním svá osobní data.

Ve čtvrté části se role obrátí. Snažím se pomoci při vytváření nezbytné bezpečnostní politiky a programu školení minimalizujícího pravděpodobnost, že

se některý z našich zaměstnanců stane obětí sociotechnika. Pochopení strategie, metody a taktiky sociotechnika pomůže uplatnit odpovídající prostředky ochrany dat, aniž by se ohrožovala produktivita podniku.

Napsal jsem zkrátka tuto knihu proto, abych zvýšil povědomí o vážné hrozbě, kterou sociotechnik představuje, a abych pomohl zmenšit šanci sociotechnika na využití firmy či některého z jejích zaměstnanců.

A možná bych měl říci — opětovného využití.

II

Umění útoku

2

Kdy nevinná informace není nevinná?

V čem spočívá reálná hrozba ze strany sociotechnika? Čeho bychom se měli vyvarovat?

Jestliže je jeho cílem získat něco cenného, dejme tomu část kapitálu firmy, pak by možná stálo za to pořídit si pevnější trezor a silnější stráže, ne?

Průnik do zabezpečené firmy často začíná od získání informace či dokumentu, který je zdánlivě bezvýznamný, je obecně dostupný a nepříliš důležitý. Většina lidí v organizaci tedy nevidí důvod, proč by měl být chráněný.

Skrytá hodnota informace

Mnoho neškodně vyhlížejících informací v majetku firmy je pro socioecnnika cenných, poněvadž mohou hrát důležitou roli během převtělování se za někoho jiného.

V této knize sa staneme „svědky" toho, jak fungují sociotechnici při útoku. Občas představíme situaci nejprve z pohledu oběti, což umožňuje vcítit sa do její kůže a pokusit se analyzovat, jak bychom se v této situaci zachovali my nebo naši zaměstnanci. V mnoha případech budou ty sa události představeny také z pohledu sociotechnika.

První příběh nám přibližuje slabé stránky firem, které působí ve finančnictví.

CreditChex

Odnepaměti se museli Britové unavovat se starosvětským bankovním systémem. Obyčejný poctivý občan nemůže jen tak přijít do banky a žaložit si konto. Banka ho nebude považovat za klienta, dokud mu již existující klient nenapíše doporučující dopis.

V našem zdánlivě rovnostářském bankovním světě to už vypadá trochu jinak. Moderní, jednoduchý způsob podnikání je nejzřetelnější v přátelské a demokratické Americe, kde může kdokoliv přijít do banky a bez problémů si otevřít účet. Ačkoliv ne tak docela kdokoliv. Ve skutečnosti mají banky přirozený odpor před otevíráním účtu někomu, kdo mohl v minulosti vypsat nekrytý šek. Takového zákazníka vidí bankéři asi s takovou radostí, jako zprávu o ztrátách při přepadení banky nebo defraudaci. Proto je standardní praxí v mnoha bankách rychlá kontrola důvěryhodnosti nového klienta.

Jednou z větších firem, které si banky na takováto ověřování najímají, je CreditChex. Poskytuje svým zákazníkům cenné služby, ale její zaměstnanci mohou také nevědomky pomoci i sociotechnikovi.

První telefonát: Kim Andrews

„National Bank, u telefonu Kim. Chtěl jste si otevřít účet?"

„Dobrý den, měl bych dotaz. Využíváte služeb CreditChex?"

„Ano."

„A jak se nazývá to číslo, které je třeba uvést, když se telefonuje do CreditChex? Obchodní číslo?"

Pauza. Kim zvažovala otázku: čeho se týká a jestli by měla odpovědět. Tazatel plynule pokračuje:

„Víte, pracuji na knížce o soukromých pátráních."

„Ano," odpovídá Kim po rozptýlení pochybností na otázku, ráda, mohla pomoci spisovatelovi.

„Takže se ťo nazývá obchodní číslo, tak?"

„Mhm."

„Skvělé. Chtěl jsem se prostě ujistit, že znám žargon. Kvůli té knížce. Moc jste mi pomohla. Na shledanou."

Druhý telefonát: Chris Walker

„National Bank, zakládání účtů, zde Chris."

"Dobrý den, tady Alex," představuje se volající. „Jsem ze zákaznického servisu CreditChex. Děláme anketu, abychom mohli zlepšit kvalitu našich služeb. Mohla byste mi věnovat pár minut?“

Chris souhlasila. Volající pokračoval:

Dobrá, jaká je otevírací doba vaší pobočky?" Chris odpovídá na tuto otázku, jakož i na řadu dalších.

„Kolik pracovníků vaší pobočky využívá našich služeb?"

„Jak často k nám voláte s dotazem?"

„Která z našich zelených linek 0800 vám byla přidělena, abyste se s námi mohli kontaktovat?"

„Byli naši zástupci vždy zdvořilí?"

„Jak dlouho nám trvá odpověd?"

„Jak dlouho pracujete v bance?"

„Jaké obchodní číslo nyní používáte?"

„Zaznamenali jste někdy v našich informacích nějakou nepřesnost?"

„Máte nějaké návrhy na zlepšení kvality našich služeb?"

„Byla byste ochotná pravidelně vyplňovat dotazníky, které bychom zasílali do pobočky?"

Chris opětovně souhlasila. Chvíli nezávazně rozmlouvali. Po ukončení hovoru se Chris vrátila ke své práci.

Třetí telefonát: Henry McKinsey

„CreditChex, u telefonu Henry McKinsey. Co pro vás mohu udělat?"

Volající řekl, že telefonuje z National Bank. Uvedl správné obchodní číslo a dále příjmení a číslo pojištění osoby, o které hledal informace. Henry se zeptal na datum narození. Volající mu je uvedl.

„Wells Fargo hlásilo NSF v roce 1998 v částce 2066 $," čte Henry po chvíli údaje z obrazovky počítače. (NSF označuje nedostatečné prostředky. V bankovním žargonu se to týká šeků, které byly vystaveny bez dostatečného krytí).

„Bylo ještě něco od té doby?" „Ne."

"Byly ještě nějaké jiné dotazy?"

"Podíváme se. Tak — tři a všechny za poslední měsíc. Bank of Chicago.“

Při čtení posledního jména — Schenectady Mutual Investments — se zakotktal a musel hláskovat. „Stát New York,“ dodal.

Soukromý detektiv v akci

Všechny tři rozhovory uskutečnila stejná osoba: soukromý detektiv kterého pojmenujme Oscar Grace. Grace získal nového klienta, jednoho z prvních. Tento bývalý policista si všiml, že část jeho nové práce se mu zdá obyčejná a část představuje výzvu pro jeho znalosti a invenci. Tuto práci mohl jednoznačně zařadit do kategorie výzev.

Drsní detektivové z románů jako Sam Spade a Philip Marlowe vysedávali dlouhé noční hodiny ve svých automobilech číhaje na příležitost aby načapali nevěrného manžela. Opravdoví detektivové dělají to samé. Kromě toho se zabývají méně popisovanými, ne však méně účinnými formami pátrání ve prospěch bojujících manželů. Opírají se ve větší míře o sociotechniku než o přemáhání ospalosti během nočního bdění.

Nová Graceova klientka byla žena, jejíž vzhled naznačoval, že s rozpočtem na oblečení a šperky nemá problémy. Jednoho dne vešla do kanceláře a usedla na jediné kožené křeslo, které nebylo zavalené stohy papíru. Položila svou velkou kabelku od Gucciho na psací stůl tak, aby logo směřovalo ke Graceovi, a prohlásila, že zamýšlí oznámit manželovi, že se chce rozvést. Přiznala zároveň, že je tu jeden „malý problém".

Zdálo se, že mužíček byl o krok napřed. Stihl vybrat peníze z jejich konta a ještě větší sumu z brokerského účtu. Zajímalo ji, kde by se tyto peníze mohly nacházet, ale její advokát jí v tom nechtěl moc pomoci. Grace předpokládal, že to byl jeden z těch výše postavených chlápků, kteří si nechtějí špinit ruce tak pochybnými věcmi jako „kam se poděly ty peníze?".

Mohl by jí Grace pomoci?

Ujistil ji, že to bude maličkost, uvedl svou sazbu, vyjasnil, že dodatečné výdaje hradí také ona a převzal šek s první splátkou honoráře

Potom si uvědomil potíž. Co může dělat, když se takovou prací nikdy nezabýval a nemá ponětí o tom, jak vypátrat stopy, kudy peníze šly? Je třeba postupovat drobnými krůčky. Zde je Graceova verze, jak ji znám já.

* * *

Věděl jsem o existenci CreditChex i o tom, jak banky využívají jejich služeb. Moje bývalá žena kdysi v bance pracovala. Neznal jsem však žargon a procedury a pokus zeptat se mé bejvalky by byl jen ztrátou času.

Krok první: zjistit terminologii a zorientovat se, jak formulovat otázky, aby zněly věrohodně. V bance, kam jsem zavolal, byla Kim, moje první partnerka, podezíravá, když jsem se jí zeptal, jak se při telefonátech do CreditChex identifikují. Zaváhala. Nevěděla, co říci. Odradilo mě to? Ani náhodou. Ve skutečnosti bylo pro mne její zaváhání znamením, že musím svoji žádost odůvodnit, aby pro ni zněla věrohodně. Když jsem vyprávěl historku o výzkumu pro potřeby knížky, zbavil jsem Kim podezřeni. Stačí říct, že jste spisovatelem nebo filmovou hvězdou a všichni se hned stanou otevřenější.

Kim měla ještě další vědomosti, které by se mi hodily — například na jaké informace se ptá CreditChex, aby identifikoval osobu, na kterou ptáme, na co se jich můžeme ptát a věc nejdůležitější: obchodní číslo klienta Byl jsem připraven jí ty otázky položit, ale její váhání mě varovalo. Spolkla sice historku o spisovateli, ale chviličku ji trápilo podezření. Kdybych odpověděla hned, poprosil bych ji o prozrazení dalších detailů dotyčných procedur.

Je třeba nechat se vést instinktem, pozorně naslouchat, co ti říkají a jak to říkají. Ta dívka se zdála natolik bystrá, že by mohla vyvolat poplach, kdybych jí začal klást příliš mnoho neobvyklých otázek. Nevěděla sice, kdo jsem a odkud volám, ale už samo rozšíření zvěsti, že je třeba si dávat pozor na telefonáty s dotazy, by nebylo žádoucí. Je lepší *nespálit zdroj* — třeba sem ještě někdy budeme chtít znovu zavolat.

Žargon
****
Spálení zdroje — útočník spálil zdroj, když dopustí, aby oběť poznala, že na ní byl podniknut útok. Tehdy pravděpodobně upozorní ostatní

pracovníky a vedení o tom, že útok nastal. V takové situaci bude těžké tento zdroj ještě někdy využít.
****

Vždycky si všímám maličkostí, ze kterých mohu usoudit, nakolik je daná osoba ochotná ke spolupráci. Hodnotím to na stupnici, která začíná na: „Zdáš se mi příjemnou osobou a věřím ti všechno, co říkáš" a končí na „Volejte policii, ten chlápek něco kuje!".

Kim byla někde uprostřed stupnice, proto jsem zavolal ještě do jiné pobočky. Během mého druhého rozhovoru s Chris se trik s anketou podařil dokonale. Taktika spočívala v propašování důležitých otázek mezi jinými, nepodstatnými, které však dávají celku důvěryhodný dojem, než sem se zeptal na obchodní číslo u CreditChex, vykonal jsem poslední test když jsem položil osobní dotaz – jak dlouho už pracuje v bance.

Osobní otázka je jako nášlapná mina – někteří lidé ji přejdou, ani si ji nevšimnou, zatímco jiní při ní vybuchnou a vyšlou tak varovný signál. Pokud tedy žádám osobní otázku a ona mi na ni odpoví a ani tón hlasu se nezmění, znamená to, že ji pravděpodobně podstata otázky neudivila. Nyní mohu klást další dotazy, aniž bych vzbuzoval podezření, a zřejmě obdržím odpověď, na kterou čekám.

A ještě jedna věc. Dobrý detekiv nikdy nekončí rozhovor hned, jak získa informaci. Dvě tři dodatečné otázky, trocha nezávazného rozhovoru a pak je možné se rozloučit. Jestli si dotazovaný něco z našeho dialogu zapamatuje, budou to nejspíš ty poslední otázky. Zbytek obvykle zůstává v paměti zahalen mlhou.

Tak mi tedy Chris sdělila obchodní číslo i číslo telefonu, které živají při dotazech. Byl bych šťastný, kdyby se mi podařilo položit ještě několik otázek týkajících se toho, jaké informace lze z CreditChex vytáhnout. Ale raději nepokoušet štěstí.

Bylo to, jako kdyby mi CreditChex vystavil bianco šek – jsem ted telefonovat a získávat informace, kdy se mi zachtělo. Ani jsem nemusel za služby platit. Jak se ukázalo, pracovník CreditChex s potěšením sdělil přesně ty informace, které jsem potřeboval: udal dvé místa, kde se muž mé klientky ucházel o otevření konta. Kde se v ta vém případě nacházely peníze, které hledala jeho „již brzy bývalá“? Kde jinde, než v ústavech prozrazených firmou CreditChex.

Analýza podvodu

Celý útok se opíral o jednu ze základních zásad sociotechniky: získat přístup k informaci, která je pracovníkem mylně považována za nevinnou.

První bankovní úřednice potvrdila termín, kterým se označuje identifikační číslo používané při kontaktu s CreditChex – „obchodné číslo". Druhá sdělila telefonní číslo používané ke spojení s CreditCheck a nejdůležitější informaci, obchodní číslo přidělené bance – pokládala za nevinné. Koneckonců si myslela, že rozmlouvá s někým z CreditCheck, co tedy může být špatného na tom, když jim to číslo řekne?

Toto všechno vytvořilo základ pro třetí rozhovor. Grace měl vše, co potřeboval, aby mohl zatelefonovat do CreditChex předstíraje, že je pracovníkem National Bank – jednoho z jejich klientů a prostě je požádal o informace, které potřeboval.

Grace uměl krást informace tak jako dobrý podvodník peníze a k tomu měl rozvinutý talent vycítit jakou mají lidé povahu a co si právě myslí. Znal všeobecnou taktiku skrývání klíčových otázek mezi úplně nevinnými. Věděl, že osobní otázka dovoluje před nevinným poloze dotazu na obchodní číslo zjistit ochotu druhé úřednice ke spolupráci.

Chybě první úřednice, která spočívala v potvrzení terminologie identifikační číslo, se v podstatě nedalo vyhnout. Tato informace je v

bankovnictví tak široce známá, že se zdá bezcenná. Typický příklad neškodné informace. Avšak druhá úřednice, Chris, neměla odpovídat na otázky, aniž by si ověřila, že volající je opravdu ten, za koho se vydával. Přinejmenším se měla zeptat na jeho jméno a číslo telefonu a zavolat mu zpět.Týmto způsobem, kdyby později vznikly nějaké pochybnosti, by měla alespoň telefonní číslo, ze kterého volala daná osoba. V tomto případě by telefonát vetřelci značně ztížil předstírání, že je z CreditChex.

Lepším řešením by byl telefonát do CreditChex na číslo, které banka běžně používala a ne na číslo, které by dal volající. Účelem takového telefonátu by bylo ověření, jestli tam taková osoba skutečně pracuje a jestli forma právě provádí nějaké výzkumy u klientu. Vezmeme-li v úvahu praktické aspekty a fakt, že většina lidí pracuje pod tlakem termínů, je přehnané takovou verifikaci vyžadovat, ledaže by měl pracovník podezření, že je to pokus o průnik.

Poznámka Mitnicka
****
V této situaci plnilo obchodní číslo stejnou úlohu jako heslo. Kdyby personál banky zacházel s tímto číslem jako s čísly PIN svých bankovních karet, uvědomil by si důvěrný charakter této informace.
****

Past na inženýra

Je známo, že je sociotechnika často používána „lovci mozků" za účelem získání talentovaných pracovníků. Zde je příklad.

Koncem devadesátých let jistá nepříliš poctivá personální agentura podepsala smlouvu s novým zákazníkem, který hledal elektroinženýry se zkušenostmi z telekomunikační branže. Záležitostí se zabývala žena známá svým hlubokým hlasem a svůdným chováním, což se naučila, aby si získávala důvěru a blízký kontakt přes telefon.

Rozhodla se provést nájezd na operátora mobilní telefonie a pokusit se objevit lidi, kteří by mohli přejít ke konkurenci. Nemohla samozřejmě zavolat na ústřednu firmy a říci: „Chtěla bych mluvit s nějakou osobou s pětiletou praxí na pozici inženýra." Namísto toho z důvodů, které se za chvili vyjasní, začala lov od vyhledání zdánlivě bezcenné informace, takové, kterou je firma ochotna sdělit skoro každému, kdo si o ni řekne.

První rozhovor: recepční

Žena, predstavující sa jako Didi Sands uskutečnila telefonát do hlavního sídla mobilního operátora. Zde je část rozhovoru.

RECEPČNÍ: „Dobrý den, zde Marie. Jak vám mohu pomoci?"

DIDI: „Mohla byste mne spojit s odborem dopravy?"

R: „Nejsem si jista, jestli takový odbor existuje. Podívám se do známu. A kdo volá?"

D: „Didi."

R: „Voláte z budovy, nebo...?"

D: „Ne, volám z venku."

R: „Didi jak dál?"

D: „Didi Sands. Měla jsem někde linku na dopravu, ale ztratil jsem ji."

R: „Moment."

Aby utišila podezření, položila Didi na tomto místě lehkou konverzační otázku, která měla ukázat, že je „naše" a že jí není neznámé rozložení budov firmy.

D: „Ve které budově pracujete? V Lakeview nebo v hlavní?"

R: „V hlavní, (pauza) Tady je to číslo – 805 555 6469."

Aby měla něco do zásoby, kdyby jí telefon do dopravy nijak nepomohl, požádala Didi ještě o telefon na odbor nemovitostí. Recepční sdělila i ten. Když Didi poprosila o přepojení na dopravu, recepční to zkusila, ale bylo obsazeno.

V tomto okamžiku se Didi zeptala na třetí číslo, do účtárny, která se nacházela v hlavním sídle firmy v Austinu, stát Texas. Recepční ji požádala, aby chvilku počkala a vypnula na chvíli linku. Že by volala na ochranku, že má podezřelý telefonát a něco se jí nelíbí? Kdepak. A Didi dokonce tuto možnost ani nebrala v úvahu. Byla sice trochu dotěrná, ale to pro recepční při jejich práci není nic neobvyklého. Přibližně po minutě se recepční vrátila, zjistila číslo na účtárnu a spojila Didi s tímto oddělením.

Druhý rozhovor: Peggy

Následující rozhovor proběhl takto:

PEGGY: „Účtárna, Peggy."

DIDI: „Dobrý den, Peggy, tady Didi z Thousand Oaks."

P: „Dobrý den, Didi."

D: „Jak se daří?"

P: „Dobře."

Didi nyní použila termínu, který se ve firemním světě často vyskytuje a který popisuje kód poplatku, připisující výlohy konkrétní organizační jednotce nebo pracovní skupině:

D: „Skvělé. Měla bych dotaz. Jak mám najít nákladové středisko ke konkrétnímu odboru?"

P: „Musíš se spojit s účetním analytikem daného odboru."

D: „Nevíš, kdo je analytikem pro ředitelství v Thousand Oaks? Právě vyplňuji formulář a neznám správné nákladové středisko."

P: „Ja jen vím, že když někdo potřebuje nákladové středisko, tak volá analytikovi.“

D: „A máte vlastni nákladové středisko pro svůj odbor v Texasu?"

P: „Máme vlastní nákladové středisko. Ale nedali nám kompletní seznam středisek.

D: „A z kolika čísel se skládá nákladové středisko? Jaké je například vaše nákladové středisko?"

P: „A vy jste 9WC,nebo SAT?“

Didi neměla ponětí, jakých odboru se týkala tato označení, ale to jí nevadilo. Odpověděla: „9WC“.

P: „Tak to má obvykle 4 znaky. Odkud že voláš?"

D: „Z ředitelství v Thousand Oaks."

P: „Aha, tak pro Thousand Oaks to je 1A5N. N jako Nancy."[2]

Stačilo, aby Didi mluvila dostatečně dlouho s osobou, která byla ochotná pomoci, a získala číslo nákladového střediska, které potřebovala. Byla to jedna z těch informací, kterou se nikdo nesnaží chránit, protože se zdá pro kohokoliv mimo organizaci bezcenná.

Třetí rozhovor: užitečný omyl

V následujícím kroku Didi vymění číslo nákladového střediska za něco, co má skutečnou hodnotu. Využívá ho jako vyhraný žeton v následujícím kole hry.

Nejprve zavolala na odbor nemovitostí a předstírala, že se dovolala na špatné číslo. Začala slovy: „Nechtěla bych obtěžovat..." a pokračovala, že je

[2] Pozn překl.: Podle české hláskovací tabulky se u písmene N má říkat Neruda, což se mi ale v amerických reáliích zdálo poněkud úsměvné.

zaměstnancem firmy a někde ztratila telefonní seznam a ted neví, komu by měla zavolat, aby dostala nový... Muž jí odpověděl, že tištěny seznam už není důležitý, protože aktuální seznam je přístupný na firemním intranetu.

Didi odvětila, že by dala přednost tištěné verzi. Muž jí poradil, aby zatelefonovala do edičního oddělení a následně jí z vlastní vůle – možná chtěl trochu prodloužit hovor se ženou s tak příjemným hlasem - vyhledal a sdělil příslušné telefonní číslo.

Čtvrtý rozhovor: Bart z edičního

V edičním oddělení mluvila s člověkem, který se jmenoval Bart. Didi pověděla, že volá z Thousand Oaks a že mají nového konzultanta, který by potřeboval kopii vnitřního telefonního seznamu. Dodala, že pro konzultanta bude tištěný seznam lepší, i kdyby nebyl nejčerstvější. Bart odvětil, že musí vyplnit příslušný formulář a poslat mu ho.

Didi prohlásila, že jí došly formuláře, věc dosti spěchá a jestli by mohl být Bart tak laská v a tu žádost vyplnil za ni. Souhlasil. A dokonce rád. Didi mu poskytla údaje. Místo fiktivní adresy mu sdělila něco, co sociotechnici označují jako *tajná schránka* – v tomto případě šlo o jednu z poštovních skříněk, které si její firma pronajímala speciálně pro takovéto příležitosti.

> *Žargon*
> **********
> **Tajná schránka** – v jazyce sociotechniků místo, kam obět posílá dokumenty nebo jiné zásilky (může to být například poštovní skříňka, kterou si sociotechnik pronajímá, obvykle pod falešným jménem).
> **********

A ted se bude hodit dřívější kořist. Za vyslání seznamu se musí platit. Bez problémů – Didi uvádí číslo nákladového střediska Thousand Oaks: „1A5N – N jako Nancy."

Po několika dnech, když dorazil telefonní seznam, Didi zjistila, že získala dokonce více, než předpokládala. Seznam obsahoval nejen jména a telefonní čísla, ale ukazoval také, kdo kde pracuje, tedy organizační schéma firmy.

Didi se svým zastřeným hlasem mohla začít telefonický lov mezi pracovníky. Informace nezbytné k započetí vyhledávání získala díky výmluvnosti, kterou si pěstuje každý pokročilý sociotechnik. Nyní mohla přejít k náboru.

Analýza podvodu

V tomto sociotechnickém útoku Didi začala od získání telefonních čí do tří oddělení firmy, která ji zajímala. Bylo to jednoduché, protože čísla nebyla chráněná, zvláště ne před pracovníky firmy. Sociotechnik se učí hovořit tak, jako by byl zaměstnancem firmy – Didi to zvládla skvěle. Jeden z telefonátů ji přivedl k číslu nákladového střediska, které vzápětí použila k získání vnitřního telefonního seznamu.

Hlavní nástroje, které použila, byly přátelský tón, firemní terminologie a u poslední oběti troška verbálního svůdného mrkání řasami.

A ještě jedním, tím zásadním nástrojem, je sociotechnikova schopnost sledovat, schopnost zdokonalovaná dlouhou praxí a využívající zkušení jmých podvodníků.

Poznámka Mitnicka
****
Tak jako kamínek v mozaice nemusí jednotlivá informace nic znamenat, ale po složení mnoha takových úlomku do celku získáváme jasný obraz. V tomto případě byla tím obrazem celá vnitřní struktura podniku.
****

Další „bezvýznamné" informace

Jaké další zdánlivě nedůležité informace kromě čísla nákladového střediska nebo telefonního seznamu mohou být pro vetřelce cennou kořistí?

Telefonát Petera Abelse

„Dobrý den," slyší ve sluchátku Peter Abels, „tady Tom z Parkhurst Travel. Vaše letenky do San Franciska jsou připraveny k vyzvednutí. Máme vám je poslat, nebo si je sami vyzvednete?"

„San Francisco?" ptá se Peter. „Nejedu do San Franciska."

„Jste pan Peter Abels?"

„No to jsem, ale neplánuji žádnou cestu."

„No tak," pobaveně říká volající, „ale třeba byste se do San Franciska chtěl podívat?"

„Jestli dokážete přemluvit mého šéfa...," udržuje Peter žertovný tón.

„To musí být nějaký omyl," objasňuje hlas ve sluchátku. „V našem systému rezervujeme cestu pod číslem pracovníka a asi někdo použil špatné číslo. Jaké je vaše číslo?"

Peter poslušně odrecitoval své číslo. Co by ne? Vždyť je to číslo vidět na každém formuláři, který vyplňuje, mnoho osob ve firmě má k němu přistup: osobní, mzdové a jak je vidět i cestovní kancelář, která není součástí firmy. Nikdo je nepovažuje za tajemství. Jaký je rozdíl, jestli ho sdělí, nebo ne?

Odpověd je prostá. Dvě nebo tři informace mohou stačit k tomu, aby se někdo převtělil za zaměstnance firmy. Sociotechnik se schovává čísi totožnost. Získání jména zaměstnance, jeho telefonu, identifikačního čísla a možná ještě jména a telefonu jeho šéfa stačí i málo zkušenému sociotechnikovi, aby byl pro svou následující oběť přesvědči.

Kdyby ti včera někdo zavolal a řekl, že je z jiného oddělení, a z nějakého věrohodného důvodu tě požádal o tvé identifikační číslo, měl bys nějaké zábrany mu ho sdělit?

A jen tak mimochodem, jaké je číslo tvého sociálního pojištění?"[3]

Poznámka Mitnicka
****
Poučení z příběhu je toto: nesděluj nikomu žádné osobní ani vnitropodnikové informace či čísla, ledaže bys poznal hlas na opačném konci a ten by ty informace opravdu potřeboval.
****

Prevence

Firma je odpovědná za seznámení pracovníků s tím, jaké mohou být následky nepatřičného zacházení s neveřejnými informacemi. Dobře navržená politika

[3] Pozn. překl.: Číslo sociálního pojištěni hraje v USA podobnou roli jako naše rodné číslo.

zabezpečení informací spojená s odpovídajícím vzděláváním a procvičováním značně zvýší u zaměstnanců povědomí o významu firemních informací a o správném zacházení s nimi. Politika klasifikace dat zavádí odpovídající prostředky ohledně zveřejňování informací. Jestliže takováto opatření neexistují, všechny vnitřní informace musejí být považované za důvěrné, pokud není výslovně řečeno jinak.

Abychom předešli úniku zdánlivě neškodných informací z firmy, bylo by dobré uplatnit následující kroky:

- Odbor bezpečnosti informací musí provádět školení seznamující s metodami používanými sociotechniky. Jednou z výše popsaných metod je získávání zdánlivě nepodstatných informací a jejich následné využití s úmyslem vzbudit dočasnou důvěru. Každý zaměstnanec si musí být vědom, že informovanost volajícího co se týče firemních postupů, žargonu a vnitřních identifikátorů jej nijak neopravňuje žádat o informace. Volající může být bývalým pracovníkem nebo vnějším dodavatelem služeb, který má informace umožňující „pohyb" po firmě. Každá firma je tudíž zodpovědná za určení odpovídajících autentikačních metod, které mají zaměstnanci uplatňovat během jednání s osobami, které neznají osobně nebo je nepoznají v telefonu.
- Osoby, které mají za úkol vytvoření politiky klasifikace dat, by měly analyzovat typické druhy informací, které by mohly pomoci při získání přístupu někomu, kdo se prohlašuje za pracovníka. Možná informace vypadají nevinně, ale mohou vést k získání citlivých dat. Určitě bychom nikomu nedali PIN naší kreditní karty, jestlipak bychom ale někomu neprozradili, jaký typ serveru je používaný v naší firmě? Mohl by někdo tuto informaci využít, aby se tvářil jako zaměstnanec, který má přístup k firemní síti?

Občas může obyčejná znalost vnitřní terminologie způsobit, že sociotechnik vypadá autoritativně a věci znalý. Útočník se na to často spoléhá a svou oběť tak ošálí, že mu vyhoví. Například obchodní číslo je identifikátor, který pracovníci oddělení nových účtů dennodenně volně používají. Toto číslo se však významem nijak neliší od hesla. Pokud si každý pracovník uvědomí podstatu tohoto identifikátoru a všimne si, že slouží k pozitivní identifikaci volajícího, možná s ním začne zacházet opatrněji.

Žádná firma — řekněme skoro žádná firma — nesděluje přímé číslo členů vedení nebo dozorčí rady. Většina firem však nemá žádné zábrany sdělovat telefony většiny svých oddělení a jiných organizačních jednotek, zvláště pak osobám, které se zdají být zaměstnanci firmy. Jedním z řešení je uplatnění zákazu sdělování vnitřních linek zaměstnanců, konzultantů a přechodně zaměstnaných lidí jakýmkoliv osobám zvenku. Ba co víc — je třeba vytvořit proceduru, která by krok za krokem popisovala, jak identifikovat osoby žádající o Číslo zaměstnance firmy.

Předmětem zájmu sociotechnikú jsou často kódy účtů pracovních skupin a odborů či vnitřní telefonní seznamy (ať už ve formě výtisku či souboru na intranetu). Každá firma potřebuje písemně zpracované pokyny, které popisují postup sdělování takovýchto informací a které rozdá všem zaměstnancům. Z preventivních důvodů je vhodné zaznamenávat případy zpřístupnění informací lidem mimo podnik.

Takové informace jako zaměstnanecké číslo by neměly být jediným prvkem identifikace. Každý pracovník se musí naučit ověřovat nejen totožnost, ale také důvod žádosti.

V rámci bezpečnostního školení lze zvážit, jestli by nebylo dobré nacvičit následující přístup: učíme se zdvořile odmítat odpovídat na dotazy a poskytovat služby neznámým lidem, dokud nebude ověřena oprávněnost žádosti. Dále: předtím, než podlehneme přirozené ochotě pomáhat jiným, postupujeme podle firemních pokynů popisujících ověřovaní a zpřístupňování neveřejných dat. Tento styl chování sice může v rozporu s naší samozřejmou tendencí

pomáhat, ale trocha paranoie se zdá být nezbytná, abychom se nestali další obětí sociotechnika.

Příběhy uvedené v této kapitole ukazují, jak se zdánlivě nedůležité informace mohou stát klíčem k nejbedlivěji střeženým tajemstvím firmy.

Poznámka Mitnicka
****
Jak hlásá staré rčení, i paranoici mívají opravdové nepřátele. Musíme předpokládat, že každá firma má své nepřátele, jejichž cílem je dostat se do síťové infrastruktury a tedy i k firemním tajemstvím. Opravdu chceme přispět do statistiky počítačových zločinů? Je nejvyšší čas zesílit obranu a zavést odpovídající kontrolní postupy s využitím promyšlených bezpečnostních pravidel a procedur.
****

3

Přímý útok: stačí se zeptat

Mnoho sociotechnických útoků bývá složitých; skládají se z mnoha kroků a důkladného plánování, často spojují manipulaci a technologické znalosti.

Vždy mne však zaráží to, že dobrý sociotechnik dokáže dojít ke svému cíli jednoduchým, přímým útokem. Jak se přesvědčíme, občas stačí o informace prostě požádat.

MLAC — rychlovka

Zajímá vás něčí neveřejné telefonní číslo? Sociotechnik ho může vypátrat půltuctem způsobů (část z nich lze najít v jiných příbězích této knihy), ale nejjednodušší scénář je ten, který vyžaduje jen jeden telefonát. Zde je.

Prosil bych číslo...

Útočník zavolal do mechanizovaného centra přiřazování linek (MLAC) jedné telekomunikační firmy a řekl ženě, které zvedla telefon: „Dobrý den, tady je Paul Anthony. Jsem montážní technik. Poslyšte, mám tu spálenou rozvodnou skříňku. Policie si myslí, že se nějaký chytrák pokoušel podpálit svůj dům, aby získal z pojišťovny prachy. Poslali mne sem, abych tu zapojil novou skříňku s dvěma sty koncovkami. Potřeboval bych vaši pomoc. Jaká zařízení by měla fungovat na South Main pod číslem 6723?"

V jiných odděleních telekomunikačních firmy, kam zavolal, vědeli, že neveřejná telefonní čísla nebo jakékoliv informace přiřazující k jméno Lze sdělovat pouze oprávněným zaměstnancům. Ale o existencii MLAC vědí spíš jen pracovníci firmy. Tyto informace jsou sice chráněné, ale kdo by odmítl pomoci kolegovi, který má vykonat těžkou a důleži práci? Dotazovaná s ním soucítila — vždyť jí se také občas přihodilo, měla velmi náročné pracovní dny — takže trochu pominula zásady a mohla kolegovi ze stejné firmy, který měl problém. Sdělila mu označení kabelů, svorek a všechna čísla přiřazená této adrese.

Analýza podvodu

Jak už si bylo možné v popisovaných příbězích mnohokrát všimnout, znalost firemního žargonu a vnitřní struktury firmy — různých kanceláří a oddělení, jaké mají úkoly a informace — je část základní sestavy nástrojů, které sociotechnik používá.

Poznámka Mitnicka
****
Lidé od přírody důvěřují jiným, zejména když je prosba odůvodněná. Sociotechnici toho využívají, aby využili oběť a dosáhli svých cílu.
****

Na útěku

Člověk, říkejme mu třeba Frank Parsons, už léta utíkal. Neustále po ní pátrala federální vláda[4] za účast v ilegální protiválečné skupině v 60. letech. V restauracích seděl tváří ke vchodu a měl návyk neustále se ohlíž za sebe, což jiné lidi znervózňovalo. Vždy po několika letech se stěhoval jinam.

Jednou takhle přijel do nového města a začal se rozhlížet po práci. Pro někoho takového jako je Frank, který se dobře vyznal v počítačích (a také v sociotechnice, ale o tom ve svých motivačních dopisech jaksi nepsal), nebylo těžké nalézt práci. S výjimkou období recese nemají talentovaní lidé s hlubokými technickými znalostmi počítačů s nalezením práce problém. Frank rychle našel nabídku dobře placené práce v velkém pečovatelském zařízení poblíž svého bydliště.

To je ono, pomyslel si. Ale když se začal prokousávat formuláři, narazil na překážku: zaměstnavatel vyžadoval od uchazeče výpis z trestního rejstříku státní policie. Štůsek papírů obsahoval odpovídající formulář se žádosti, na kterém bylo též vyhrazené místo na otisky prstů. Sice byl požadován jen otisk pravého ukazováčku, ale jestli ten otisk zkontrolují v databázi FBI, pravděpodobně bude sice brzy pracovat, ale v kuchyni „pečovatelského domu" sponzorovaného federální vládou.

Na druhou stranu Franka napadlo, že by se mu možná mohlo podařit proklouznout. Co když státní policie jeho otisky do FBI vůbec nepošle? Ale jak to zjistit?

Jak? Od čeho je sociotechnikem? Jak myslíte, že se to dozvěděl? Samozřejmě uskutečnil jediný telefonát na policii: „Dobrý den. Provádíme vvzkum pro Ministerstvo spravedlnosti státu New Jersey. Zkoumáme požadavky na nový systém identifikace otisků prstů. Mohl bych mluvit s někým, kdo se v tom u vás dobře orientuje a mohl by nám pomoci?"

Když místní odborník přišel k telefonu, Frank zadal řadu otázek na systém, který používají, možnosti vyhledávání a ukládání otisků. Měli jste se zařízením nějaké potíže? Využíváte vyhledávač otisků NCIC (National Crime Information Center)[5], nebo jen v rámci státu? Nebylo obtížné naučit se zacházet se zařízením?

Chytře vpašoval do otázek jednu klíčovou.

Odpověd mu zněla jako rajská hudba. Ne, nebyli provázáni s NCIC, kontrolovali pouze u státního Cli (Criminal Information Index)[6]. To bylo všechno, co chtěl Frank vědět. V tomto státě neměl záznam. Poslal tedy svou přihlášku, byl zaměstnán a nikdy se u něho nikdo neobjevil se slovy: „Tito pánové jsou z FBI a říkají, že by si s tebou chtěli popovídat."

Poznámka Mitnicka
****
Důmyslní zloději informací se neobávají volat federálním či státním úředníkům nebo představitelům místních úřadů, aby se dozvěděli něco o procedurách na podporu dodržování zákonů. S takovými informacemi je sociotechnik schopen obejít standardní firemní zabezpečení.
****

Nechtě to na vrátnici

[4] Pozn. překl.: Ani ne tak vláda, jako federální orgány, například FBI. Těžko lze očekávat, že by nějakého podvodníčka stíhala opravdu vláda v tom slova smyslu, jak ho používáme my, tedy těch asi 20 pánů a dam. Vládním úřadům či státní správě vůbec se v Americe prostě říká vláda.

[5] Pozn. překl.: Národní centrum informací o zločinech.

[6] Pozn. překl.: Rejstřík informací o zločinech.

V rozporu s mýtem elektronické bezpapírové kanceláře firmy stále potisknou tuny papíru denně. Důležitý dokument může být v naší firmě ohrožen, i když zavedeme příslušná bezpečnostní opatření a označíme jej jako důvěrný. Zde je příběh, který ukazuje, jak může sociotechnik přijít k vašim nejtajnějším dokumentům.

V osidlech podvodu

Každý rok publikuje telekomunikační společnost knížku „Seznam testovacích čísel" (nebo alespoň publikovala — a jelikož jsem stále ještě pod dohledem kurátora, nebudu raději zjišťovat, jestli tak činí i nadále). Tento dokument představoval pro phreakery ohromný poklad, protože obsahoval seznam přísně chráněných telefonních Čísel, která používali firemní odborníci, technici a jiné osoby k testování meziměstského spojení a ke kontrole trvale obsazených čísel.

Jedno z těch čísel, v žargonu označované jako *smyčka* (loop-around) bylo obzvláště užitečné. Phreakeři ho používali k vyhledávání jiných phreakerů a tlachání s nimi zadarmo. Kromě toho díky němu tvořili čísla pro zpětná volání, která bylo možné sdělit například v bance. Sociotechnik nechával úředníkovi v bance číslo, na kterém byl k zastižení. Když banka vytočila testovací číslo (smyčku), phreaker mohl hovor klidně přijmout, protože byl zabezpečený použitím čísla, přes které ho nešlo vystopovat.

Seznam testovacích čísel zpřístupňoval mnoho užitečných údajů, které mohly být phreakery lačnými informací využity. A tak se nově vydaný seznam každoročně stával objektem zájmu mladých lidí, jejichž koníčkem byl průzkum telefonní sítě.

> *Poznámka Mitnicka*
> **********
> Bezpečnostní školení vedené v souladu s politikou firmy, navrženou za účelem ochrany dat, se musí týkat všech jejích zaměstnanců, zejména pak těch, kteří mají elektronický či fyzický přístup k datům.
> **********

Stevův fígl

Telekomunikační firmy se pochopitelně nesnaží ulehčovat přístup k takovému seznamu, proto se tady phreakeři musejí vykázat jistou dávkou invence. Co mohou udělat? Dychtivý mládenec, jehož snem bylo získat seznam, mohl postupovat podle následujícího scénáře.

* * *

Jednoho teplého podzimního večera v jižní Kalifornii zavolal Steve do kanceláře nevelké telekomunikační firmy. Odtud vedou linky do všech domovu, kanceláří a škol v okolí.

Když služebukonající technik přijal hovor, Steve prohlásil, že volá z oddělení firmy, které se zabývá tiskem a distribucí tištěných materiálů. Máme pro vás nový ‚seznam testovacích čísel'," řekl. „Ale s ohledem na bezpečnost vám nemůžeme předat nový seznam, dokud od vás nedotkneme ten starý. Kluk, který rozváží seznamy, má zpoždění. Kdybyste mohl nechat váš seznam na vrátnici, mohl by se jen zastavit, vyzvednout starý seznam, zanechat nový a jet dál."

Nic netušící technik uznává, že to zní rozumně. Dělá přesně to, o co bvl požádán, a nechává na vrátnici svůj výtisk seznamu. Je na něm napsáno velkvm červeným písmem: „FIREMNÍ TAJEMSTVÍ — PO SKONČENI PLATNOSTI ZNIČIT."

Steve přijíždí a pozorně se rozhlíží kolem, jestli tu není policie nebo firemní ochranka, která by se mohla ukrývat za stromy nebo ho pozorovat ze zaparkovaného auta. Nikoho nevidí. V klidu si vyzvedává vytouženou knížku a odjíždí.

Další příklad, jak je pro sociotechnika snadné něco získat pouhým požádáním.

Plynový útok

Nejen firemní materiály se mohou stát předmětem sociotechnikova zájmu. Občas jsou jeho kořistí klienti firmy. Práce v oddělení klientských služeb přináší někdy frustraci, někdy smích, někdy nevinné chyby — některé mohou mít nepříjemné důsledky pro klienty firmy.

Příběh Josie Rodriguez

Josie Rodriguez pracovala třetí rok v kanceláři klientských služeb firmy Hometown Electric Power ve Washingtonu. Byla pokládána za jednu z lepších pracovnic. Byla bystrá a rozvážná.

V týdnu okolo Dne díkůvzdání[7] zazvonil telefon. Ze sluchátka se ozývá:

„Tady Eduardo z fakturačního oddělení. Mám na druhé lince jednu paní. Je to sekretářka z ředitelství, která pracuje pro jednoho z náměstků. Žádá mě o jednu informaci a já nyní nemůžu pracovat na počítali protože jsem dostal od jedné holky z osobního e-mail se subjectem „ILOVEYOU" a když jsem otevřel přílohu, počítač mi zatuhl. Virus. Nechal jsem se napálit hloupým virem. Mohl bych vás proto poprosit o vyhledání informace o jednom zákazníkovi?"

„Jistě," odpověděla Josie. „Ono to úplně ničí počítač? To je hrozné!"

„Ano."

„A co pro vás mohu udělat?" zeptala se Josie.

Ted mohl útočník uplatnit informace, které získal dříve během pátrání po různých datech, která mu měla pomoci při získávání důvěry. Dozvěděl se, že hledaná informace je uložena v tzv. „systému informací zákaznických faktur" (CBIS) a dozvěděl se také, jak ho pracovníci nazývali — CBIS.

„Mohla byste vyvolat účet ze CBISu?"

„Ano, jaké je číslo konta?"

„Nemám číslo, musíme hledat podle jména."

„Dobrá, jaké je to jméno?"

„Heather Marning," přehláskoval jméno a Josie je vyťukala do počítače.

„Hotovo."

„Výborně. To je běžný účet?"

„Mhm, běžný."

„Jaké má číslo?"

„Máte něco na psaní?"

„Mám."

„Číslo konta je BAZ6573NR27Q."

Zopakoval číslo konta a otázal se: „A jaká je adresa klienta?"

Sdělila mu adresu.

„A telefon?"

Josie poslušně přečetla i tuto informaci.

Volající jí poděkoval, rozloučil se a zavěsil. Josie přijala další hovor a dál už o tom nepřemýšlela.

[7] Pozn. překl.: V USA čtvrtý čtvrtek v listopadu.

Výzkumná práce Arta Sealyho

Art Sealy opustil práci redaktora na volné noze pracujícího pro malé nakladatelství, když si uvědomil, že si může vydělávat získáváním informací pro spisovatele a pro film. Brzy zjistil, že honoráře, které mohl pobírat, rostou úměrně s tím, jak se blíží k neostré hranici oddělují činnost legální od nezákonné. Aniž by si to uvědomil, natož aby to nazval pravým jménem, stal se sociotechnikem používajícím metody známé každému lovci informací. Ukázalo se, že je v této oblasti talentem od přírody, protože sám došel k postupům, které se většina sociotechniků musí naučit od jiných. Brzy překročil zmíněnou hranici bez sebemenšího pocitu viny.

* * *

Najal si mne chlápek, který psal knihu o vládě z doby prezidenta Nixona a hledal informátora, který by mu dodal méně známé skutečnosti o Williamu E. Simonovi, ministru financí v Nixonově vládě. Pan Simon zemřel, ale autor znal jméno ženy, která u něj pracovala. Byl si téměř jist, že bydlí ve Washingtonu, ale nedokázal zjistit její adresu. Neměla ani telefon, nebo alespoň její číslo nebylo v telefonním seznamu. Když mi tedy zavolal, řekl jsem mu, že to není žádný problém.

To je práce, kterou lze obvykle vyřídit jedním nebo dvěma telefonáty, pokud se při tom myslí hlavou. Od každého místního podniku veřejných služeb lze snadno vytáhnout informace. Samozřejmě je potřeba si trošičku vymýšlet, ale co koneckonců znamená jedna neviňoučká lež?

Rád používám pokaždé jiný přístup — potom je to zajímavější. „Tady ten-a-ten ze sekretariátu ředitele" vždycky fungovalo spolehlivě. Nebo „mám na drátě někoho z kanceláře náměstka XY", což také mnohokrát zafungovalo.

Je potřeba vypěstovat si určitý sociotechnický instinkt. Vycítit u osoby na druhém konci ochotu ke spolupráci. Tentokrát se mi poštěstilo, narazil jsem na přátelskou a užitečnou paní. Stačil jeden telefonát a adresa a telefon byly mé. Úkol splněn.

Analýza podvodu

Josie si samozřejmě uvědomovala, že informace o klientovi jsou důvěrné. Nikdy by si nedovolila hovořit o účtu nějakého klienta s jiným klientem nebo prozradit někomu cizí osobní údaje.

Ale k volajícímu člověku z téže firmy se přistupuje jinak. Kolega z práce je člen téhož týmu — musíme si při práci pomáhat. Člověk z fakturačního oddělení by si mohl informace zjistit v počítači sám, kdyby mu ystem nenarušil zákeřný virus. Byla ráda, že mohla pomoci spolupracovníkovi.

Art se postupně přibližoval ke klíčové informaci, po které opravdu pátral zadávaje cestou otázky na věci pro něj nedůležité, jako je například číslo konta. Zároveň údaj o číslu konta představoval únikovou cestu — kdyby Josie začala něco tušit, uskutečnil by jiný telefonát, který by měl více šancí uspět, protože znalost čísla účtu by ho učinila v očích dalšího úředníka ještě důvěryhodnějším.

Josie se ještě nikdy nestalo, aby jí někdo tímto způsobem lhal. Nenapadlo by ji, že volající vůbec nemusí být z fakturačního oddělení. Vina samozřejmě není u Josie, protože nebyla dobře proškolena o zásadách ověřování totožnosti volajícího před probíráním informací týkajících se něčího konta. Nikdy jí nikdo neřekl o nebezpečích takového rozhovoří který s ní Art uskutečnil. Nebylo to součástí politiky firmy, předmětem školení a její nadřízený s ní o tom také nikdy nemluvil.

Poznámka Mitnicka
****

Neměli bychom si myslet, že všechny sociotechnické útoky musejí být důkladně promyšlenou intrikou, tak složitou, že je prakticky neodhalitelná. Některé útoky jsou překvapivě přímé, jednoduché. Někdy se prosté stačí jenom zeptat.
****

Prevence

Bod, který je potřeba přidat do plánu bezpečnostního školení, se týká skutečnosti, že i když volající nebo návštěvník zná jména nějakých osob z podniku nebo zná žargon a postupy, neznamená to, že je opravdu tím, za koho se prohlašuje. Rozhodně tím nezískává oprávnění k získávání vnitřních informací nebo k práci na našem počítači či podnikové síti. Školení musí jasně učit, že v případě pochybností se musí ověřovat, ověřovat a ověřovat.

V dávných časech byl přístup k vnitřním informacím znamením hodnosti a privilegiem. Zaměstnanci otevírali pece, spouštěli stroje, psali dopisy, vyplňovali hlášení. Předák nebo vedoucí jim říkal, co mají dělat, kdy a jak. Pouze předák nebo šéf věděli, kolik toho má každý dělník udělat na jedné směně, jaké barvy a jaké rozměry se vyrábějí tento týden, následující týden a na konci měsíce.

Pracovníci obsluhovali stroje, používali nářadí a využívali materiál. Šéfové měli informace a pracovníci se dovídali jen to, co bylo nezbytné pro jejich práci.

Dnes to vypadá poněkud jinak, že? Mnoho pracovníku v továrnách obsluhuje nějaký počítač nebo stroj počítačem řízený. Zaměstnancům jsou dostupné kritické informace, což jim usnadňuje výkon jejich práce v současnosti většina věcí, které dělají, má nějaký vztah k informacím. Proto také firemní bezpečnostní politika musí zasahovat všude, nezávisle na postavení. Každý musí pochopit, že nejen šéfové a vědení disponují informacemi, které mohou zajímat útočníka. Dnes se může stát předmětem útoku pracovník na každém stupni, dokonce ani nemusí pracovat s počítači. Čerstvě přijatý konzultant v oddělení zákaznických služeb může představovat slabý článek, který sociotechnik využije ke svým záměrům.

Bezpečnostní školení a politika firmy musejí posilovat právě takovéto slabé články.

4

Budování důvěry

Některé tyto příběhy by mohly svádět k dojmu, že považuji pracovníky firem za úplné idioty schopné nebo snad dokonce ochotné vyzradit každé tajemství. Sociotechnik si uvědomuje, že to není pravda. Proč jsou tedy útoky sociotechnikú tak úspěšné? Určitě ne proto, že jsou lidé hloupí nebo zbavení zdravého rozumu. Jsme pouze lidé — každého z nás je možné podvést. Pod vlivem jistého druhu manipulace můžeme uvěřit tam, kde to nebylo na místě.

Sociotechnik předem předpokládá, že se setká s podezíravostí nebo odporem a je vždy připravený na překonávání bariér nedůvěry. Dobrý sociotechnik plánuje svůj útok jako šachovou partii, předvídá otázky, které může oběť klást a připravuje si patřičné odpovědi.

Jednou z typických metod je budování pocitu důvěry u oběti. Jak si může podvodník získat naši důvěru? Ví, jak na to...

Poznámka
****
Když si tu povídáme o sociotechnicích, phreakerech a podvodnících, obvykle používám mužský rod. Není to šovinismus, ale prostě to odráží skutečnost, že většina osob v této „branži" jsou muži. Přestože v současnosti není mnoho žen zabývajících se sociotechnikou, jejich počet stále roste.

Ženy v roli sociotechnikú jsou natolik vyzrálé, že vědí, že pouhý zvuk dámského hlasu neprolomí žádnou bariéru. Mají však jednu velkou výhodu, protože při překonávání překážek mohou využívat svou sexualitu. Na stránkách této knihy je však slabší pohlaví zastoupeno jen v nevelké míře.
****

Důvěra jako klíč k manipulaci

Čím více se rozhovor připravený sociotechnikem týká každodenních obyčejných záležitostí, tím lépe se vyhýbá podezřeni. V situaci, kdy nemají k podezíravosti důvod, si sociotechnik snadno získá jejich důvěru. Jakmile se mu to podaří, spouští se padací most a brány hradu se otevírají, aby mohl vejít a získat všechny informace, které potřebuje.

První rozhovor: Andrea Lopez

Andrea Lopez zvedla vyzvánějící telefon ve videopůjčovně, kde pracovala a po chvíli se na její tváři objevil úsměv. Je příjemné, když zákazník říká, že je spokojený se službami firmy. Volající říkal, že má s touto půjčovnou velmi dobré zkušenosti a že by o tom chtěl napsat jejímu manažerovi dopis.

Zeptal se na jeho jméno a korespondenční adresu. Andrea odpověděla, že manažer se jmenuje Tommy Allison a uvedla jeho adresu. Když už chtěla zavěsit, volajícího ještě něco napadlo — řekl: „Možná bych napsat ještě na vaše ústředí. Jaké je číslo vaší půjčovny?"

Andrea mu sdělila i tuto informaci. Volající jí poděkoval, dodal něco milého o tom, jak mu pomohla a rozloučil se.

Takový telefon — pomyslela si — vždycky potěší a den rychleji uteče. Kéž to tak bylo častěji.

Druhý rozhovor: Ginny

„Děkujeme za zavolání do VideoMasters, u telefonu Ginny. Co pro mohu udělat?"

„Dobrý den, Ginny," ohlásil se vesele volající, jako by hovořil s Ginny alespoň jednou týdně. „Tady Tom Allison, manažer z ForestPark, půjčovna číslo 863. Máme tu klienta, který by si chtěl půjčit film *Rocky 5* a nemáme žádnou kopii. Mohla by ses koknout, jestli tam náhodou nemáte?" Po několika okamžicích se vrátila ke sluchátku a řekla: máme tu tři kopie."

„Bezva, zeptám se, jestli by se nechtěl pro ten film zastavit u vás. děkuji. Kdybys něco potřebovala z naší půjčovny, klidně zavolej a chtěj Tommyho. Bylo by mi potěšením, kdybych mohl pro tebe něco udělat.

Během několika následujících týdnů měla Ginny více telefonátů od Tommyho, který prosil o pomoc v různých záležitostech. Byly to obyčejné prosby a Tommy byl vždycky velmi příjemný a nic nenasvědčovalo tomu, že by ji chtěl nějak využít. Byl trošku povídavý, říkal například: „Slyšelas o tom požáru v Oak Park? Prý uzavřeli několik ulic." Jeho telefonáty byli pro ní příležitostí odtrhnout se na chvíli od běžné práce a byla vždy ráda, když se ozval.

Jednodo dne byl Tommy trochu nervózní a ptal se: „Neměli jste nějaké problmémy s počítači?“

„Ne,“ odpovědela Ginny. „Proč?“

„Nějaký chlápek naboural do telefonního sloupu a údržbář z telekomunikační firmy říká, že celá čtvrť bude bez Internetu, dokud to nespraví.“

„To je hrůza! Stalo se někomu něco?"

„Toho řidiče odvezli sanitkou. Hele, mohla bys mi pomoci? Mám tu vašeho zákazníka, který si chce půjčit třetí díl *Kmotra*, ale zapomněl si průkazku. Mohla by ses na něho mrknout?"

„Samozřejmě."

Tommy uvedl jméno a adresu zákazníka. Ginny ho našla v počítači a sdělila mu číslo zákaznického účtu v systému.

„Nějaké pozdní návraty nebo nedoplatky?" ptal se Tommy.

„Nic tu není."

„Bezva. Vložím ho do databáze později, až nám pojede Internet. Chtěl by zaplatit Visa kartou, kterou prý platí ve vaší půjčovně a nemá ji tu při sobě. Jaké je číslo karty a datum platnosti?"

Ginny uvedla číslo i datum.

„Díky za pomoc. Tak zatím." řekl Tommy a zavěsil.

Příběh Doyla Lonnegana

Doyl Lonnegan byl mladý člověk, kterého by určitě nikdo nechtěl spatřit u svých dveří. Kdysi se zabýval vymáháním dluhů z hazardních her. Nyní také občas tyto služby příležitostně poskytuje, pokud ho to nestojí moc usilí. V tomto případě mu byla nabídnuta poměrně zajímavá částka za něco, co vyžadovalo několik telefonátů do půjčovny videokazet. Práce se zdála jednoduchá, ale žádný ze "zákazníku" nevěděl, jak takovou akci provést. Potřebovali tedy někoho s talentem a dovednostmi, jaké měl Lonnegan

* * *

Lidé, kteří nemají u pokerového stolku dost štěstí nebo rozumu, své dluhy obvykle neplatí. Každý to ví. Proč moji známí hráli s podvodníkem, který nedával prachy na stůl? Těžko říct. Možná měli slabé výsledky IQ testu. Ale jednou jsou to mí kamarádi, tak co jsem měl dělat?

Chlápek neměl peníze, tak tedy přijali šek. Ptám se, jestli s tím člověkem prostě nemohli dojít k bankomatu. Ne — vzali si šek. Na 3230 dolarů.

Samozřejmě nebyl krytý. A co jako očekávali? Zavolali mi tedy a ptali se, jestli bych jim mohl pomoci. Už nestrkám nohu mezi dveře, dnes už jsou lepší metody. Požadoval jsem třicet procent provizi a řekl jsem, že uvidím, co se dá dělat. Dali mi jeho jméno a adresu a já usedl k počítači, abych zjistil, kde je nejbližší půjčovna videokazet.

Nespěchal jsem. Čtyři telefonáty, abych se vetřel do přízně zaměstnanců půjčovny a bingo — dostal jsem číslo kreditní karty toho šejdíře.

Jeden známy má bar s obsluhou „nahoře bez". Za padesát doláčů propustí pokerový dluh přes konto baru. A teď ať si to ten šejdíř doma vysvětluje manželce. A co by se stalo, kdyby řekl, že to není jeho transakce? Uvažujme chvilku. On ví, že ho známe. Uvědomuje si, že jestliže jsme dokázali získat číslo jeho kreditky, určitě bychom svedli mnohem víc. Takže bez obav.

Analýza podvodu

První Tommyho telefonáty měly u Ginny jen vybudovat důvěru. Když přišel čas na útok, Ginny nechala ostražitost stranou a brala Tommyho jako pracovníka jiné půjčovny téže sítě.

Proč by ho tak neměla akceptovat? Vždyť už ho znala. Samozřejmě spolu hovořili jen po telefonu, ale stihli už navázat obchodní známost, která je základem důvěry. Jakmile ho přijala jako někoho, kdo pracuje ve stejné firmě, byl už zbytek jednoduchý.

> *Poznámka Mitnicka*
> **********
> Technika budování důvěry známá jako „žihadlo" je jednou z účinnějších sociotechnických taktik. Vždy je třeba se zamyslet, jestli opravdu známe osobu, se kterou hovoříme. Muže se totiž stát, že ten člověk je někdo úplně jiný, než za koho se vydává. Podobně je dobré naučit se pozorovat, ověřovat a posuzovat pracovní postavení či pozici volajícího.
> **********

Variace na téma získání čísla karty

Vybudování pocitu důvěry nevyžaduje pokaždé několik telefonátů oběti, jak by se mohlo zdát z předchozího příběhu. Byl jsem svedkem situace, kdy to zabralo sotva pět minut.

Překvápko, táti!

Seděl jsem jednou v restauraci u stolku s Henrym a jeho tátou. Během hovoru Henry plísnil tátu, že sděluje číslo kreditní karty, jako by to byt číslo telefonu.

jasně, že jim musíš říct číslo kreditky, když něco kupuješ," povídal, ale říkat ho v obchodě, který si ho ukládá do svých záznamů, to je vrchol stupidity."

Jediným místem, kde to dělám, je Studio Video," odpověděl pan Conklin, „ale každý měsíc si prohlížím výpis z karty. Pokud by nějak navyšovali moje platby, všiml bych si toho."

„Samozřejmě," řekl Henry, „ale když mají tvé číslo oni, může jim ho někdo snadno ukrást."

„Myslíš nějaký nepoctivý zaměstnance?"

„Ne. Kdokoliv. Nemusí to být zrovna zaměstnanec."

„Plácáš nesmysly," řekl pan Conklin.

„Můžu tam ted zavolat a přesvědčit je, aby mi řekli číslo tvé karty," odvětil Henry.

„To není možné," řekl otec.

„Dokážu to během pěti minut přímo tady, aniž bych vstal od stolu."

Oči pana Conklina byly zúžené — tak se dívá někdo, kdo si je sebou jistý, ale snaží se to skrýt.

„Říkám ti, že povídáš hlouposti," vyštěkl, vytáhl peněženku a plácl na stůl padesátidolarovou bankovku. „Jestli se ti to podaří, je tvá."

„Nejde mi o tvé peníze, táti," řekl Henry.

Vytáhl mobil, zeptal se otce, do které půjčovny chodí a zazvonil na informace s dotazem na telefonní číslo půjčovny a ještě telefonní číslo půjčovny poblíž Sherman Oaks.

Pak zatelefonoval do půjčovny u Sherman Oaks. Použil taktiku popsanou v předchozím příběhu a rychle získal jméno manažera a číslo půjčovny.

Následoval telefonát do půjčovny, kde měl otec otevřený účet. Použil stárý trik, „vtělil se do manažera", představil se jeho jménem a uvedl také číslo půjčovny, které získal předtím. Potom použil již známý uskok: „Fungují vaše počítače? Protože nám každou chvíli zamrzají." Vyslechl si odpověď a pokračoval: „Víte, paní, mám tu jednoho vašeho klienta, který si chce půjčit nějaké kazety, ale počítače opět nefungují. Potřeboval bych sa podívat na konto klienta a ujistit se, že je u vás zapsaný."

Henry uvedl otcovo jméno. Pak použil variantu dříve popsané metody a poprosil o přečtení údajů z monitoru: adresa, číslo telefonu, datum otevření účtu. Potom řekl: „Omlouvám se, mám už tady strašnou frontu zákazníků. Jaké je číslo karty a datum platnosti?"

Henry jednou rukou držel telefon a druhou psal na útržek. Ukončil hovor a přesunul lístek před otce, který na něho hledě! s vřenou pusou. Vypadal, chudák, jako kdyby se mu zhroutil celý hodnot.

Analýza podvodu

Zamysleme se nad tím, jak bychom se zachovali my ve stejné situaci, když by nás neznámá osoba prosila o laskavost. Když na naše dveře zaklepe otrhaný tulák, nebudeme ho chtít pustit dovnitř. Pokud se však na prahu objeví neznámý dobře oblečený člověk, ve vyleštěných botách, s úsměvem na tváři a slušně vystupující, naše podezíravost bude o mnoho menší. Může to být dokonce Jason z hororu *Pátek třináctého*, ale uvěříme mu, pokud vyhlíží normálně a nedrží v ruce nuž.

Méně zřejmé je, že stejným způsobem hodnotíme lidi i po telefonu Chová se daná osoba, jako by nám chtěla něco prodat? Je přátelská a otevřená, nebo se dá vycítit z její strany jisté nepřátelství a nátlak? Vyjadřuje se jako vzdělaný člověk? Hodnotíme tyto aspekty a jistě ještě tucet dalších úplně podvědomě. Je to dojem, který získáváme během několika prvních okamžiků rozhovoru.

V práci od nás pořád někdo něco chce. Máš adresu tohoto člověka? Kde je poslední verze dopisu klientům? Kdo řeší tuto část projektu? Pošlete mi nejnovější verzi projektu. Potřebuji aktuální verzi zdrojového kódu.

Stává se, že lidi, kteří nás žádají o různé věci, neznáme osobně, protože to jsou osoby pracující v jiné organizační jednotce našeho podniku nebo se tak alespoň představují. Informace, které mají, navozují dojem že tito lidé jsou „zevnitř" („Marianna říkala...", „To je na serveru K-16...“, „verze 26 plánů nového produktu"). Rozšiřujeme na ně naše uzemí důvěry a bezstarostně jim dáváme, co požadují.

Můžeme mít samozřejmě jisté pochybnosti: „Na co potřebuje někdo z továrny v Dallasu plány nového produktu?" nebo „Není sdělování jména serveru, který používám, riskantní?". Zadáme tedy ještě jěště jednu nebo dvě otázky. Pokud

se odpovědi zdají být smysluplné a chování volajícího nevzbuzuje podezření, přestaneme se bránit a vracíme se k přirozenému sklonu důvěřovat spolupracovníkům a děláme (v rozumné míře) to, o co nás žádají.

Neměli bychom dojít k závěru, že předmětem útoku jsou pouze formy, které mají počítačové systémy dostupné zvenku. Vezměme si osobu odpovědnou za firemní korespondenci: „Mohla byste pro mě něco udělat a hodit tohle do firemní poštovní přihrádky?" Uvědomuje si osoba přebírající zásilku, že obsahuje disketu se speciálním programem pro sekretárku ředitele? Jakmile ho spustí, útočník dostane kopie šéfových e-mailů. Mohlo by se něco takového stát v naší firmě? Odpověd zní: samozřejmě

Poznámka Mitnicka
****
V lidské přirozenosti je myslet si, že během právě probíhající transakce síše nebude, ledaže bychom měli konkrétní důvody myslet si opak. Zvažujeme riziko a ve většině případů nakonec odhazujeme pochybnosti. To je přirozené chování civilizovaného člověka, či alespoň civilizovaného člověka, který nebyl nikdy podveden ani zmanipulován, nebo z něj nebylo vymámeno značné množství peněz.
Když isme byli malí, rodiče nás učili: „Nedůvěřuj neznámým lidem". Stálo by to se zase vrátit k tomuto starému pravidlu.
****

Mobil za jeden cent

Mnoho lidí se při nákupech pozorně rozhlíží, dokud nenajdou tu nejlepší nabídku. Sociotechnik nehledá jenom lepší nabídku, ale způsoby, které by ji ještě vylepšily. Občas firma vyhlašuje prodejní akci, která je tak atraktivní, že doslova nejde odolat. Sociotechnik se zamýšlí, jestli by se nedala nějakým způsobem ještě zatraktivnit.

Před nějakým časem jeden z mobilních operátorů uspořádal zaváděcí prodejní akci a nabízel nový mobilní telefon za jeden cent těm, kteří s nimi podepíší smlouvu na jeden z paušálních tarifů.

Mnoho lidí příliš pozdě zjistí, že existuje hodně otázek, které by si mel rozvážný zákazník položit, než podepíše smlouvu: je to služba analogová, digitální nebo hybridní, kolik je měsíčně minut zdarma, jestli jsou nějaké dodatečné poplatky za roaming apod. Zvlášť důležitá je doba trváni smlouvy, tedy počet měsíců či let, po který budeme muset platit paušál.

Představme si sociotechnika ve Filadelfii, kterého zaujala lákavá nabídka mobilního telefonu, ale nestál o tarifní program, který se s ní vázal. Žádný problém. Zde je jeden ze způsobů, jak si mohl poradit.

První rozhovor: Ted

Nejprve sociotechnik volá do obchodu s elektronikou na West Girard.

„Electron City, u telefonu Ted."

„Dobrý den, Tede. Tady Adam. Před několika dny jsem hovořil s prodavačem o mobilním telefonu. Řekl jsem mu, že se ozvu, až si vyberu nejaký tarifní program, ale zapomněl jsem, jak se jmenoval. Kdo u vás dělá na druhé směně?"

„Pokaždé někdo jiný, není to vždycky ta samá osoba. Možná William?"

„Nejsem si jist. Možná to byl William. Jak vypadá?"

„Vysoký chlápek, hodně hubený."

„Myslím, že to byl on. Jaké má příjmení?"

„Hadley. H-A-D-L-E-Y."

„Opravdu. Zní mi to povědomě. Kdy bych ho mohl zastihnout?“

„Nemám rozvrh služeb na tento týden, ale odpolední směna začíná v pět."

„Dobře. V tom případě se pokusím ho chytit dnes večer. Díky.“

Druhý rozhovor: Katie

Další telefon je do obchodu téhož řetězce na North Broad Street.

„Dobrý den, Electron City. U telefonu Katie. Co pro vás mohu udělat?"

„Ahoj Katie. Tady je William Hadley z prodejny na West Gira Jak se dneska máš?"

„Nestíhám. Co se stalo?"

„Mám zákazníka, který by chtěl ten mobil za jeden cent. Víš, o čem je řeč?"

„Jistě, minulý týden jsem prodala dva."

„A máte ještě nějaké ty přístroje, které jsou v té akci?"

„Celou hromadu."

„Skvělé, protože jsem právě jeden prodal zákazníkovi. Mám ověřenou jeho platební způsobilost a podepsali jsme s ním smlouvu. Potom jsem se podíval do skladu a ukázalo se, že ty aparáty došly. Trapas. Mohla bys pro mne něco udělat? Můžete mu prodat ten mobil za jeden cent a vystavit mu účet? Jak dostane telefon, tak by mi měl zavolat abych mu vysvětlil, jak se programuje."

„Jasně, pošli ho k nám."

„Dobrá. Jmenuje Todd. Todd Yancy."

Když se člověk představující se jako Todd Yancy objevil v prodejně na North Broad, Katie vystavila fakturu a prodala mu telefon za jeden cent, tak jak ji požádal její „spolupracovník". Spolkla návnadu.

Když přišel čas na placení, zákazník neměl v kapse drobné, hrábí tedy na tácek s centovými mincemi, co ležel u kasy, a vtiskl minci dívce za pultem. Obdržel tak telefon, aniž by za něj zaplatil alespoň ten jeden cent.

Teď může jít k jiné firmě, která používá stejný model telefonu a vybrat tarif, který by mu vyhovoval. Nejlépe takový se smlouvou na jeden měsíc.

Analýza podvodu

Lidé mají od přírody větší sklon akceptovat někoho, kdo se vydává za spolupracovníka a zná firemní zvyklosti a žargon. Sociotechnik, kterého jsme si ukázali v tomto příběhu, toho využívá. Pod záminkou zjišťování detailů o reklamní akci identifikuje pracovníka firmy a v jiné prodejně ieho jménem prosí o službu. Odehrává se to v různých pobočkách firmy, jejichž pracovníci spolu nejsou v osobním kontaktu, ale často zařizují záležitosti se spolupracovníky, které vůbec neznají.

Průnik do FBI

Lidé se moc často nezamýšlejí nad tím, jaké materiály jejich organizace zpřístupňuje na Internetu. Pro potřebu rozhlasového pořadu, který mám v KFI Talk Rádio v Los Angeles náš producent prohledal síť a našel kopii návodu k obsluze na přístup do databáze NCIC[8] Později našel návod na samotnou obsluhu rejstříku — důvěrný dokument, který obsahuje všechny procedury potřebné k získávání informací z databáze FBI.

Tento návod je příručkou pro pracovníky policejních složek, který udává příslušné kódy a formáty potřebné k získávám informací o zločincích a zločinech ze zmíněného rejstříku. Úřady z celé země mohou tuto databázi

[8] Pozn. překl.: Národní centrum informací o zločinech.

prohledávat při pátrání po informacích, které by jim pomohly ve vyšetřování. Příručka obsahuje číselníky použité v databázi na popis všeho možného, druhem tetování počínaje, přes typ lodního trupu, až po označení kradených peněz a cenných papírů.

Každý, kdo měl přístup k návodu, si mohl vyhledat příslušný sled příkazů umožňující výpis informací z databáze. Potom si mohl podle těchto procedur a při trošce pevných nervů stáhnout informace z rejstříku. Příručka uvádí rovněž telefonní čísla, kam je možné zavolat o pomoc při obsluze. Možná jsou ve vaší firmě zveřejněné podobné příručky s kódy produktů nebo s kódy dovolujícími přístup k důvěrným informacím.

Pracovníci FBI určitě nikdy neodhalili, že jejich důvěrné instrukce a postupy jsou přístupné na síti. Myslím, že by je to příliš nepotešilo. Jedna z kopií byla vydána jednou vládní institucí v Oregonu, druhá pak v Texasu. Proč se tak stalo? V každém případě si asi někdo pomyslel že tyto informace nejsou pro nikoho cizího užitečné a jejich zveřejnil nenapáchá žádné škody. Možná je někdo prosté dal na intranet pro pohodlí pracovníků, ale neuvědomil si, že zpřístupnil tyto informace všem, kteří mají přístup k dobrému vyhledávači, jako je například Google. Obyčejným zvědavcům, kandidátům na policisty, hackerům či členům skupin organizovaného zločinu.

Vstup do systému

Zásada využití takových informací k podvedení úředníka nebo zaměstnance firmy je pořád stejná. Poněvadž sociotechnik ví, jak se dostat do určitých databází či aplikací nebo zná čísla, názvy serveru a podobné, získává si důvěru.

Jakmile má sociotechnik takové kódy, je už poměrně jednoduché získat data, která potřebuje. V tomto konkrétním příkladu by mohl začít telefonátem do kanceláře, kde se nachází terminál a položit otázku týkající se jednoho kódu z příručky. Mohla by znít například takto: „Když píšu dotaz OFF v NCIC, ukazuje se mi chyba *systém nefunguje*. Mohl byste to zkusit napsat vy?" Mohl by také povědět, že se pokouší vyvolat *wpf* (v policejní hantýrce to je spis hledané osoby).

Úředník u počítače na druhém konci vidí, že volající je obeznámen s operačními procedurami a příkazy zadávanými databázi NCIC. A kdo jiný kromě vyškolených osob by mohl znát tyto postupy?

Když člověk obsluhující počítač potvrdí, že u něj všechno funguje, rozhovor by mohl pokračovat:

„Mohl byste mi pomoci?"

„A co potřebujete?"

„Musím zadat příkaz OFF na jméno Martin Reardon, datum narození 18.10.1966."

„Jaké je SOSH?"

Žargon
****
SOSH — zkratka označující v hantýrce FBI číslo sociálního pojištění.
****

„700-14-7435"

„Má 2602," mohl by odpovědět úředník po nalezení hledané osoby

Útočník teď musí pouze nahlédnout do příručky NCIC, aby našel význam této hodnoty. Ukázalo se, že tento člověk je obviněný z falšování svých osobních dokladů.

Analýza podvodu

Dobrý sociotechnik by při hledání cesty, jak proniknout do databáze NCIC, ani na chvilku nezaváhal. Ostatně proč by měl váhat, když získat potřebné informace vyžaduje pouze jeden telefonát na místní policejní služebnu a trochu plynulého hovoru, aby se představil jako člověk zevnitř. Příště zatelefonuje jinam a bude postupovat stejně.

Možná přemýšlíte, jestli není telefonování na policii nebezpečné. Neriskuje útočník příliš?

Odpověd zní: ne ... ze specifických důvodů. Policisté mají, podobně jako vojáci, od prvního dne pobytu v akademii naočkovaný respekt vůči hodnostem. Pokud se sociotechnik představuje jako seržant nebo poručík — prostě někdo vyšší než osoba, se kterou hovoří — oběť bude postupovat podle hluboko zakořeněné zásady, která říká, že se nepochybuje o tom, co tvrdí osoba vyšší šarže, která má nad nimi moc. Jmými slovy, hodnost dává privilegia a zejména jedno — nemožnost být kontrolován osobami níže v hierarchii.

Policejní a armádní instituce však nejsou jediná místa, kde může sociotechnik využít respekt před šarží. Sociotechnici často využívají autoritu vyplývající z pozice ve struktuře organizace jako zbraně při útoku na firmy — ukáže to několik historek popsaných v této knize.

> Poznámka Mitnicka
> **********
> Každý by si měl uvědomovat, jaký je sociotechnikúv modus operandi: sesbírej co nejvíce informací o objektu útoku a použij je se záměrem získat si důvěru, prezentuj se přitom jako osoba zevnitř. A pak udeř!
> **********

Prevence

Jaké kroky je možné podniknout ve vaší firmě, aby se snížila pravděpodobnost, že sociotechnik využije přirozený instinkt zaměstnanců důvěrovat jiným lidem? Zde je několik návrhů.

Ochrana zákazníků

V současnosti mnoho firem, které něco prodávají, uchovává mezi údaji o klientovi také data o jeho kreditní kartě. Existuje k tomu důvod: zákazník se osvobozuje od otravného poskytování údajů o své kartě při každém nákupu. Přesto bychom měli s touto praxí skoncovat.

Pokud už musíme uchovávat čísla kreditních karet, musí s tím být spojené bezpečnostní klauzule, které jdou dále, než je šifrování a kontrola přístupu. Pracovníci musejí byt proškoleni v rozeznávání sociotechniků jako jsou ti, kteří byli popsaní v této kapitole. Údajný spolupracovník se kterým jsme se nikdy osobně nesetkali, ale se kterým jsme se stačili přes telefon seznámit, může být stejně tak dobře někdo úplně jiný, než za koho se vydává. Možná vůbec nepotřebuje, aby se mu zpřístupňovala důvěrná data. Možná vůbec není zaměstnancem firmy.

Důvěřuj, ale prověřuj

Nejen lidé, kteří mají přístup k zjevně důvěrným datům, jako jsou programátoři či pracovníci vývojových oddělení, se musejí bránit proti vetřelcům. Skoro každý člen organizace by měl projít odpovídajícím bezpečnostním školením o průmyslové špionáži a zlodějích informací.

Základem k němu by měla být analýza podnikových dat se zvláštním zřetelem na každé z důvěrných, kritických či cenných dat spolu s kladením otázek, jaké metody by sociotechnik mohl použít, aby k nim získal přístup. Odpovídající školení zorganizované pro osoby, které mají přístup k těmto informacím, by mělo zohledňovat výše zmíněné problémy.

Když někdo, koho osobně neznáme, žádá nějaké informace či materiály nebo prosí o vykonání nějaké činnosti na počítači, musí si pracovníci položit několik otázek. Kdyby ty informace obdržel náš úhlavní nepřítel, mohly by ublížit mně nebo mé firmě? Opravdu plně chápu příkazy, které mám na základě prosby zadat do počítače?

Nejde o to, abychom každou novou osobu považovali za podezřelou. Čím jsme však důvěřivější, tím více riskujeme, že nás sociotechnik podvede a získá přístup k chráněným firemním datům.

Kam až dosahuje náš intranet?

Část vnitřní firemní počítačové sítě může být zpřístupněna uživatelům zvenku a část jen pracovníkům firmy. Jak často a důsledně naše firma kontroluje, jestli důvěrné informace nejsou umístěné na místech potenciálně přístupných lidem, před kterými je třeba je chránit? Kdy naposled někdo z firmy kontroloval, jestli nějaké důvěrné informace z intranetu nebyly neúmyslně umístěné v oblastech přístupných vnějším uživatelům?

Jestliže naše naše firma používá proxy servery jako prostředky ochrany před útoky zvenku, tak kdy byla naposledy zkontrolována správnost jejich konfigurace?

A možná bychom se měli zeptat, jestli jsme si vůbec někdy dali tu práci a zkontrolovali zabezpečení našeho firemního intranetu?

5

Mohu vám nějak pomoci?

Všichni pociťujeme vděk, když nám někdo, kdo něco ví, umí a je zkušený, nabídne pomoc při řešení našeho problému. Sociotechnik si to uvědomuje a ví, jak tuto skutečnost využít.

Ví také, jak vyvolat problém a následně získat naši vděčnost za jeho vyřešení. Potom s námi může manipulovat, aby se dostal k informacím nebo aby poprosil o drobnou službičku, v jejímž důsledku poneseme my nebo naše firma ztráty. Není vyloučeno, že si ani nebudeme uvědomovat, že jsme o něco cenného přišli.

Zde jsou typické příklady toho, jak sociotechnici „pomáhají".

Síť nám spadla

Čas: pondělí 12. února, 15.25
Místo: kanceláře loděnic Starboard

První rozhovor: Tom DeLay

"Tom DeLay, účtárna."

„Ahoj Tome, tady Eddie Martin z technického oddělení. Musíme odstranit problém se sítí. Neměl někdo z vaší skupiny v poslední době problémy s výpadky sítě?"

"O ničem nevím."

"A ty sám jsi neměl žádné problémy?"

„Ne, všechno se zdá v pořádku."

„To je dobře. Víš, voláme lidem, kterým mohou nastat problémy, protože nám záleží na tom, aby nám dali vědět, kdyby jim spadla síť"

„To nezní moc optimisticky. Myslíš, že se něco takového opravdu může stát?"

„My doufáme, že ne, ale kdyby se ti něco takového stalo, tak zavolej, jo?"

„Radši bych, aby se nic nestalo."

„Zdá se, že ztráta spojení by pro tebe byl problém..."

„Samozřejmě."

„V tom případě ti dám na sebe mobil, abys mě mohl chytit, kdyby se něco stalo."

„Skvělé, píšu si."

„555-867-5309."

„555-867-5309, mám. A vůbec díky za varování. Řekni mi ještě jednou, jakže se jmenuješ?"

„Eddie. Ještě jedna věc. Musím si ověřit, na který port je připojený tvůj počítač. Mohl by ses podívat? Měla by tam někde být nálepka, kde se píše ‚číslo portu'."

„Okamžik... ne, nic takového tu nevidím."

„Dobrá, v tom případě najdi u počítače zezadu síťový kabel."

„Mám."

„Koukni se, kam vede a jestli je tam nějaká nálepka nad zásuvkou ve zdi."

„Tak chvilku počkej. Jo, moment... musím se tam sehnout, abych to přečetl. Píše se tam 6 pomlčka 47."

„Souhlasí, mám tě poznamenaného u tohoto portu, ale chtěl jsem se ujistit."

Druhý rozhovor: informatik

O dva dny později zvoní telefon v centru správy sítě.

„Ahoj, tady Bob. Jsem právě v kanceláři Torna DeLaye z účtárny Máme tu problém s kabely. Mohl bys na chvíli deaktivovat zásuvku 6-47?"

Informatik odpověděl, že to během několika minut udělá a aby mu dali vědět, až bude moci zásuvku opět zapojit.

Třetí rozhovor: pomocná ruka vetřelce

Když o hodinu později byl člověk, který se představoval se jako Eddie Martin, na nákupech v Circuit City, zazvonil mu mobil. Než hovor přijal, vyhledal si nějaké tišší místo. „Servis, tady Eddie."

„Ahoj Eddie. Teda máš tam ale ozvěnu! Kde jsi?"

„Jsem v rozvodné skříni s kabely. Kdo volá?"

„Tom DeLay. Ještě štěstí, že mám na tebe číslo. Vzpomínáš si, jak jsi mí posledně volal? Spadlo mi spojem se sítí, jak jsi mne varoval, a ted trochu panikařím."

„Ano, spadlo to u více lidí. Měli bychom to do večera spravit. Stačí to?"

„Ne! Jestli budu tak dlouho bez spojení, jsem v háji. Nedalo by se to nějak urychlit?"

„Jak moc spěcháš?"

„Chvíli mohu dělat něco jiného. Ale za půl hodiny bych to opravdu potřeboval."

„Půl hodiny?! To bude těžké... No dobrá, přeruším teď, co mám rozdělané, a podívám se, jestli by se to dalo nějak zařídit."

„Budu ti, Eddie, opravdu vděčný."

Čtvrtý rozhovor: Mám tě!

O tři čtvrtě hodiny později...

„Tom? Tady Eddie. Zkus síť."

Po chvilce...

„Hurá! Funguje. Bezva!"

„To je dobře. Jsem rád, že jsem ti mohl pomoci."

„Moc ti děkuji."

„Poslyš, jestli chceš mít jistotu, že ti nebude padat spojení, mám jeden takový prográmek, který by sis měl spustit. Nepotrvá to dlouho."

„Ted zrovna na to není ten nejlepší čas."

„Chápu... ale příště by nám to mohlo ušetřit hodně problémů."

„No dobře, jestli je to opravdu jen několik minut.“

„Takže ted musíš udělat..."

Edie provedl Toma jednotlivými kroky instalace jedné malé aplikace z Internetu. Po stáhnutí programu řekl Eddie Tomovi, aby ho spustil. Tom udělal, co mu bylo řečeno, a ohlásil:

„Nefunguje. Nic se neděje."

„Asi je tam něco divného. No nic, odinstalujeme ho a zkusíme to někdy jindy."

Eddie po telefonu provedl Toma přes odinstalaci programu.

Čas trvání operace: 12 minut.

Verze útočníka

Bobbyho Wallacea vždycky pobavilo, když se klient po zadání vyhýbal vysvětlení, k čemu konkrétní informaci potřebuje. V tomto případě ho napadaly jen dva možné důvody. Buďto klient zastupoval nějakou skupinu, která se zajímala o koupi firmy Starboard Shipbuilding a chtěl se seznámit se skutečným finančním stavem podniku — zejména pak s těmi daty, která by firma chtěla potenciálním kupcům zatajit. Anen zastupoval investory, kterým byl podezřelý způsob finančního řízení a chtěli zjistit, jestli někdo z managementu nedefrauduje peníze firmy. A možná klient nechtěl uvést pravý důvod zakázky, poněvadž kdybv Bob zjistil, jak cenná je hledaná informace, požadoval by za svou více peněz.

* * *

Existuje mnoho způsobů, jak získat i ta nejlépe střežená firemní data. Bobby strávil několik dní přemýšlením, jakou metodu zvolit, a zvažováním různých možností před konečným rozhodnutím. Nakonec si vybral metodu vyžadující takový uskok, který měl obzvláště rád: zmanipulováni oběti tak, aby se sama na něho obrátila s prosbou o pomoc.

Nejprve si Bobby koupil v obchodě 7-Eleven mobil za 39,95 $. zavolal osobě, kterou si vyhlédl jako obět a představil se jako firemní technik a následně si připravil situaci tak, aby mu ten člověk zavolal na jeho mobil, když se objeví nějaký problém s počítačovou sítí.

Pak počkal dva dny, aby to vypadalo přirozeněji, a zavolal na správu sítě té firmy. Prohlásil, že odstraňuje Tomovi nějaký problém, a poprosil o odpojení jeho zásuvky. Bobby věděl, že toto byla nejobtížnější částce akce — v mnoha firmách technici úzce spolupracují se správou sítě, nebo jsou přímo součástí oddělení informatiky. Ukázalo se však, že informatik vzal ten telefonát rutinně a aniž by se zeptal na příjmení technika, akceptoval jeho požadavek na deaktivaci portu. Jakmile ho odpojil, byl Tom odříznut od vnitřní sítě firmy, byl zbaven možnosti stahovat si souboryn ze serveru, výměny souborů s kolegy, čtení pošty a dokonce i tisku dokumentů. V dnešním světě to znamená skoro návrat do jeskyně.

Zanedlouho, jak Bobby očekával, zazvonil telefon. Samozřejmě byl ochotný pomoci kolegovi odstřihnutému od světa. Zavolal na správu sítě a požádal o opětovnou aktivaci zásuvky své oběti. Posléze znovu zavolal Tomovi a opět ho zmanipuloval tak, aby se cítil provinile, kdyžBobbymu odmítl službičku. Nakonec Tom ještě jednou zvážil Bobbyho návrh a souhlasil se zkopírováním programu na svůj počítač.

Samozřejmě si neuvědomoval, čím vlastně doopravdy souhlasil. Program, který měl předcházet výpadkům spojení, byl ve skutečnosti *trojským koněm* - aplikací, která zafungovala na Tomově počítači stejně jako mýtický *trojský kůň* — vpustila nepřítele do města. Tom po spuštení programu neviděl, že by se něco dělo. Ona totiž ta aplikace byla napsána tak, že navenek nic neukazovala, ani tehdy, když instalovala skrytý program umožňující špehovi skrytý přístup k počítači.

> *Žargon*
> *****************
> **Trojský kůň** — program obsahující kód, který ničí napadený počítač či soubory nebo umožňuje přístup k informacím na počítači oběti či v lokální síti Některé trojské koně se skrývají v operačním systému a zaznamenávají stisk každé klávesy nebo činnost pracovníka. Jiné samy něco vykonávají. Uživatel si neuvědomuje, že má takový program v systému.
> *****************

Po spuštění programu získal Bobby plnou kontrolu nad Tomovým počítačem. Přes vzdálené terminálové okno mohl prohlížet a kopírovat účetní data. Potom

mohl beze spěchu analyzovat zkopírované soubory a hledat informace, které jeho zaměstnavatelé požadovali.

Žargon
****
Vzdálené terminálové okno — textové rozhraní, přes které je možné zadávat příkazy vykonávající jisté funkce nebo spouštět programy. Útočník, který využívá bezpečnostní díry v systému nebo je schopný nainstalovat trojského koně na počítač oběti, může též získat tento vzdáleny přístup k příkazovému řádku.
****

A to není všechno. Kdykoliv se mohl vrátit, aby si přečetl poštu a soukromé poznámky vedení firmy a hledat klíčová slova, která by ho mohla dovéest k zajímavým informacím.

Bobby ještě téhož večera, kdy přesvědčil svou oběť, aby si nainstalovala trojského koně, vyhodil mobil na smetiště. Samozřejmě předtím vymazal paměť telefonu a vytáhl z něho baterie — poslední věc, kterou by si přál bylo, aby někdo omylem vytočil číslo a mobil začal vyzvánět.

Analýza podvodu

Útočník obkličkuje oběť, přesvědču)e ji že má problém, který vlastně neexistuje nebo, jak° v tomto případě, informuje o problému, který ještě nenastal, ale vyskytne se v nejbližší budoucnosti (o to už se útočník postará). Potom se útočník představuje jako člověk, který muže problém vyřešit.

Úskok tohoto typu je pro útočníka obzvláště vhodný, protože základ byl připraven dříve a oběť — jakmile zjistí, že začínají nějaké potíže - sama zavolá útočníkovi a žádá o pomoc. Pachatel prostě čeká na telefón — tato taktika je známá jako *obrácená sociotechnika*. Útočník, který je schopný přesvědčit oběť, aby mu zavolala, získává okamžitou důveru: když oběť telefonuje někomu, o kom si myslí, že je technik, určitě i nebude klást otázky, které by ověřovaly jeho totožnost. Útočník si ji stihl vytvořit.

Žargon
****
Obrácená sociotechnika — sociotechnický útok, kdy útočící vytváří situaci, ve které si oběť všimne nějakého problému a kontaktuje útočníka se žá-sP dosti o pomoc. Jiná forma obrácené sodotechniky spočívá v obrácení rolí. Obéť zjistí, že byla napadena a využívajíc psychologických znalostí působí na atakujícího, snaží se z něho vytáhnout co nejvíce informací zaj účelem ochrany firmy.
****

Při použití lsti tohoto druhu se sociotechnik snaží vybrat za oběť osobu, která se v počítačích moc nevyzná. Čím více toho oběť ví, tím je pravděpodobnější, že začne něco tušit nebo se prostě zorientuje, že je manipulována. Pracovník, kterému činí obsluha počítače potíže, který nezná ani pokyny ani zásady, se bude snáze podvolovat vůli útočníka. Taková osoba se dá snáze oklamat lstí typu: „Mohl by sis stál tento malý prográmek?", protože nemá ponětí o případných škodách, jaké by mohl takový prográmek způsobit. Ba co víc, je mnohem menší pravděpodobnost, že si uvědomuje hodnotu informací, které se nalézají ve firemní síti, a riziko spojené s jejich zpřístupněním.

Poznámka Mitnicka
****

Jestliže ti někdo cizí prokáže službu a posléze o službu prosí tebe, neodvděčuj se, aniž se zamyslíš nad tím, o co jsi vlastně byl požádán.
****

Pomáháme novým zaměstnancům

Noví zaměstnanci jsou ideálním cílem útoku. Neznají ještě hodně svých spolupracovníků, neznají platné pokyny a zásady. Pro vyvolání dobrého prvního dojmu ochotně ukazují svoji vůli spolupracovat, jakož i rychlost.

Nápomocná Andrea

„Osobní oddělení, Andrea Calhoun."
"Ahoj Andreo, tady Alex z bezpečnostního."
„Ano?"
„Jak se máš?"
„Dobře. Jak ti mohu pomoci?“
„Hele, připravujeme program školení z oblasti bezpečnosti pro nové pracovníky a musíme shromáždit pár lidí, abychom ho vyzkoušeli, potřeboval bych jména a telefonní čísla všech nově přijatých osob. Mohla bys mi pomoci?"
„Dobře, ale až po obědě. Stačí to? Jakou máš linku?"
„Jistěže stačí. Linka 52... hm, ale dnes mám v podstatě celý den různá jednání. Zavolám ti, až se vrátím do kanceláře, pravděpodobně okolo čtvrté."
Když Alex zavolal přibližně v 16.30, Andrea už seznam měla a přečetla mu jména s telefonními linkami.

Zpráva pro Rosemary

Rosemary Morgan byla svou novou prací nadšená. Nikdy předtím nepracovala v časopise a lidé tady byli mnohem příjemnější, než očekávala. Bylo to překvapující vzhledem ke stresu, ve kterém pracují, aby dodrželi každoměsíční termín vydání dalšího čísla. Telefon, který měla jednoho čtvrtečního rána, ji v tomto přesvědčení utvrdil.
„Mohl bych mluvit s Rosemary Morgan?"
„U telefonu."
„Ahoj Rosemary. Tady Bill Jorday z oddělení ochrany informací."
„Ano?"
„Probíral už někdo s tebou bezpečnostní pravidla?"
„Ani ne."
„Dobrá. Tak tedy: Za prvé nikdo nesmí instalovat programy přinesené jinud. To proto, že nechceme přijímat odpovědnost za používání nelicencovaného softwaru a také se tím vyhýbáme problémům s viry."
„Rozumím."
„Slyšela jsi o našich pokynech týkajících se elektronické pošty?"
„Ne."
„Jakou máš adresu?"
„*Rosemary@ttrzine.net*“
„Přistupuješ na své konto přes uživatelské jméno 'Rosemary'?"
„Ne. R_Morgan.“
„Dobře. Chceme připomenout všem novým zaměstnancům, že otevírání neočekávaných příloh je nebezpečné. Posílá se mnoho viru a dostávají se k nám ve zprávách od známých osob. Proto jestli dostány zprávu s přílohou, kterou jsi nečekala, měla bys vždycky zkontrolovat, jestli ti ji odesílatel skutečně poslal. Je to jasné?"

„Ano, slyšela jsem o tom."

„Dobře. Doporučujeme také změnu hesla každých 90 dní. Kdy sis naposledy měnila heslo?"

„Pracuji tu teprve tři týdny a po celou dobu mám to, co jsem si dala na začátku."

„V pořádku. Můžeš počkat, až uplyne zbytek z těch 90 dní. Musíme se také ujistit, jestli si lidé nastavují hesla, která nejde snadno uhodnout Máš heslo, které obsahuje písmena i číslice?"

„Ne."

„V tom případě to musíme napravit. Jaké je tvé současné heslo?"

„Je to jméno mé dcerky – Annette."

„To není bezpečné heslo. Nikdy by sis neměla dávat heslo, které má něco společného s údaji týkajícími se tebe nebo členů tvé rodiny. Co s tím uděláme... Mohla bys třeba dělat to co já. Můžeš používat své současné heslo jako první část a potom vždy, když ho měníš, dodávat číslo aktuálního měsíce."

„A když si ho změním ted, měla bych dát 3 nebo 03?"

„To záleží na tobě. Která varianta je pro tebe pohodlnější?"

"Myslím, že Annette3."

„Dobře. Mám tě provést přes změnu hesla?"

„Ne, to už umím."

„Výborně. Ještě jedna věc, o které si musíme promluvit. Na tvém počítači je nainstalován antivirový program a důležitá je jeho aktualizace: Nikdy bys neměla vypínat automatickou aktualizaci, ani když se tvůj počítač občas zpomalí, ano?"

„Jasně."

„Velmi dobře. Máš na nás telefon, abys mohla zavolat, kdyby se něco stalo s počítačem?"

Neměla. Volající jí dal číslo, které si pečlivě zapsala a vrátila se k práci znovu potěšená, jak si jí tu považují.

Analýza podvodu

V tomto příběhu bych chtěl znovu upozornit čtenáře na záležitost, která se vine celou knížkou. Nejtypičtější informace, které bude chtít sociotechnik od pracovníka nezávisle na konečném cíli útoku získat, jsou jeho identifikační údaje. Když má uživatelské jméno a heslo jednoho jednoho z pracovníků vyhlédnutého oddělení, má útočník k dispozici základní prvek, který mu může pomoci dostat se do systému a najít požadovanou informaci. Držení těchto údajů je jako držení klíčů od hradních bran. Díky nim se lze svobodně pohybovat uvnitř a najít hledaný poklad.

Poznámka Mitnicka
****
Předtím, než se novým pracovníkům firmy umožní jakýkoliv přístup do vstému, musejí být proškoleni z oblasti bezpečnosti. Zvláštní důraz je třeba dát na to, aby nikdy neprozrazovali svá hesla.
****

Ne tak bezpečné, jak by se mohlo zdát

Firma, která nevynakládá žádné úsilí, aby svá citlivá data zabezpečila, je lehkomyslná firma. Ale dokonce i ty firmy, které se snaží svá důvěrná data chránit, jsou vystaveny vážnému nebezpečí.

Zde je příběh, který ještě jednou ilustruje, jak management firmy obelhává sám sebe, když se domnívá, že zavedené bezpečnostní postupy vytvořené kompetentními a zkušenými odborníky se nedají obejít.

Příběh Steva Cramera

Trávník nebyl velký. Určitě nepatřil k těm drahým a příliš rozlehlým, které až vzbuzují závist. Zcela jistě nebyl tak velký, aby si jeho vlastník mohl obhájit nákup automatické sekačky. Ostatně i tak by ji Steve nevyužíval. Rád sekal trávu elektrickou kosou, protože námaha s tím spojená mu dávala pohodlnou výmluvu, která mu dovolovala soustředit se na vlastní myšlenky a neposlouchat Annu, která vyprávěla historky o lidech z banky, kde pracovala nebo mu vymýšlela různé úkoly. Nenáviděl ty její věčné seznamy „Miláčku, udělej:", které se staly nedílnou součástí jeho víkendů. Hlavou mu prolétla myšlenka, že jeho dvanáctiletý syn Pete měl geniální nápad, když se zapsal do plaveckého oddílu. Teď mohl být každou sobotu na srazech či trénincích, což ho uvolňovalo od sobotních domácích povinností.

Nekomu by se mohlo zdát, že jeho práce spočívající v navrhování nových přístrojů pro firmu GeminiMed byla nudná. Steve si však uvědomoval, že zachraňuje lidské životy. Pokládal svou práci za tvůrčí. Umělci, hudebníci, skladatelé a inženýři — ti všichni se podle Steva ocitali před podobnou výzvou jako on: vytvářeli něco, co nikdo jiný nimi. Nejnovější dítě — objevný, nekonvenční projekt umělé srdce chlopně — bylo jeho největším úspěchem a důvodem k hrdosti.

Byla neděle, blížila se půl dvanáctá, Steve byl podrážděný, protože končil s trávníkem a nijak nepostoupil ve vymýšlení způsobu redukce energetické náročnosti chlopně, poslední překážky v projektu, kterou í třeba překonat. Ideální téma na přemýšlení během kosení, ale řešení nepřišlo.

* * *

Ve dveřích se objevila Anna s vlasy zavinutými do pruhovaného červeného šálu, který nosila vždy, když luxovala.

„Telefon," zavolala na něj. „Někdo z práce."

„Kdo?" zeptal se Steve.

„Nějaký Ralph. Snad."

Ralph? Steve si nevzpomínal na nikoho z GeminiMed, kdo by se jmenoval Ralph a měl by mu volat o víkendu. Zřejmě se Anna přeslechla,

„Steve, u telefonu Ramon Perez z technického oddělení."

Ramon? Jakým zázrakem se podařilo Anně zaměnit španělské jméno za Ralpha, zamýšlel se Steve.

„Mám malé upozornění," říkal Ramon. „Tři servery přestaly pracovat, možná je napadl virus. Budeme muset vymazat disky a obnovit data ze zálohy. Jestli půjde všechno podle plánu, mělo by se nám povést vaše data vrátit někdy ve středu, ve čtvrtek."

„To je absolutně nepřijatelné," odpověděl tvrdě Steve. Snažil se nepropadnout frustraci. Copak jsou tak neschopní? Copak si doopravdy mysli že si poradí bez přístupu ke svým souborům po celý víkend a většinu příštího týdne? „O tom nemůže být řeč. Za dvě hodiny si chci doma sednout k počítači a budu potřebovat své soubory. Mluvím jasně?"

„Což o to. Všichni, kterým jsem dosud volal, chtějí byt první v poradí. Nestačí, že jsem musel přijít o víkendu do práce, abych to opravil ale ještě se každý, komu telefonuju, zlobí na mě."

„Mám napjatý termín, firma čeká na můj projekt. Musím to udělat dnes odpoledne. Copak je na tom něco nepochopitelného?"

„Musím ještě obvolat spoustu lidí, než vůbec začnu něco dělat" řekl Ramon. „A co kdybych obnovil ty vaše soubory v úterý?"

„Žádné úterý, žádné pondělí, ale dnes! Hned ted!" naléhal Steve a přemýšlel, komu zatelefonuje, jestli se mu nepodaří toho chlapi přivolat k rozumu.

„No dobrá, dobrá," odvětil Ramon a Steve uslyšel jeho rezignovaní povzdechnutí. „Uvidíme, co se dá dělat. Vy používáte server RM22, že?“

„RM22 i GM16. Oba používám."

„Dobrá. Mohl bych jít trochu zkratkou, abychom ušetřili čas. A v tom případe bych potřeboval uživatelské jméno a heslo.“

Hmm, pomyslel si Steve. *Co to na mne hraje? Na co potřebuje moje heslo? Proč se mne hlavní správce ptá na takové věci?*

„Mohl byste mi ještě jednou říci vaše jméno? A pod koho patříte?"

„Ramon Perez. Heledte, když jste byl přijat do práce, dostal jste vyplnit formulář, abychom vám založili konto a musel jste tam napsat také heslo. Mohu teď ten formulář najít a ukázat, že ho tu máme, jo?"

Steve o tom chvilku přemýšlel a posléze souhlasil. Čekal s rostoucí netrpělivostí, zatímco Ramon odešel vytáhnout ze skříně kartu. Konečně se vrátil k telefonu. Steve slyšel, jak se prohrabuje stohem papírů.

„Už to mám," řekl nakonec Ramon. „Napsal jste tu heslo Janice."

Janice, pomyslel si Steve. To bylo jméno jeho matky a skutečně je občas používal jako heslo. Možná, že je uvedl jako heslo při vyplňování toho formuláře.

„Souhlasí," potvrdil.

„To je dobře, protože takhle jen ztrácíme čas. Ted už snad věříte, že opravdu existuji. Vy chcete, abych to zkrátil a vaše soubory obnovil okamžitě, tak mi s tím, prosím, pomozte."

„Moje uživatelské jméno je s-podtržítko-cramer. Heslo je pelicanl."

„Hned se dám do práce" pověděl Ramon, který se konečně zdál ochotnější pomoci. „Dejte mi pár hodin."

Steve dokončil trávník, poobědval a když se posadil k počítači, ukázalo se, že všechny jeho soubory jsou na svém místě. Byl sám se sebou spokojen, že donutil neochotného správce pomoci a doufal, že Anna slyšela, jak dovede být asertivní. Pomyslel si, že by bylo dobré dát informatikovi či jeho Šéfovi pochvalu, ale věděl, že to je jedna z těch věcí, ke kterým se nikdy nedokáže přimět.

Příběh Craiga Cogburnea

Craig Cogburne byl obchodním zástupcem firmy prodávající vyspělé technologie a vykonával svou práci dobře. Brzy si začal uvědomovat svou dovednost „přečíst" klienta, rozpoznat jeho slabé i silné stránky a nesouhlas dané osoby, zkrátka záležitosti, jejichž znalost usnadňuje uzavření transakce. Začal tedy přemýšlet o jiných způsobech využití svého talentu a to ho přivedlo k lukrativnějšímu zaměstnání — k průmyslové špionáži.

* * *

Zákazka by atraktivní, nezdálo se, že by mi zabrala hodně času a za honorář by bylo možné si zaplatit výlet na Havaj či Tahiti.

Člověk, který si mne najal, neprozradil, kdo je ve skutečnosti mým klientem, ale vypadalo to, že je to firma, která touží dohonit konkurenci pomocí jednoho velkého skoku vpřed. Já měl za úkol pouze získat projekty a specifikace nového produktu nazvaného „umělá srdeční chlopeň“ ať už to znamená cokoliv. Firma se nazývala GeminiMed. Nikdy jsem o ní neslyšel, ale byla velká, s pobočkami v šesti různých místech - což činilo můj úkol snazší než v případě nějaké menší firmy, kde existuje velká pravděpodobnost, že osoba, se kterou mluvíme, zná člověka, kterého hrajeme a zorientuje se, že my nejsme on. Může nám to, jak říkají piloti o vzdušné kolizi, zkazit náladu na celý den.

Člověk, co si mne najal, mi poslal fax s výstřižkem z nějakého lékařského časopisu, kde se psalo o tom, že GeminiMed pracuje na umělé chlopni převratné konstrukce, která se bude nazývat STH-100. Ukázalo se, že nějaký reportér už stihl vykonat část práce za mě. Měl jsem už jednu z věcí, které musím mít, než začnu jednat — jméno onoho nového produktu.

Prvním problémem bylo získat jména lidí ve firmě, kteří na STH-100 pracují nebo mají potřebu prohlížet konstrukční plány. Zatelefonoval jsem na firemní ústřednu a řekl jsem: „Slíbil jsem, že se spojím s jistým člověkem z vaší inženýrské skupiny, ale zapomněl jsem, jak se jmenuje. Pamatuji si jen, že jeho křestní jméno začínalo na S."

„Máme tu Scotta Archera a Sama Davidsona," odpověděla.

Zkusil jsem jít přímo na věc: „Který z nich pracuje ve skupině STH-100?"

Nevěděla. Tak jsem si vybral Scotta Archera jako prvního v pořadí a byl jsem na něj přepojen. Když zvedl sluchátko, pověděl jsem:

„Ahoj, tady Mike z podatelny. Máme tu kurýrní zásilku adresovanou na skupinu pracující na umělé srdeční chlopni STH-100. Nevíš, komu to předat?" Věděl a sdělil mi jméno šéfa projektu Jerryho Mendela. Přiměl jsem ho také k tomu, aby mi sdělil jeho číslo telefonu.

Zavolal jsem tam. Mendel tam nebyl, ale zpráva v hlasové schránce informovala, že je do třináctého na dovolené, což znamená, že ještě přes týden si bude lyžovat a odpočívat a každý, kdo mu něco chce, má zavolat Michelle na číslo 9137. Jak jsou ti lidé někdy nápomocní!

Tak jsem zavolal Michelle. Když to zvedla, povídám:

„Tady Bill Thomas. Jerry mi říkal, že vám mám zavolat, až budu mít specifikace, které mají zkontrolovat lidé z jeho skupiny. Vy také patříte k té skupině, co dělá na umělé chlopni, že?"

Michelle přitakala.

Ted přišel čas na nejtěžší taneční figuru. Kdybych vycítil v jejím hlase odezíravost, byl jsem připraven vysvětlovat, že se pouze snažím Jerryimu prokázat službu, o kterou mne poprosil.

„Na jakém systému pracujete?" zeptal jsem se.

„Systému?"

„Jaký používáte servery?" Aha," pochopila, „RM22. A část týmu je také na GM16."

Podařilo se! To jsem vlastně potřeboval a byla to informace, kterou jsem získal, aniž bych vzbuzoval přílišné podezření. To mi připravilo půdu pro následující dotaz, který jsem se snažil položit co nejpřirozeněji.

„Jerry říkal, že byste mi mohla dát seznam e-mailových adres členů výzkumného týmu," řekl jsem a zatajil dech.

„Samozřejmě. Rozesilací seznam je ale moc dlouhý na to, abych ho tady četla do telefonu. Mohla bych vám to poslat mailem?"

Stop! Každá mailová adresa, která se nekončí na geminimed.com, by mohla spustit poplach.

„A mohla byste mi to nafaxovat?" zeptal jsem se.

Neviděla v tom žádný problém.

„Náš fax je nyní v opravě. Musím zjistit číslo druhého. Za chvilku znovu zavolám," pověděl jsem a položil sluchátko.

Mohlo by se zdát, že mám jistý problém. Ale jeho řešení bylo velmi jednoduché. Chvilku jsem počkal, aby můj hlas nebyl povědomý recepční, vytočil jsem číslo a řekl:

„Ahoj, tady Bill Thomas. Náš fax začal stávkovat, mohl bych přijmout fax na vašem přístroji?"

Odpověděla, že to není žádný problém a dala mi číslo.

A pak jsem si tam šel vyzvednout ten fax, že? Ani náhodou. Pravidlo číslo jedna: nikdy osobně nenavštěvuj sídlo firmy, pokud to není bezpodmínečně nutné. Není jednoduché identifikovat někoho, kdo je pro vás jenom hlasem v telefonu. A jestli tě nemohou identifikovat, nemohou tě ani zavřít. Je těžké nasadit želízka hlasu v telefonu. Zavolal jsem tedy za chvilku znovu do recepce a zeptal jsem se, jestli přišel můj fax.

„Ano."

„Mám prosbu," řekl jsem. „Musím to poslat našemu konzultantovi. Mohla bys to poslat místo mně?"

Souhlasila. Ostatně proč by neměla souhlasit. Těžko očekávat od každé recepční schopnost rozeznávat důvěrná data. Během doby, kdy vysílala fax „konzultantovi", jsem si mohl protáhnout kosti procházkou do místního obchůdku, na kterém se skvěl nápis: „Faxy — posílání/přijímání". Očekával jsem, že můj fax tam dorazí přede mnou. Což se také stalo. Když jsem vstoupil do obchodu, už tam na mne čekal. Šest strán po 1,75 $ každá. Za jednu desetidolarovou bankovku a trochu drobných jsem měl v rukou seznam e-mailů všech členů výzkumného týmu.

Průnik

Zatím jsem v průběhu několika hodin mluvil se třemi nebo čtyřmi li a dostal jsem se o velký kus dopředu směrem k dosažení přístupu k firemním počítačům. Potřeboval jsem však ještě několik informací.

Nejprve telefonní číslo pro přístup k serveru zvenku. Znovu jsem zavolal na GeminiMed, požádal jsem recepční o spojení s oddělením informatiky a poprosil člověka, který tam ten telefon zvedl, aby spojil s někým, kdo mi může pomoci s počítačovým problémem. Přepojil mne a já jsem začal hrát zmatenou a v technických záležitostech nepříliš talentovanou osobu.

„Jsem doma, právě jsem si přinesl nový notebook a potřeboval bych ho nastavit tak, abych se mohl připojovat zvenku."

Konfigurace byla jednoduchá, ale trpělivě jsem ho nechal, aby mne provedl konfigurací, abych obdržel vytoužené číslo. Informatik mi sdělil, jako by to byla další běžná informace. Poprosil jsem ho, aby ještě počkal, než vyzkouším, jestli to funguje. Fungovalo.

Překonal jsem další překážku a mohl jsem se připojit k síti. Zkusil jsem to a objevil jsem, že jejich terminál dovoluje spojit se se všemi počítači sítě. Po několika pokusech jsem narazil na něčí počítač, na kterém bylo založeno konto pro hosty zkonfigurované tak, že nebylo nutné přihlašování psát heslo. Některé operační systémy vyžadují po uživateli po instalaci vytvoření uživatelského jména a hesla, ale zároveň vytvářejí konto pro hosty. Uživatel by měl nastavit tomuto účtu zvláštní heslo nebo účet úplně deaktivovat, ale většina lidí se s tím vůbec nenamáhá nebo dokonce ani netuší, že nějaké takové konto vůbec existuje. Ta byl zřejmě čerstvě nainstalovaný systém a uživatel ještě nestačil konto pro hosty znepřístupnit.[9]

Díky tomuto účtu jsem měl nyní přístup k jednomu z počítačů, který, jak se ukázalo, běžel pod starší verzí operačního systému UNIX. V tomto systému je umístěn soubor, který obsahuje zašifrovaná hesla vá uživatelů, kteří zde mají konto.[10] Všechna hesla jsou jednosměrně *hašována*[11], výsledek není možné dekódovat do původního tvaru. Po jednosměrném hašování je skutečné heslo uloženo v zašifrované formě. V tomto případě je překonvertované na řetězec třinácti alfanumerických znaků.

Žargon

[9] Pozn. překl.: Takový účet se zpravidla jmenuje guest. Zkuste se naschvál v práci přihlásit na konto guest, podařilo se?

[10] Pozn. překl.: Tento soubor se jmenuje /etc/passwd, nové verze už uchovává hesla odděleně v souboru /etc/shadow — ještě na to přijde řeč v jiné kapitole

[11] Pozn překl.: Hašovat je ryze české slovo stvořené z anglického *to hash*, stejne jako jiná česká slova: mailovat, surfovat, zipovat. Na jednom semináři jsem slyšel tento zázrak: *Z tohoto fajlu vyselektujeme příslušné rekordy a vyprintujeme je na monitor.* Nemusím snad dodávat, že přednášející byl rodilý Čech.

****
Hašování hesla — proces, v jehož důsledku je heslo překódováno do nesrozumitelného tvaru. Tento proces je už z principu nevratný. Jinými slovy: předpokládá se, že rekonstrukce hesla je po hašování nemožná.
****

Když někdo chce nahrát soubory do počítače, musí se identifikovat tím, že zadá uživatelské jméno a heslo. Systémový program, který ověřuje přístup, šifruje heslo a porovnává výsledek[12] s tím, co má ve svém seznamu uživatelů a hesel. Jestliže jsou oba řetězce stejné, uživatel je vpuštěn.

Protože hesla v souboru jsou zašifrovaná, je samotný soubor přístupný pro kohokoliv v souladu s přesvědčením, že nikdo nedokáže hesla v něm obsažená rozlousknout. Směšné! Stáhl jsem si soubor a pustil na něj slovník (o této metodě si můžete přečíst ve 12. kapitole), abych se přesvědčil, že jeden z členů výzkumného týmu, Steve Cramer, měl konto s heslem „Janice". Zkusil jsem napsat jeho uživatelské jméno a heslo na jeden z badatelských serverů. Kdyby to zafungovalo, ušetřil bych si trochu času i rizika. Bohužel, nepodařilo se.

Znamenalo to, že musím toho Člověka nějak obelstít, aby mi prozradil své uživatelské jméno a heslo. Rozhodl jsem se s tím počkat na víkend.

Zbytek už znáte. V sobotu jsem zavolal Cramerovi a pověděl jsem mu historku o zavirovaných serverech a nezbytnosti obnovy dat ze záložních kopií, abych v něm zahnal případné pochybnosti.

A ta pohádka, že vyplňoval heslo na jednom z formulářů, když byl přijímán do práce? Prostě jsem počítal s tím, že si nebude pamatovat, že nic takového nebylo. Nově přijatý pracovník vyplňuje tolik formulářů, že je po letech těžké si připomenout každou rubriku. Kdyby se mi to nepovedlo, pořád jsem měl dlouhý seznam dalších jmen.

Když jsem znal jeho uživatelské jméno a heslo, dostal jsem se na server, trochu jsem to tam prošmejdil a brzy jsem nalezl soubory s projektem STH-100. Nebyl jsem si jist, které z nich jsou klíčové, tak jsem raději přetáhl všechny do mrtvé schránky - bezplatné ftp[13] konto v Číně, kde mohly být uložené, aniž by vzbuzovaly nějaké podezření. Nyní musel můj klient mezi soubory najít informace, které pro něj byly zajímavé.

Žargon
****
Mrtvá schránka — místo pro uložení informací, pro jiné obtížně nalezitel- j né. Ve světě tradičních špionů to mohla být uvolněná cihla ve zdi; ve světě hackerů je to obvykle internetová adresa v nějaké vzdálené zemi.
****

Analýza podvodu

Pro člověka, kterého nazýváme Craig Cogburne, nebo pro kohokoliv obeznámeného s uměním sociotechniky, je zde popsané jednání téměř rutinní. Cílem byla lokalizace a získání souborů umístěných na firemním počítači chráněném firewallem a jinými zabezpečovacími systémy.

[12] Pozn překl.: Pro ten výsledek šifrování jsem navrhoval slovo šifrát, ale jazyková korektorka mi vyhrožovala ublížením na zdraví.

[13] Pozn. překl.: FTP — Filé Transfer Protocol, způsob přenášení souboru mezi naším a vzdáleným počítačem oběma směry. Zkrátka náš sociotechnik nemusel s těmi disketami jet do Číny osobně, stejně jako později jeho klient.

Většina jeho úkolů byla jednoduchá jako chytání dešťové vody do sudu. Nejprve Craig předstíral, že je z podatelny a tím, že hovořil o kurýrní zásilce, dodal věci nádech urgence. Tento podvod ho přivedl ke jménu šéfa skupiny pracující na projektu umělé srdeční chlopně, který byl sice na dovolené, ale — zajisté kvůli pohodlí zlodějů informací — zanechal na záznamníku jméno a telefonní číslo na Michelle. Během rozhovoru s Michelle rozehnal veškeré pochybnosti, když se uvedl tím, že se snaží vyhovět prosbě šéfa týmu. Jelikož byl šéf na dovolené, Michelle neměla možnost ověřit si jeho tvrzení. Uvěřila mu a bez problémů souhlasila se zpřístupněním důležité a cenné informace — seznamu e-mailových adres členů týmu.

Nenabyla podezření ani tehdy, když ji Craig poprosil, aby mu seznam poslala faxem místo elektronickou poštou, což je způsob, který je obvyklé pro obě strany pohodlnější. Proč byla tak naivní? Protože by se šéf po návratu z dovolené mohl dozvědět, že jeho podřízení někomu ztěžovažovali splnění jím zadaného úkolu. Kromě toho volající řekl, že šéf nejenže podporuje jeho prosbu, ale dokonce ho žádal o pomoc. Další příklad osoby, která se chce prezentovat jako dobrý spolupracovník a kvůli tomu se stává snadným cílem útoku.

Craig se vyhnul riziku spojenému s osobní návštěvou v budově firmy tím, že zařídil, aby byl fax zaslán na recepci, věděl, že ta bude nápomocná. Konečně jako recepční jsou přijímány osoby šarmantní a dělající dobrý dojem. Drobné službičky jako poslání či přijetí faxu je pro recepční věc samozřejmá, čehož Craig ihned využil. To, co obsahoval fax, mohlo vyvolat poplach u každého, kdo znal hodnotu této informace, ale od recepční není možné vyžadovat schopnost rozeznávat důvěrné informace od těch běžných.

Pak Craig využil jiného způsobu manipulace — hrál zmateného a nezkušeného uživatele, aby získal od informatika přístupové telefonní Číslo na firemní terminálový server — zařízení spojující všechny počítačové systémy ve vnitřní síti.

Craig se snadno připojil k síti, když vyzkoušel defaultní hesla některých účtů, která nebyla nikdy změněna. Je to jedna z evidentních děr, které existují v mnoha vnitřních sítích, které se spoléhají na ochranu firewallem. Defaultní hesla mnoha operačních systémů, routerů a podobných zařízení včetně pobočkových ústředen jsou všeobecně dostupná. Každý sociotechnik, hacker, průmyslový špion nebo jen obyčejný zvědavec může jejich seznam najít na adrese *http://www.phenoelit.de/dpl/dpl.html* . (Je až neuvěřitelné, jak Internet usnadňuje život těm, kteří vědí, kde hledat. Ted už i *ty* víš, kde hledat.)

Cogburnovi se následně podařilo přesvědčit opatrného a podezíravého pracovníka („Mohl byste mi ještě jednou říci vaše jméno? A pod koho patříte?"), aby mu prozradil své uživatelské jméno a heslo na server, který používal výzkumný tymi pracující na projektu umělé srdeční chlopně. Tak otevřel Craigovi dveře a umožnil mu prohlížet si nejpřísněji chráněná tajemství firmy a zkopírovat plány nejnovějšího firemního produktu.

A co kdyby Steve Cramer získal v souvislosti s Craigovým telefonátem nějaké podezření? Je málo pravděpodobné, že by o něm někoho informoval před pondělním příchodem do práce, kdy už by bylo příliš pozdě útoku zabránit.

A zde je klíčový prvek posledního podvodu: Craig ze začátku neprojevoval žádný zájem o Stevovy problémy. Potom otočil a vykazoval ochotu pomoci, aby Steve mohl dokončit práci. Ve většině případů, kdy oběť věří, že se ji pokoušíme pomoci, bude náchylná se s námi podělit o důvěrné informace, které by jinak střežila jako oko v hlavě.

Poznámka Mitnicka
****
V zaměstnání je pro každého nejdůležitější dokončit rozdělanou práci. Pod tímto tlakem jsou věci spojené s bezpečností odsunuty na vedlejší kolej a jsou opomíjeny nebo ignorovány. Sociotechnici toho dokáží využít.
****

Prevence

Jedním z nejúčinnějších sociotechnických triků je obrácení situací. Viděli jsme to v této kapitole. Sociotechnik vytváří problém a následně ho zázračně řeší, přičemž vyláká od oběti informace o přístupu k nejbedlivěji střeženým firemním tajemstvím. Dala by se takto ošálit vaše firma? Dali jste si tu práci a popsali a zavedli jste odpovídající bezpečnostní pravidla, která by dovolila se těmto problémům vyhnout?

Učit se, učit se, učit se

Možná znáte ten starý vtip o turistovi v New Yorku, který zastavil ulici chodce s dotazem: „Jak se mohu dostat do Carnegie Hall?" Oslovenj kolemjdoucí odpovídá: „Cvičit, cvičit a cvičit". Každý je potenciálně vystaven nebezpečí sociotechnického útoku, proto jedinou možnou ochranou firmy jsou příslušná školení a vzdělávání pracovníku, které učí rozpoznávat sociotechniky. Potom je nutné neustále připomínat věci, které se na školení naučili a které se nejčastěji zapomínají.

Každý člen organizace musí být proškolen tak, aby si vypracoval příslušný stupeň podezíravosti a opatrnosti nezbytný během jednání s lidmi, které osobně nezná. Zejména tehdy, jestliže ho někdo žádá o informace o nějaké formě přístupu k počítači či síti. Lidská nátura ná přikazuje jiným důvěřovat, ale jak říkají Japonci, byznys je válka. Ví firma si nemůže dovolit polevit v ochraně. Bezpečnostní politika firmy musí definovat patřičné a nepatřičné chování.

Zásady bezpečnosti nejsou univerzální. Osazenstvo firmy má obvykle různé úkoly a s každou pozicí v práci se váže jiné nebezpečí. Měla by existovat jistá základní úroveň školení a pak musejí lidé projít školením odpovídajícím jejich druhu práce a plněných povinností, což umožní snížit pravděpodobnost výskytu problémů. Lidé, kteří prac s citlivými údaji na speciálních pozicích s vysokým stupněm důvěry, by měli projít dalším speciálním školením.

Zabezpečení důvěrných informací

Když cizí člověk nabízí pomoc, tak jako jsme to viděli v příbězích této kapitoly, musejí mít zaměstnanci firmy na paměti pravidla bezpečnost která jsou šitá na míru potřebám, velikosti a zvyklostem vaši firmy.

Nikdy nepomáhejte cizím lidem, kteří vás žádají o vyhledání nějakých informací, o zadání nějakých neznámých příkazů do počítače, o změny v nastavení vašich aplikací nebo (což je nejnebezpečnější varianta) o otevírání příloh elektronické pošty a stahování neověřených programů. Žádný program — dokonce ani takový, který zdánlivě nic nedělá — nemusí být tak nevinný, jak vypadá.

Jsou věci, se kterými si bez ohledu na kvalitu školení přestaneme dělat starosti. A v kritickém okamžiku potom nevíme, jak správně zareagovat. Mohlo by se zdát, že pravidlo neposkytování svého uživatelského jména a hesla je pro všechny samozřejmé (nebo by to alespoň mělo být samozřejmé) a není důvod se o tom zmiňovat, protože to je otázka zdravého rozumu. Ve skutečnosti je nutné často připomínat, že zpřístupňování uživatelského jména a hesla ke svému počítači v kanceláři či doma je srovnatelné s prozrazením PIN kreditní karty.

Vzácně se může stát, že sdělení nějaké důvěrné informace někomu je opravdu nutné. Z tohoto důvodu není vhodné vytvářet absolutní pravidla typu „nikdy".

Nicméně však bezpečnostní politika a procedury by měly jasně vymezovat okolnosti, za kterých může pracovník sdělit své heslo a — což je nejdůležitější — kdo je oprávněný se na takové údaje ptát.

Poznámka Mitnicka
****
Osobně se domnívám, že firmy by neměly dovolovat žádnou možnost sdílení hesel. Je mnohem jednodušší ustavit jednoznačné pravidlo, které zakazuje personálu jakékoliv sdílení nebo výměnu hesel. Je to také bezpečnější. (Ale každá firma si musí určit svou vlastní kulturu a bezpečnostní zájmy.)
****

Kdo se ptá?

Ve většině organizací by mělo platit pravidlo, že každá informace, jejíž zpřístupnění by mohlo uškodit firmě nebo jejímu pracovníkovi, může být sdělena pouze známým osobám, jejichž hlas zní natolik povědomě, že nejsou žádné pochybnosti o jejich totožnosti.

Ve věcech vysokého stupně důvěrnosti by měly být akceptovány pouze dotazy vznesené osobně nebo pomocí silné formy ověření — například dvou nezávislých zabezpečení, jako je třeba společné tajemství a časově závislý identifikátor.

Procedury klasifikace dat musejí obsahovat to, že žádná informace z té části organizace, která se zabývá důvěrnými projekty, nemůže být poskytnuta neznámé osobě nebo osobě, za kterou se nikdo nezaručil.

Poznámka
****
Je to téměř k nevíře, ale dokonce ani nalezení jména a telefonního čísla volajícího ve firemní databázi zaměstnanců a zpětné zavolání nedává žádné záruky — sociotechnici znají cesty, jak vložit nějaké jméno na seznam pracovníků a jak přesměrovat telefonní hovory.
****

Jak tedy odpovědět na prosbu spolupracovníka, která se zdá odůvodněná a týká se například seznamu pracovníků našeho odboru a jejich elektronických adres? Jak zvýšit povědomí, že informace tohoto typu, která má výrazně menší význam než například specifikace nového robku, je určena výhradně k vnitřnímu použití? Ve velké míře by tu mohlo pomoci určení osob v každém odboru, které se budou zabývat žádostmi o sdělování informací mimo příslušný odbor. Tyto osoby měly projít pokročilým školením týkajícím se bezpečnosti, které by je seznamovalo s ověřovacími procedurami, kterých by se měly držet.

Nezapomeň na nikoho

Je snadné určit ty části organizace, které vyžadují vysoký stupeň ochrany před útoky. Často však zanedbáváme jiné, méně samozřejmé leč velmi zranitelné oblasti. V jednom příběhu se prosba o vyslání faxu na vnitřní telefonní číslo zdála nevinná, a přece se tu útočníkovi pod využít díru v bezpečnostním systému. Vyplývá z toho následující zavěr: každý, sekretářkou počínaje a vedením konče, potřebuje speciální kurs z oblasti bezpečnosti, aby u něj podobné pokusy spouštěly mentální poplašný signál. Nesmíme zapomínat na obranu „první linie": recepční bývají často prvním cílem sociotechnického útoku a je vhodné seznámit je s tím, jaké postupy používají někteří hosté nebo volající.

Bezpečnostní systém firmy by měl stanovovat kontaktní bod pro pracovníky, kteří mají podezření, že se stali cílem sociotechnického útoku. Jednoznačné místo ohlašování incidentu spojených s bezpečností firmy zaručuje efektivní systém včasné ochrany, který umožní odhalit organizovaný útok a uvědomit si ihned eventuální ztráty.

6

Mohli byste mi pomoci?

Už víme, jak sociotechnici podvádějí lidi, když jim nabízejí pomoc. Jiný často používaný trik obrací role: sociotechnik manipuluje s lidmi tím, že předstírá, že od nich sám pomoc potřebuje. Všichni dokážeme soucítit s lidmi, kteří se ocitli v tísni, proto tento přístup umožňuje sociotechnikovi krůček po krůčku dosáhnout cíle.

Příchozí

Jedna z historek uvedených ve třetí kapitole ukazuje, jakým způsobem může útočník přesvědčit oběť, aby mu prozradila své zaměstnanecké číslo. V následujícím příkladu je stejného výsledku dosaženo jinou metodou. Navíc je tu popsáno, jak lze informaci získanou tímto způsobem využít.

Určitě existuje nějaký Jones

V Křemíkovém údolí (Sillicon Valley) měla své sídlo jistá mezinárodní firma - její jméno zde taktně přejdeme mlčením — jejíž pobočky, rozseté po celém světě, byly propojené s ústředím přes WAN (rozsáhlá síť). Vetřelec, chytrý a mazaný chlápek Brian Atterby — si uvědomoval,že téměř vždy je snazší se nabourat do sítě v nějaké vzdálenější lokalitě, kde ochrana určitě nebude tak přísná jako v centrále.

Zavolal tedy do chicagské pobočky a poprosil o spojení s panem Jonesem. Recepční se zeptala, jestli ví, jaké je křestní jméno pana Jonese. Odpověděl:

„Někde ho tu mám, právě ho hledám. Kolik máte lidí s příjmením Jones?"

„Tři," odpověděla. „Ve kterém oddělení by měl pracovat?"

„Kdybyste mi přečetla jejich jména, možná bych si vzpomněl" navrhl Brian.

Vyhověla mu:

„Barry, Joseph a Gordon."

„Joe. Myslím, že je to on," zareagoval. „Ze kterého je oddělení?"

„Z oddělení rozvoje."

„Výborně. Mohla byste mne s ním spojit?"

Recepční přepojila hovor. Když se ozval Jones, útočník zahájil:

„Pan Jones? Dobrý den, tady Tony ze mzdového. Jak jste žádal, převedli jsme vaši výplatu na konto u Credit Union."

„Cože?! To si snad děláte srandu! O nic takového jsem nežádal! A u Credit Union ani konto nemám!"

„Do háje! Ale já už jsem tam ty peníze poslal!"

Jones, rozčilený, že jeho výplata byla převedena na účet někoho cizí se už chystal člověku na druhém konci vynadat, ale než stačil cokoliv říci, protějšek se ozval:

„Musíme si rychle vyjasnit, jak se to vlastně stalo. Ten podnět byl podaný pod číslem pracovníka. Jaké je vaše zaměstnanecké číslo?"

Jones mu ho sdělil.

„Skutečně, máte pravdu. Ta žádost nebyla od vás."

Blbnou čím dál tím víc — pomyslel si Jones.

„Pohlídám, aby se to vyřešilo. Hned zařídím nápravu, nedělejte obavy. Výplata se vám brzy vrátí na vaše konto," ujišťoval nepravý Tony.

Poznámka Mitnicka
****

Nemysli si, že zabezpečení sítě a firewally ochrání tvá data. Hledej nejslabší článek. Obvykle jím bývá člověk.
****

Na služební cestě

Zanedlouho poté zvonil telefon u systémového správce ve firemní pobočce v Austinu, stát Texas.

„Tady Joe Jones," prohlásil člověk na druhém konci. „Volám z ústředí z oddělení rozvoje. Budu na týden u vás ve městě, v hotelu DriSkill. Chtěl bvch vás poprosit o založení dočasného konta, abych měl přístup v poště bez volání meziměsta."

„Řekněte mi ještě jednou vaše jméno a číslo" odpověděl systémák. Falešný Jones uvedl číslo a pokračoval:

„Máte čísla na vysokorychlostní modemy?"

„Momentíček, kamaráde, napřed si vás musím najít v databázi." Po chvíli dodal: „Dobrá, Joe, povězte mi ještě číslo vaší budovy?"

Útočník dělal domácí úkoly a tak měl odpověd připravenou.

„Dobrá," řekl správce sítě, „přesvědčil jste mne." Jak prosté! Systémák si ověřil jméno Joseph Jones, oddělení a číslo zaměstnance a „Joe" poskytl správnou odpověd na kontrolní otázku.

„Váš login bude stejný jako ve firmě: ‚jbjones'," oznámil mu správce. „Nastavuji vám počáteční heslo ‚zmen_mne'."

Analýza podvodu

Několik telefonátů a patnáct minut stačilo, aby vetřelec získal přístup do podnikové sítě WAN. Byla to jedna z mnoha firem, jejichž ochrana připomíná lentilky, podle popisu uvedeného poprvé výzkumníky z Bellových laboratoří Stevem Bellovinem a Stevenem Cheswickem. Popsali takový druh zabezpečení jako „tvrdou skořápku s měkkým vnitřkem". Vnější skořápka, firewall, podle nich jako zabezpečení nestačí, protože v okamžiku, kdy skrz ni útočník pronikne, má už vnitřní počítačový systém zabezpečení slabé a není patřičně chráněný.

Popsaný příběh odpovídá definici *lentilkového zabezpečení*. S připojovacím číslem a kontem se útočník nemusel zabývat problémem, jak překonat firewall. A když už se jednou dostal dovnitř, průzkum celého systému již byl jednoduchý.

Žargon
****
Lentilkové zabezpečení — termín vytvořený Bellovinem a Cheswickem z Bellových laboratoří. Popisuje systém zabezpečení, kde vnější bariéra, např. firewall, je silná, kdežto vnitřní infrastruktura nemá žádnou ochranu. Označení vzniklo přirovnáním tohoto systému k lentilkám, které mají tvrdou skořápku a měkkou náplň.[14]
****

Podle mých informací byl uskok tohoto druhu proveden proti jednomu z největších výrobců počítačových programů. Člověk by si představoval, že systémoví správci v takových firmách budou školení, aby podobné útoky odhalili. S největší pravděpodobností se to však opravdu takto stalo a firma dodnes neví, jakým způsobem někdo získal přístup do jejich sítě.

[14] Pozn překl: Pánové Bellovin a Cheswick žili v Americe a tak své pravidlo nazvali *candy security*, tedy bonbónové zabezpečení, a jako vzor si vzali bonbóny M&M. My však máme naše lentilky.

Možná P. T. Barnum nikdy neřekl, že „každou minutu se rodí ne prosťáček", ale ať už to řekl kdokoliv, výstižně popsal případ pracovníka firmy, kterého sociotechnik se svým darem výmluvnosti oklamal.

Zabezpečení z časů prohibice

V době prohibice existovaly nelegální noční kluby, kde gin tekl proudem. Klient mohl vejít dovnitř a stačilo k tomu pouze přijít ke dveřím a zaklepat. Po chvíli se otevřelo malé okénko a ukázala se v něm hrozivá tvář vyhazovače. Jestliže byl host zasvěcen, vyslovil jméno některého ze štamgastů („Posílá mne sem Joe" — to někdy úplně stačilo). Tehdy vrátný otevíral dveře a vpouštěl příchozího dovnitř.

Trik byl v tom, že se musely znát ty správné dveře, muselo se vědět, kde se nachází to doupě. Dveře byly neoznačené a vlastníci se nijak zvlášť nesnažili usnadňovat cestu rozvěšováním neonových reklam ukazujících směr. Ve většině případů prostě stačilo objevit se na pravém místě, aby nám otevřeli dveře. Bohužel, stejný druh zabezpečení je často používán v obchodním světě, který se tak vrací do časů prohibice.

Žargon
****
Zabezpečení z času prohibice — toto zabezpečení se spoléhá na to, že je nutné znát místa, kde jsou umístěny informace a zároveň je nutné znát slovo nebo jméno, které umožňuje přístup do tohoto místa v počítačovém systému.
****

„Tři dny kondora"

Jako ilustrace může posloužit vynikající film, který si mnoho lidí pamatuje. Ve Třech dnech kondora je hlavní hrdina — Turner, kterého hraje Robert Redford — zaměstnán v malé firmě, která pracuje pro CIA. Jednoho dne si odskočí na svačinu a po návratu zjistí, že všichni jeho spolupracovníci byli zastřeleni. Zůstal sám a chce se dozvědět, kdo a proč udělal zároveň si však uvědomuje, že ať už jsou zabijáci kdokoliv, nyní pátrají po něm.

Později se ve filmu podaří Turnerovi získat telefonní číslo jednoho pachatelů. Kdo to je a jak se Turnerovi podařilo vypátrat místo jeho pobytu? Měl štěstí: scénárista David Rayfiel ho „vybavil" minulostí ohreakera, který znal technologie a zavedené postupy telekomunikačních firem.

S telefonním číslem vraha v rukou ví Turner dokonale, co udělat. Ve scénáři je ta scéna rozepsána takto:

TURNER SE ZNOVU PŘIPOJUJE A VYŤUKÁVÁ DALŠÍ ČÍSLO.

Tút...Tút...

ŽENSKÝ HLAS (ze sluchátka): Kancelář CNA, u telefonu Coleman.

TURNER DO SLUCHÁTKA: Tady je Harold Thomas ze zákaznického servisu. Prosím CNA pro 202 555-7389.

ŽENSKÝ HLAS (ze sluchátka): Moment, prosím (po chvíli) Leonard Atwood, 765 MacKensie Lane, Cheve Chase, Maryland.

Co se tu vlastně odehrálo, kromě toho, že scénárista omylem použil směrové číslo Washingtonu D.C. pro adresy ze státu Maryland?

Turner jako vyškolený telekomunikační montážní pracovník věděl, jaké vytočit číslo, aby se spojil s kanceláří CNA, která má rejstřík jmen a adres abonentů a poskytuje je v případě nutnosti montážním pracovníkům a dalším oprávněným zaměstnancům firmy. Technik mohl zavolat do CNA, uvést číslo telefonu a požádat o jméno a adresu osoby, které číslo patřilo.

Jak oklamat telekomunikace?

Ve skutečnosti bylo číslo do CNA bedlivě střeženým tajemstvím. Dnes už se firmy dokázaly poučit a nejsou už tak štědré při udílení informací, ale v tehdejších časech u nich fungovala „bezpečnostní opatření z časů prohibice". Ta předpokládala, že každý, kdo se dovolal do kanceláře CNA a používal správný žargon („Zákaznický servis, prosím CNA pro 555-1234" nebo něco v tom stylu), tak byl oprávněnou osobou, aby dostal požadovanou informaci. Nebylo třeba se identifikovat, ověřovat totožnost, sdělovat číslo pracovníka nebo se ohlašovat nějakým každodenně měněným heslem. Jestli známe číslo, kam je třeba zavolat a náš hlas zní přesvědčivě, jsme oprávněni získávat informace.

Pro ty firmy to nebyl ten nejšťastnější předpoklad. Jediným bezpečnostním opatřením, které její pracovníci používali, byla periodická změna telefonního čísla, přinejmenšim jednou za rok. Avšak i tehdy bylo aktuální číslo velmi rozšířené mezi mladými phreakery, kteří s radostí čerpali informace z tak pohodlného zdroje a ochotně se o ně dělili s ostatními kolegy. Trik s kanceláří CNA byl jednou z prvních věcí které jsem se jako teenager při uvedení do kruhů phreakingu naučil. Ve světě obchodu a politiky je tento druh zabezpečení stále častý. Obvykle si muže každý středně zkušený vetřelec hrát na autorizovovnou osobu, když si předem nasbírá trochu informací o struktuře, personálu a žargonu firmy. Občas si vystačíme prostě jen se znalostí čísla vnitřní telefonní linky.

Poznámka Mitnicka
****
Zabezpečení z časů prohibice nijak nezabrání sociotechnickým útokům. Každý počítačový systém na světě má alespoň jednoho operátora. Jestliže útočník dokáže manipulovat lidmi, kteří obsluhují systém, omezený rozsah znalostí pro něj nepředstavuje žádnou překážku.
****

Bezstarostný ředitel výpočetního centra

Přestože si mnoho členů organizace neuvědomuje problémy bezpečnosti a ani se o ně nezajímá, od někoho, kdo zastává funkci ředitele výpočetního centra v jedné z větších organizací by se dala očekávat základní znalost těch nejlepších bezpečnostních metod, že?

Těžko předpokládat, že šéf výpočetního centra, osoba, která je pracovníkem odboru informačních technologií, se stane obětí jednoduché sociotechnické hříčky. Zvláště, když útočníkem je postpubertální mladík, skoro ještě děcko.

Hledání frekvence

Před léty bylo pro mnoho lidí zábavou vyladění rádia na frekvenci místní policie nebo hasičů a poslouchání vzrušujících rozhovořil o probíhajících bankovních přepadeních, hořící budově nebo vývoje událostí během automobilové honičky. Tyto frekvence bylo možné najít knihách dostupných v blízkých knihkupectvích. Dnes je možné je získat na Internetu i v knize, kterou lze koupit v obchodní síti Rádio Shack. Nacházejí se tam frekvence, na kterých vysílají úřady místní, okresní, státní a v některých případech i federální.

Samozřejmě neposlouchali jen zvědavci. Lupiči rabující obchod uprostřed noci mohli poslouchat, jestli do jejich blízkosti nebyla vyslána nějaká radiohlídka. Drogoví dealeři mohli sledovat činnost místních protidrogových úřadů. Pyroman mohl poslouchánim hasičů bojujících s požárem zvětšit svou chorobnou radost ze žhářství.

V posledních letech se s rozvojem počítačových technologií umožnilo šifrovat hlasovou komunikaci. Jak se vědcům dařilo nalézat způsoby jak vtěsnat cím dál tím větší výpočetní sílu do jednoho malého čipu, mohly se začít vyrábět malé radiostanice s možností šifrování znemožňujícího zločincům odposlouchávání.

Všetečný Danny

V devadesátých letech se odposlouchávací nadšenec a zkušený hacker — nazývejme ho Danny — rozhodl zkusit získat zdrojový kód programu od výrobce „bezpečných" radiostanic. Doufal, že po prostudování kódu najde způsob, jak odposlouchávat služby a dokonce možná použije tuto technologii, aby znemožnil i těm nejmocnějším vládním úřadům odposlouchávání jeho rozhovorů s přáteli.

Takoví jako Danny patřili v temném světě hackerů do zvláštní kategorie, která se nachází někde mezi poměrně neškodnými na jedné straně a nebezpečnými zločinci na straně druhé. Mají znalosti expertů spojené s nezkrotnou touhou boření zdí a barikád. Nabourávají se však pouze z důvodu uspokojení. Utočí na internetové stránky výlučně kvůli zábavě, vzrušení a aby ukázali, že to dokáží. Nic nekradou, nevydělávají si svou činností peníze. Neničí soubory ani síťové spojení a neboří počítačové systémy. Samotné nabourání se a přístup k souborům a e-mailům za zády správců sítě ponižuje lidi odpovědné za udržování si hackerů od těla. Vlastně právě to ponížení správců představuje pro hackery to největší uspokojení.

S tímto postojem si chtěl Danny prohlédnout projekt nejbedlivěji střeženého produktu firmy, který měl na mušce, aby uspokojil svou touhu a měl možnost obdivovat poslední inovace vložené do projektu.

Není třeba zvlášť připomínat, že plány výrobku byly přísně chráněným obchodním tajemstvím, cenným majetkem firmy. Danny si to uvědomoval, ale ani trochu si s tím nedělal starosti. Ostatně to byla jedna z těch velkých bezejmenných korporací.

Jak v takovém případě získat zdrojový kód programu? Jak se ukázalo,krádež korunních klenotů týmu Secure Communications Group byla neobyčejně jednoduchá, dokonce i přesto, že firma byla jednou z těch, které používali praxi *dvojitého ověřování*. Je to takové řešení, kde jsou pracovníci povinni používat dvou forem ověřování totožnosti.

> *Žargon*
> **********
> **Dvojité ověřování** — použití dvou různých forem autentikace k ověří totožnosti. Například osoba se může identifikovat telefonátem z určité konkrétního místa a uvedením hesla.
> **********

Zde je příklad z jiné oblasti, který pomůže trochu ukázat postup: když dostáváme novou kreditní kartu, banka nás žádá o telefonát potvrzující, že jsme ji obdrželi a že se nedostala do rukou někoho, kdo například ukradl obálku s kartou z poštovní schránky. Připojené instrukce vyžadují uskutečnění hovoru z domova. Když voláme, počítačový program v bance analyzuje ANI, automatickou identifikaci čísla (automatic number identification), které probíhá na bezplatné lince, za jejíž používání platí banka.

Program porovnává údaje z ANI čísla, ze kterého voláme, s číslem, které jsme v bance uvedli spolu se svými osobními údaji. Když pracovník banky přijímá hovor, vidí na obrazovce informace z databáze týkající se zákazníka,

který volá z tohoto čísla. Tak úředník pozná, že klient volá z domova. Je to první forma autentikace.

Následně si úředník vybírá některou ze zobrazených informací o klientovi — nejčastěji je to číslo sociálního pojištění, datum narození nebo dívčí jméno matky — a ptá se klienta na tuto informaci. Správná odpověd na tuto otázku je druhá forma autentikace založená na údajích, které by měl klient znát.

V naší firmě vyrábějící bezpečné vysílačky měl každý pracovník normální uživatelské jméno a heslo a ještě navíc dostával malé elektronické zařízení nazývané token. Existují dva typy takových zařízení: ten první je velký asi jako polovina kreditní karty, ale trochu silnější a druhý je tak malý, že je možné ho připnout ke svazku klíčů. Tento čudlík ze světa kryptografie má malé okénko, kde se zobrazuje šestimístné číslo. Každou minutu se obsah displeje mění na jiné šestimístné číslo. Když se oprávněná osoba pokouší vstoupit do počítačové síte zvenku, musí se nejprve představit jako autorizovaný uživatel a napsat tajné PIN a číslice zobrazené na tokenu. Po ověření vnitřní sítí musí ještě uvést své uživatelské jméno a heslo.

Aby mladý hacker Danny dostal do rukou tolik vytoužený zdrojový kód, musel získat nejen login[15] a heslo některého z pracovníků, což není pro zkušeného sociotechnika nic obtížného, ale zároveň musel obejít časově závislý kód.

Překonaní bariéry dvojité autentikace, tedy bezpečné identifikace spojené s tajným číslem PIN, je výzva hodná hrdinů filmu *Mission Impossible*. Sociotechnikovi však tato výzva připomíná spíše jednání pokerového hráče, který i při špatné kartě díky své neobyčejné schopnosti číst z chování jiných lidí dokáže odejít od hracího stolku se značnou částí peněz svých protihráčů v kapse.

Útok na pevnost

Danny začal domácími úkoly. Brzy sesbíral tolik informací, že se mohl převtělit za pracovníka firmy. Znal jméno pracovníka, oddělení, telefonní i zaměstnanecké číslo a také jméno a telefon jeho šéfa.

Nastal klid před bouří. A to doslova. Podle vymyšleného plánu potřeboval nyní Danny ještě jednu věc, než vykoná další krok, a to bylo něco, na co neměl pražádný vliv. Potřeboval sněhovou bouři. Čekal na trochu pomoci od matičky přírody — konkrétně na tak špatné počasí, které by znemožnilo pracovníkům příjezd do práce.

Během zimy v Jižní Dakotě, kde měla sídlo jmenovaná firma, nikdo, kdo doufá ve špatné počasí, nemusí čekat příliš dlouho. V pátek v noci přišla bouře. Sníh rychle přešel v mrznoucí déšť a do rána se silnice proměnily v kluziště.

Zavolal do firmy a poprosil o spojení s nějakým informatikem. Člověk, který vzal telefon, se představil jako Roger Kowalski.

Danny se představil jako existující pracovník, o němž si předem nashromáždil informace:

„Tady je Bob Billings. Pracuji v Secure Communications Group. Jsem ted doma a nemohu přijet kvůli té strašné bouři. Problém je v tom, ze se musím přilogovat na server, ale token jsem si zapomněl na stole v kanceláři. Mohl byste tam, prosím, skočit a přinést ho nebo tam pro něj někoho poslat? A potom přečíst kód, až se budu chtít přihlásit? Naš tým má šibeniční termín a nedokázal bych včas dokončit svou práci. Nemohu přijet, protože silnice jsou nesjízdné."

„Nemohu opustit výpočetní centrum," odpověděl informatik.

Danny rychle zareagoval: „A vy byste neměl svůj identifikátor?"

„Máme jeden ve výpočetním centru pro operátory pro případ nouze," řekl.

„Heleďte, mám velkou prosbu. Mohl bych využít ten váš identifikátor, když se budu hlásit na server? Dokud neposypou silnice."

[15] Pozn. překl.: Slovo login se používá jako synonymum k pojmu uživatelské jméno

"Jakže se jmenujete?" zeptal se Kowalski.
"Bob Billings."
"A Pod kým pracujete?"
„Ed Trenton je můj šéf."
„Aha, toho znám."
Jestliže se dají očekávat potíže, dobrý sociotechnik si nashromáždí o mnoho více informací než obyčejně.
„Pracuji na druhém patře," pokračoval Danny. „Vedle Roye Tuckera.“
Informatik znal i toto jméno. Danny pokračoval v náporu: „Možná by bylo snazší dojít do mé kanceláře a přinést můj identifikátor."
Danny si byl poměrně jist, že Kowalski se k tomu nedá přemluvit. Jednak by neopustil své místo uprostřed směny, aby se někde potloukal po vzdálených chodbách budovy, a kromě toho neměl příliš chuť hrabat se v cizím stole. Bylo možné se vsadit, že to neudělá.
Kowalski nechtěl říci „ne" člověku, který potřebuje pomoc, ale neměl v úmyslu říci „ano". Proto přehodil rozhodnutí na někoho jiného. „Moment, zeptám se šéfa."
Položil sluchátko na stůl a Danny slyšel, jak zvedá sluchátko druhého telefonu, vytáčí číslo a vysvětluje záležitost. A tady udělal Kowalski něco nevysvětlitelného — zaručil se za volajícího, který používal jméno Bob Billings.
„Znám ho," řekl řediteloví. „Pracuje pod Edem Trentonem. Můžeme mu zpřístupnit náš identifikátor?"
Danny se sluchátkem u ucha byl udivený tou neobyčejnou a neočekávanou pomocí, které se mu dostalo. Nevěřil vlastním uším. Po několika okamžicích se Kowalski vrátil k telefonu a řekl: „Ředitel by s vámi chti mluvit" a nadiktoval mu číslo mobilu a jméno ředitele.
Danny mu hned zatelefonoval a převyprávěl celou historku ještě jednou, tentokrát s dalšími podrobnostmi o projektu, na kterém pracoval a o tom, proč jeho tým musí nutně dodržet termín.
„Bylo by jednodušší, kdyby prostě někdo došel pro můj identifikátor a přinesl ho," řekl. „Stůl by neměl být zamčený a karta bude nejspíš v levém horním šuplíku."
„Myslím, že vám můžeme povolit používat havarijní identifikátor pouze na tento víkend. Řeknu lidem, kteří budou mít službu, aby vám přečetli kód, když zavoláte," řekl ředitel a sdělil mu PIN, který má používat zároveň s identifikátorem.
Po celý víkend vždy, když se Danny chtěl dostat do firemní počítačové sítě, musel pouze zatelefonovat do výpočetního centra a poprosil o přečtení šesti čísel na displeji identifikátoru.

Práce uvnitř

Tak tedy Danny získal přístup do firemního počítačového systému. Ale co dál?! Jak má nyní nalézt server, na kterém je uložen algoritmus šifrování?
Byl už na to připraven.
Mnoho uživatelů zná diskusní skupiny, objemnou sbírku internetových debat, kam lidé zasílají dotazy, na které jiní odpovídají, nebo vyhledávají nové známé, kteří se také zajímají o hudbu, počítače či jiné z tisíců dalších témat.[16]

[16] Pozn. překl.: Některé tyto diskusní skupiny komunikují pomocí elektronické pošty. Zájemce se přihlásí do konference a pak dostává do své poštovní schránky příspěvky, které se objeví v této konferenci. Sám může poslat svůj příspěvek na jednu adresu a ten je poslán všem přihlášeným účastníkům. Druhý způsob předpokládá, že má uživatel nainstalován na svém počítači program na čtení diskusních skupin (často se říká newsy) na zvláštním serveru; pokud se uživatel chce zúčastnit diskuse, musí se podívat na příslušné místo, jestli je tam něco nového

Jen nemoho lidí si však uvědomuje, že když posílají příspěvek do diskusní skupiny, příspěvek zůstává přístupný po celá léta! Danny začal vyťukáním adresy http://groups.google.com .

Jako dotaz uvedl „šifrování rádio komunikace"[17] a jméno firmy a našel příspěvky vyslané do skupiny jedním zaměstnancem. Byly napsány v době, kdy ve firmě teprve začínali práci na projektu, pravděpodobně dlouho předtím, než policie a úřady začaly uvažovat o možnosti šifrování vysílání.

Zpráva obsahovala signaturu odesilatele obsahující nejen jméno a příjmem (Scott Press), ale také telefon a název pracovního týmu — Secure Communications Group.

Danny zvedl sluchátko a vytočil číslo. Byla to střela od červené — jestlipak bude pracovat po tolika letech ve stejné skupině? Bude v práci za takového počasí? Telefon zazvonil jednou, dvakrát, třikrát a konečně sena druhé straně ozvalo: „Scott, prosím."

Danny se představil jako zaměstnanec odboru informatiky a přesvědčil Presse jedním ze způsobů známých z předešlých kapitol, aby mu prozradil jména serverů, které používal. To byly servery, kde se nejspíše mohl nalézat zdrojový kód obsahující utajovaný algoritmus a firmware bezpečných radiostanic.

Danny se čím dál tím víc přibližoval k cíli a jeho vzrušení se stupňovalo. Cítil už ten blížící se opojný pocit spojený se získáním znalostí dostupných jen nemnohým.

Ale mise ještě neskončila. Po zbytek víkendu se mohl díky ochotnémi řediteli výpočetního centra každou chvíli hlásit k firemní síti. Věděl také které servery ho zajímají. Ale když se připojil, terminálový server mu spojení s programátorskými systémy Secure Communications Group nedovolil. Musel najít jinou cestu.

Následující krok vyžadoval odvahu. Danny znovu zavolal Kowalské-mu do výpočetního centra.

„Můj server mně nechce pustit dovnitř," řekl. „Potřeboval bych nějaké konto na vašem serveru, abych se mohl přes telnet dostat na můj server."

Ředitel už dříve dovolil, aby mu diktovali kód z identifikátoru, takže tato nová žádost zněla docela normálně. Kowalski založil dočasné konto na jednom serveru výpočetního centra a řekl Dannymu: „Dejte mi pak vědět, až už ho nebudete potřebovat, abych ho mohl zase zrušit."

Po přihlášení na dočasný účet se už Danny mohl přihlásit k vývojářským systémům Secure Communications Group. Po další hodině vyhledávání slabých míst, která by mu dovolovala dostat se na hlavní vývojářský server, se mu to konečně podařilo. Správce systému zjevně nebyl seznámen s nejnovějšími způsoby obcházení systémových zabezpečení a o vzdáleném přístupu k systému, což se o Dannym říci nedalo.

Brzy našel soubory s hledanými zdrojovými kódy a přenesl je na server, který nabízel bezplatný diskový prostor. I kdyby tam odhalili ukradené soubory, nedokázali by ho vystopovat.

Před opuštěním systému zbývala ještě jedna operace: systematický proces odstraňování stop po své přítomnosti. Skončil ještě před koncem večerního vydání Jay Leno Show. Danny došel k závěru, že ten víkend nepromarnil. Navíc se v žádném okamžiku nevystavil riziku odhalení. Prožil jen opojné vzrušení, lepší než na snowboardu nebo bungee-jumpingu.

Té noci se Danny opil ne ginem, pivem či skotskou, ale pocitem moci a převahou, které v něm narostly během prohlížení ukradených souborů obsahujících přísně tajné programové vybavení pro vysílačky.

Analýza podvodu

[17] Pozn překl.: Napsal to pochopitelně anglicky „encryption radio communications".

Podobné jako v předchozím příběhu podvod zafungoval, protože jeden ze zaměstnanců příliš zbrkle uvěřil, že telefonující osoba je opravdu tím, za koho se prohlašuje. Na jednu stranu ochota pomoci spolupracovníkovi zvětšuje produktivitu firmy a způsobuje, že s někým rádi spolupracujeme zatímco s jinými ne. Na druhou stranu se však naše ochota pomoci může projevit jako naše slabost, kterou sociotechnik rád využije.

Jistý prvek Dannyho manipulace byl obzvláště rafinovaný: když žádal, aby šel někdo pro jeho identifikátor, který ležel na stole, tak použil slovo „přinést“. „Přines" je příkaz, který se dává psu. Nikdo nemá rád, kdvž mu někdo říká, aby něco „přinesl". Když tedy Danny použil toto slovo, mohl si být jistější, že nikdo nebude chtít splnit tento „příkaz" a vybere si raději nějaké jiné řešení, což právě chtěl.

Pracovník výpočetního centra Kowalski se dal Dannym doběhnout, když uslyšel jména lidí, které znal. Ale jak je možné, že nadřízený Kowalského — nikdo menší než manažer IT — dovolil cizí osobě přístup do vnitřní firemní sítě? Prostě prosba o pomoc se může stát dokonalým přesvědčovacím nástrojem v arzenálu sociotechnika.

Mohlo by se něco podobného stát ve vaší firmě? Nebo se to snad už stalo?

Poznámka Mitnicka
****
Popsaný příběh ukazuje, že časově závislé kódy a podobné autentikační metody nezaručují ochranu před chytrým sociotechnikem. Jedinou účinnou obranou je svědomitý pracovník, který postupuje podle bezpečnostních pravidel a rozumí tomu, jak mohou lidé s nekalými úmysly ovlivňovat jeho chování.
****

Prevence

Často se opakujícím prvkem v popisovaných příbězích této knížky je útočník, který se dostává do firemní sítě zvenku díky osobě, která se neobtěžuje ověřit, jestli volající je opravdu ten, za koho se vydává. Proč se k tomu pořád vracím? Protože v mnoha sociotechnických útocích je to základní činitel úspěchu operace. Pro sociotechnika je to ten nejsnazší způsob k dosažení cíle. Proč by měl sociotechnik trávit dlouhé hodiny na pokusy nabourat se do systému, když se tam může dostat pomocí jednoho telefonátu?

Jednou z nejúčinnějších taktik je jednoduchý fígl s prosbou o pomoc — proto je také často používaný. Určitě nechceme, aby naši zaměstnanci přestali úplně pomáhat svým kolegům nebo zákazníkům, proto je třeba je vybavit jednoznačnými pokyny, jak ověřovat, když nastane situace, kdy někdo prosí o důvěrná data nebo o přístup k počítači. Tímto způsobem způsobem moho dále pomáhat těm, kteří to opravdu potřebují, ale zároveň chrání majetek a počítačový systém firmy.

Firemní bezpečnostní politika a pravidla musejí jednoznačně popisovat detaily ověřovacího mechanismu, který by měl být používán za různých okolností. V 16. kapitole lze najít podrobný seznam pokynů a níže je uvedeno několik bodů jako námět k přemýšlení.

- Jeden z účinných způsobů ověřování osoby, která žádá o přístup do chráněných oblastí, spočívá v zavolání na číslo pracovníka. Jestliže volající je vetřelec, ověřovací telefon dovolí spojit se se skutečným pracovníkem, zatímco útočník je na druhé lince. Eventuálně se spojíme s jeho hlasovou schránkou a porovnáme hlas volajícího s hlasem osoby, za kterou se prohlašuje.
- Pokud používá firma čísla zaměstnanců k identifikačním účelům, pak musejí tato čísla být pokládána za důvěrné informace, bedlivě chráněná a nesmějí být poskytována neznámým osobám. To samé se týká všech

jiných vnitřních identifikátorů, které se v podniku používají, jako jsou například čísla vnitřních linek, účetnické identifikátory a dokonce i e-mailové adresy.

- Školení by mělo upozorňovat na všeobecnou tendenci považovat neznámé lidi za pracovníky firmy jen proto, že se zdá, jako by měli odpovídající znalosti nebo autoritu. Samotná skutečnost, že osoba má přístup do chráněné oblasti firmy nebo že zná firemní reálie a postupy, ještě neznamená, že už nebudeme ověřovat její totožnost jiným způsobem.
- Pracovníci ochrany a správci systému se nemohou soustředit jen na kontrolu jiných. Rovněž sami se musejí řídit těmito pravidly, pokyny a zásadami.
- Hesla a jim podobné identifikátory nemohou být sdělovány jiným osobám. Toto pravidlo má zvláštní váhu v případě používání časově závislých kódů a podobných vyspělých ověřovacích zařízení. Všem by mělo být zřejmé, že prozrazování těchto informací poškozuje celý smysl instalace a používání takového systému. Využívání cizích identifikátorů způsobuje zánik odpovědnosti. Znamená to, že jestliže někdo něco provede, nebude potom možné najít viníka.
- Jak v této knížce neustále opakuji, pracovníci musejí znát finty používané sociotechniky. Hraní scének, kde má každý nějakou roli, by mělo být základním prvkem školení. Umožní to zaměstnancům lepší pochopem metod jednání sociotechnikú.

7

Falešné stránky a nebezpečné přílohy

Je všeobecně známo, že nic není zadarmo. A přece je trik spočívající v nabídce něčeho zadarmo stále s úspěchem používaný jak poctivými firmami, tak těmi druhými.

Většina z nás bývá možností získat něco zadarmo tak oslněná, že se nad nabídkou a sliby v ní obsaženými střízlivě nezamýšlíme. Takové nabídky se často objevují v naší schránce. Je dobré dávat si pozor na přílohy e-mailů a na programy poskytované zdarma. Zběhlý útočník je schopný použít všechny prostředky, aby se naboural do firemní počítačové sítě, včetně využití naší slabosti pro dárky. Tady máme několik příkladů.

Chtěl bys zadarmo...?

Stejně jako jsou odedávna viry prokletím lidstva, počítačové viry jsou tím samým ve světě počítačů. Počítačové viry, kterým se ve sdělovacích prostředcích věnuje nejvíce pozornosti, nejsou nutně těmi, které způsobují největší ztráty. Jsou to výtvory počítačových vandalů.

Tito lidé se za každou cenu snaží pochlubit svou chytrostí. Občas jejich činy připomínají iniciační obřady, které mají udivit starší a zkušenější crackery. Cílem těchto osob je stvoření viru, který by způsobil co možná největší škody. Jestliže „dílo" ničí soubory nebo celé pevné disky a hlavně jestli se samo posílá tisícům nic netušících uživatelů Internetu, pak je cracker pyšný na to, co udělal. Pokud je virus tak účinný, že o něm píší noviny a varují před ním hlášky na síti, pak je crackerova pýcha ještě větší.

Mnohé už bylo o virech a jejich tvůrcích řečeno. Byly vydány knížky, napsány antivirové programy a byly také založeny firmy, které nabízejí ochranu před viry. Proto se také v této knize nebudeme zabývat technologickými detaily útoků. Předmětem našeho zájmu se stanou namísto vandalských útoků činy vandalova vzdáleného příbuzného - socíotechnika, zaměřeného více na konkrétní cíle.

To přišlo v e-mailu

Snad každý den dostáváme e-maily obsahující reklamy nebo nabízející zadarmo něco, co ani nechceme, ani nepotřebujeme. Známe je dobře. Slibují investiční rady, slevy na počítače, televizory, kamery, vitamíny nebo zájezdy, nabízejí kreditní karty, které nepotřebujeme, zařízení umožňující sledovat kabelovou televizi bez placení předplatného, návody na zlepšení zdraví nebo sexuálního života atd.

Čas od času se však objeví v naší schránce nabídka, která upoutá pozornost. Může to být hra zadarmo, nabídka fotografií oblíbené hvězdy, bezplatný kalendářní program nebo levný program typu shareware, který zabezpečí náš počítač před viry. V každém takovém případě e-mail obsahuje odkaz na stránku, která obsahuje nabízený produkt.

Občas dostáváme zprávu s předmětem typu: „Jacku, stýská se mi po Tobě" nebo „Anno, proč jsi mi tak dlouho nenapsala?" nebo také „Ahoj Říšo, zde je ta sexy fotka, kterou jsem Ti slíbila". Zdá se nám, že to nemůže být e-mail s reklamou, protože obsahuje naše jméno a tón je velí osobní. Otevíráme tedy přílohu, abychom se podívali na fotky nebo přečetli text.

Stahování si programů, o kterých jsme se dozvěděli z reklamního e-mailu, klikání na odkaz, který nás přenese na stránku, o které jsme nikdy předtím neslyšeli, nebo otevírání příloh od někoho, koho neznáme — tím vším si jenom koledujeme o nepříjemnosti. Pochopitelně ve většině případů budeme zklamaní, ale nijak nám to neublíží. Občas je však to, co nám bylo posláno, dílem počítačového vandala.

Zaslání nebezpečného programu na náš počítač je pouze jeden z prvků útoku. Aby se útok povedl, musí nás útočník ještě přesvědčit, abychom si tu přílohu otevřeli.

Fungování nejničivějších virů, mezi jinými to byly LoveLetter, Sir-Cam a Anna Kurnikova, se opíralo o sociotechnickou manipulaci - využívalo naši touhu dostat něco zadarmo. Díky tomu se mohly účinně rozšířit. Virus se objeví v příloze mailu, který nabízí něco hodného pozornosti, například důvěrné informace, bezplatnou pornografii nebo (velmi mazaný trik) zprávu, Že příloha obsahuje účet za nějakou drahou věc, kterou jsme si údajně koupili. V posledním případě otevíráme přílohu hnáni obavou, že byla naše kreditní karta zatížena výdajem za zboží, které jsme si neobjednali.

Je zarážející, kolik lidí se dá na takové triky nachytat, dokonce i když jim bylo mnohokrát vysvětlováno nebezpečí spojené s otevíráním příloh. Povědomí o nebezpečí se časem vytrácí a pak se stáváme bezbrannými.

Rozeznávání nebezpečného softwaru

Jiným druhem nebezpečných programů — takzvaného *malwaru* — jsou ty, které po spuštění pracují bez našeho vědomí či souhlasu nebo vykonávají i činnost, o které nevíme. Takové programy mohou vypadat zcela nevinně — mohou to být dokonce dokumenty ve Wordu, prezentace v PowerPointu nebo soubory z jakékoliv aplikace, která umí pracovat s makry — ale přitom skrytě instalují neautorizovaný program. Může to být nějaká verze trojského koně, o kterém jsme mluvili už dříve v páté kapitole. Jakmile se program usídlí na našem počítači, může posílat útočníkovi všechno, co píšeme na klávesnici včetně hesel a čísel kreditních karet.

Žargon
****
Malware — slangový výraz pro malicious software, tedy záludný či zákeřný software. Je to počítačový program jako třeba virus, červ nebo trojský kúň, který provádí škodlivou činnost.
****

Poznámka
****
Existuje též obměna tohoto programu zvaný RAT[18] (trojský kúň se vzdáleným přístupem), který umožňuje útočníkovi plný přístup na náš počítač, jako by seděl u naší klávesnice.
****

Existují ještě dva druhy nebezpečného softwaru, jejichž způsob fungování nás může šokovat. Jeden z nich je schopný posílat každé slovo, které vyslovíme v dosahu počítačového mikrofonu, *dokonce i tehdy, když se nám zdá, že je vypnutý*. A máme-li počítač vybavený webovou kaměrou, útočník muže pomocí obměny této techniky vidět všechno, co děje v okolí našeho počítače, co je v zorném poli kamerky, a to i tehdy, když si myslíme, že je vypnutá.

Hacker se zvláštním smyslem pro humor muže zkusit do našeho systému nainstalovat program vytvořeny jen proto, aby nás vyvedl z rovnováhy. Může například každou chvíli vysunovat mechaniku CD nebo zmenšovat velikost okna

[18] Pozn. překl.: RAT můžeme chápat buďto jako zkratku pro „trojského koně - vzdáleným přístupem", tedy Remote Access Trojan, anebo doslova — rat je anglicky krysa

aplikace, se kterou právě pracujeme. Může také spustit přehrávání zvukového souboru na plnou hlasitost uprostřed noci. Je to nepříliš zábavné, ale alespoň to nepůsobí nějaké skutečné Škody.

Poznámka Mitnicka
****
Vyvarujme se všech „dárečků" nabízených nám v e-mailech, aby naši firmu nepotkal osud podobný tragédii města Trója. V případě pochybností je vhodné použít antivirové programy.
****

Zpráva od přítele

Výsledek ale může být ještě horší, dokonce i když jsme byli opatrní. Představme si, že jsme se rozhodli nedat hackerům žádnou šanci. Proto si nebudeme stahovat žádné soubory z internetových stránek kromě těch, které známe a víme o nich, že jsou bezpečné, například SecurityFocus.com či Amazon.com. Nebudeme také klikat na odkazy v mailech, které jsme dostali z neznámých adres. Nebudeme už otevírat přílohy v elektronické poště, kterou jsme neočekávali. Budeme kontrolovat, jestli se v prohlížeči objevuje symbol bezpečného spojení během každé transakce přes Internet nebo při zasílání důvěrné informace.

Jednoho dne však dostaneme e-mail od přítele nebo spolupracovníka, který obsahuje přílohu. Copak tam může být něco nebezpečného, když pochází od někoho, koho dobře známe? Řekli bychom, že ne, zvláště když víme, koho máme potom obviňovat, kdyby se něco stalo a naše data byla zničena.

Otevíráme přílohu a... PRÁSK HO! Dostali jsme virus nebo trojského koně. Jak nám mohl někdo, koho dobře známe, provést něco takového. Některé věci nejsou takové, jaké se zdají. Už o tom byla řeč: virus, který se dostane na něčí počítač a rozesílá se všem, které najde v seznamu adres. Každá z těchto osob dostává zprávu od někoho, koho dobře zná a komu důvěřuje a každá z těchto zpráv obsahuje virus, který se šíří jako kola na vodě, když do ní vhodíme kámen.

Tato technika je účinná, protože tu máme příslovečné dvě mouchy jednou ranou: možnost šíření nic netušícím obětem a identifikaci odesílatele, která vyvolává zdání původu od důvěryhodné osoby.

Je to smutné, ale je to tak. Při současné úrovni technologie můžeme dostat e-mail od někoho blízkého a přemýšlet, jestli je bezpečné ho otevřít.

Poznámka Mitnicka
****
Člověk vymyslel mnoho skvělých věcí, které změnily svět i náš život. Jenže zároveň s nástupem nových technologií, ať už telefonu, počítačů či Internetu, se objevily nové možnosti jejich zneužití k nekalým účelům.
****

Variace na téma

V období všeobecné dostupnosti Internetu se stal populární podvod spočívající v přesměrování uživatelů na falešnou webovou stránku. Stává se to dost pravidelně a má to mnoho variant. Zde uvedený příklad založený na skutečných událostech je dosti reprezentativní.

Veselé svátky

Pojišťovací agent v důchodu Edgar dostal jednoho dne e-mail z PayPal – firmy nabízející rychlý a pohodlný způsob realizace plateb přes síť. Tento druh služby je vhodný zejména, když osoba z jedné části země (nebo světa, na tom už nesejde) kupuje něco od jiné osoby, kterou nezná. PayPal zatíží kreditní kartu kupujícího a převede peníze ihned na konto prodávajícího.

Edgar jako sběratel starých zavařovacích sklenic prováděl hodně transakcí přes internetový aukční dům eBay a často využíval PayPal – občas dokonce i několikrát týdně.

Proto ho zaujala zpráva, kterou obdržel někdy o Vánocích 2001, a která nabízela odměnu za aktualizaci konta v PayPal. Zpráva zněla takto:

> Veselé svátky stálému klientu PayPal:
> Přichází Nový rok. Aby ten starý uplynul rychleji, PayPal zvýši stav Vašeho konta o 5 $!
> Abyste získal zmíněný dárek, stači aktualizovat informace na našem bezpečném serveru PayPal do 1. ledna 2002. Každý rok přináší hodně změn. Tým, že aktualizujete informace na svém kontu, umožníte nám poskytnout Vám i dalším našim stálým zákazníkům služeb služby nejvyšší kvality a pomůže nám to udržet pořádek v našich datech!
> Abyste zaktualizoval nyní informace a dostal ihned 5 $ na konto PayPal. Stačí kliknout na tento odkaz:
> *http://www.paypa1-secure.com/cgi-bin*
> Děkujeme vám za používáni PayPal a pomoc v udržováni vedoucí pozice na trhu!
> Srdečné přáni veselých svátků a šťastného Nového roku.
> Team PayPal

Edgar si nevšiml ani jednoho z několika význačných znaků, že není v pořádku (například středník na konci řádky s uvítáním nebo neohrabaný text „našim stálým zákazníkům služeb služby nejvyšší kvality"). Kliknul tedy na daný odkaz, vložil požadované informace! jméno, příjmem, telefonní číslo, informace o kreditní kartě – a čekal až se na následujícím výpisu kreditní karty objeví slibovaných pět dolarů. Místo toho obdržel seznam plateb za věci, které si nikdy nekoupil.

Analýza podvodu

Edgar se stal obětí typického internetového podvodu, který nabývá různých podob. Jedna z nich (popsaná v deváté kapitole) využívá falešnou autentikační stránku vytvořenou sociotechnikem, která předstírá přihlašovací obrazovku nějaké internetová stránky. Rozdíl je v tom, že falešná stránka neposkytuje přístup na adresu, kam se uživatel pokouší dostat, ale místo toho hacker získává login a heslo uživatele.

Finta v Edgarově případě byla v tom, že si podvodníci zaregistrovali doménu *paypal-secure.com* – což vyvolává dojem, že jde o bezpečnou stránku oficiálních stránek PayPal. Ale není. Jakmile Edgar informace o sobě vložil na stránku, dostaly se k útočníkům.

> *Poznámka Mitnicka*
> **********
> Pokaždé, když navštěvujeme adresu, která od nás vyžaduje soukromé údaje, je nutné se ujistit, jestli je spojení zabezpečené a data šifrována. Ještě důležitější je však to, abychom automaticky neklikali na „Ano" v objevujících se dialogových oknech, která nás mohou varovat o nesprávném, prošlém či zrušeném bezpečnostním certifikátu.
> **********

Variace na téma variace

Kolik je různých způsobů lákání uživatelů na falešné internetová stránky, kde zanechávají své osobní údaje? Nepředpokládám, že by někdo mohl dát přesnou odpověd, ale slovo „hodně" by mělo postačit.

Poznámka o internetových obchodech
****
Jsou lidé, kteří mají zábrany nakupovat prostřednictvím Internetu dokonce od značkových firem jako jsou Amazon, eBay nebo prostřednictvím webových stránek společností Old Navy, Target či Nike. V jistém smyslu ie jejich podezíravost oprávněná.
Jestliže náš prohlížeč používá dnes standardního 128-bitového šifrování, informace, které od nás odcházejí jsou v zakódovaném tvaru. Data by mohla být po velkém úsilí rozluštěna, ale pravděpodobně se šifra nedá zlomit v rozumném čase, ledaže by se do toho pustil Národní bezpečnostní úřad (a NSA, pokud je nám známo, nevykazuje známky toho, že by měla zájem krást čísla kreditních karet nebo zjišťovat, kdo si objednává pornografické filmy a sexy prádlo).
Ačkoliv internetové obchody vynakládají velké úsilí, aby chránily data během jejich posílání, mnoho z nich chybuje, když ukládá do databází údaje týkající se klientů v nezašifrované podobě. Ještě horší je, že hodně internetových obchodů, které používají SQL server od Microsoftu, tento problém značně zhoršuje, když nemění defaultní heslo pro administrátora systému. Po instalaci softwaru heslo zní „null" a ukazuje se, že to „null" leckde funguje dodnes. Tímto způsobem se obsah databáze stává přístupný pro každého uživatele Internetu, který o této skutečnosti ví a pokusí se připojit k databázi. Tyto stránky jsou pod neustálým útokem a informace jsou vykrádány.
Na druhou stranu ti samí lidé, kteří se obávají nákupů přes Internet, protože se bojí o údaje o své kreditní kartě, nevidí problém při placení kreditní kartou v nedalekém obchodě se stavebním materiálem nebo za oběd či drinky v podezřelém baru, kam by určitě nepozvali svoji matku. Z takových míst bývají notoricky kradené porvrzenky z transakcí nebo je někdo vybírá z popelnice stojící za lokálem. Nepoctivý prodavač nebo číšník si může poznamenat naše jméno a informace o kartě, eventuálně použít čtecí přístroj, který se dá sehnat přes Internet a který ukládá údaje každé kreditní karty, kterou naskenuje.
Každý pilot ví, že nejnebezpečnější fází letu je příjezd na letiště a návrat z něho domů. Let samotný není zcela bez rizika, ale statistiky zaznamenávají, že létání je bezpečnější než jízda autem. Podobně tomu je s internetovými nákupy: existuje jisté riziko při nákupech na Internetu, ale vůbec není větší než riziko při nákupu v běžném obchodu. Banky nabízejí jistý dodatečný druh ochrany při používání karty na síti — například pokud byly provedeny nějaké neautorizované nákupy, odpovídáte pouze za prvních Padesát dolarů.
Takže podle mého názoru jsou obavy spojené s nákupy přes Internet neodůvodněné.
****

Falešné odkazy

Velmi oblíbeným trikem je posílání e-mailů, které nabízejí nějaký lákavý důvod, proč by stálo za to navštívit danou adresu a obsahují na ni bezprostřední odkaz. Bohužel tento link obvykle nevede na stránku kterou

očekáváme, protože jenom „předstírá" odkaz na tuto adresu. Zde je příklad takového falešného linku, jaké se často objevují na Internetu. Odkaz měl zdánlivě ukazovat na firmu PayPal:

www.PayPai.com

Na první pohled nápis vypadá jako „PayPal". Dokonce i když si uživatel všimne chyby, muže si pomyslet, že je to nějaká nedokonalost při zobrazování textu, která má za následek, že „1" vypadá jako „i". Kdo z nás by však prokoukl, že v adrese

www.PayPal.com

je použita číslice „1" místo našeho písmenka „1"? Je tolik lidí, kteří si nedokáží povšimnout chyb v pravopisu a podobných chybných přesměrování, že tento fígl nepřestává být mezi internetovými zloději kreditních karet oblíbený. Falešná stránka obvykle vypadá jako stránka, kam si uživatelé mysleli, že jdou, proto tam klidně a bezstarostně zanechávají číslo své kreditní karty. Podvodník si musí při kladení pasti pouze zaregistrovat falešnou doménu, rozeslat e-maily a pak jen čekat na naivní lidi, kteří prostě chtějí být podvedeni.

V polovině roku 2002 jsem obdržel mail, který vypadal jako hromadný dopis. Jako odesílatel byl uvedený *Ebay@eBay.com* . Zde je obsah té zprávy:

> Zpráva: Vážený uživateli eBay.
> všimli jsme si. že nepovolaná osoba využívá Vaše eBay konto a porušuje jeden z bodů naši smlouvy, který zde uvádíme:
> 4. Licitace a nákup
> Po nákupu předmětu za uvedenou cenu nebo při vyhrané licitaci po nabídnuti nejvyšší ceny má kupující povinnost dokončit transakci. Jestliže v okamžiku zakončení aukce je Vaše nabízená cena nejvyšší (vyšší než jiné ceny alespoň o velikost minimálního navýšeni a vyšší než minimální cena) a vaše nabídka byla přijata prodávajícím, jste povinni dokončit transakci, pokud neni v rozporu se zákony nebo touto smlouvou.
> Tímto dopisem od eBay Vás chceme upozornit, že Vaše konto způsobilo narušení obchodů jiných uživatelů eBay. proto Vás žádáme o bezodkladnou verifikaci, jinak budeme nuceni Vaše konto zrušit.
> Verifikaci lze uskutečnit na adrese
> *http://error_bay.tripod.com*
> **********
> Použitá jména a obchodní známky jsou vlastnictvím jmenovaných firem. eBay a logo eBay jsou obchodní známky firmy eBay Inc.

Ti kteří kliknuli na ten odkaz, byli přesměrováni na adresu, která vypadala velmi podobně jako oficiální stránka eBay. Byla výborně napsána, obsahovala originální logo eBay a všechna navigační tlačítka typu „prohlížej" nebo „kup" směřovala na pravé stránky eBay. Prohlížeč ukazoval, že spojení je zabezpečené. Tvůrce stránky myslel dokonce i na to, aby použil šifrovanou HTML, která znemožňuje odhalit, kam budou vložené údaje odeslány.

je to dokonalý příklad sociotechnického útoku s využitím počítače. Nebyl však zcela bezchybný.

Zpráva nebyla příliš dobře napsána. Konkrétně odstavec začínající na „Tímto dopisem od eBay Vás chceme upozornit" zní dost neobratně a neprofesionálně (lidé dopouštějící se takových činů si nikdy nenajímají profesionální textaře, což je obvykle vidět). Kromě toho si všímavější osoba mohla položit otázku, proč mne eBay žádá o informace z PayPal. Není důvod, proč by se mne eBay měl ptát na soukromé informace související s jinou firmou.

A zkušený internetový uživatel by si pravděpodobně všiml, že hyperlink nevede do domény eBay, ale na tripod.com – poskytovatele bezplatných intemetových stránek. Určitě tam však mnoho lidí vložilo své osobní údaje zároveň s číslem kreditní karty.

Poznámka Mitnicka

****
Proč se dovoluje lidem registrovat si domény, které vypadají jako potenciální léčky? Protože podle současných zákonu si může na Internetu kdokoliv zaregistrovat jakoukoliv doménu, která je volná.
****

Některé firmy se snaží proti tomuto pravidlu bojovat, ale často je to boj s větrnými mlýny. General Motors vyvolal proces proti firmě, která si zaregistrovala doménu fuckgeneralmotors.com, která pak odkazovala na stránky General Motors. A firma GM prohrála.

Buď připraven!

Individuální uživatelé Internetu by měli být ostražití a zvažovat rozhodnutí, kdy je sdělování jejich osobních údajů, hesel, čísel kont a podobně odůvodněné a bezpečné.

Kolik našich známých je schopno rozpoznat, jestli příslušná internetová stránka splňuje nároky na bezpečnou stránku? Kolik pracovníku naší firmy ví, podle čeho se to dá poznat?

Každý, kdo používá Internet, by měl znát malý symbol, který se občas objevuje na stránce a připomíná visací zámek. Je třeba mít na paměti, že zamknutý zámek znamená, že stránka má bezpečnostní certifikát. Když je zámek otevřený nebo se ikonka zámku neobjevila, stránka není autentikována jako originální a každá vyslaná informace bude nezašifrovaná.

Na druhou stranu útočník, který dokáže získat administrátorská práva na firemním počítači, může změnit kód operačního systému aby si uživatel neuvědomoval, co se vlastně doopravdy děje. Mohl například změnit část kódu prohlížeče, která je odpovědná za kontroli autentikačního certifikátu daného spojem tak, že kontrola vůbec nebude probíhat. Do operačního systému může vložit *zadní vrátka*, což je velmi těžko odhalitelné.

Žargon
****
Zadní vrátka — skrytá možnost přístupu do systému uživatele. Tento trik je často používán programátory během psaní programů a umožňuje jim snadný přístup do programu například kvůli diagnostickým účelům.
****

Bezpečné spojení ověřuje stránku jako originální a šifruje předávané informace, proto útočník není schopen využít žádných zachycených dat. Můžeme mít tedy důvěru k těm stránkám, které používají bezpečné spojení? Ne, protože vlastník stránky mohl udělat nějakou chybu ve svém zabezpečovacím systému nebo nemusí hlídat, jestli uživatelé a administrátoři dodržují patřičná pravidla na ochranu hesel. Nelze tedy předpokládat, že zdánlivě bezpečná stránka není nebezpečí vystavena.

Bezpečný protokol HTTP (*Hypertext Transfer Protocol*) nebo SSL (*Secure Socket Layer*) zajišťuje automatický mechanismus, který používá digitální certifikáty nejen k šifrování informací předávaných na jiné adresy, ale rovněž k ověřování (ujištění návštěvníka, že je na originální adrese). Avšak tento ochranný mechanismus nefunguje, jestliže si uživatel nevšímá, jestli je adresa, která se objevila v okénku, správná.

Žargon
****
SSL (Secure Socket Layer) — protokol vytvořený firmou Netscape, který provádí ověřování pro potřeby bezpečné komunikace přes Internet na straně klienta i serveru.
****

Jiným prvkem svázaným s bezpečnostní, nejčastěji ignorovaným je varovná zpráva: „Prohlížená stránka není bezpečná nebo její bezpečnostní certifikát vypršel. Chcete přesto pokračovat v prohlížení?" Mnoho internetových uživatelů nerozumí této zprávě a když se tato objevvj tak jednoduše zmáčknou OK a pokračují v surfování. Je třeba mít na paměti, že když jsme na stránce, která nepoužívá bezpečný protokol,neměli bvste nikdy vkládat důvěrné informace jako heslo, které použíme i jinde, adresu nebo telefonní číslo, číslo kreditní karty nebo bankovního konta a vlastně žádné soukromé údaje.

Thomas Jefferson kdysi řekl, že udržení svobody od nás vyžaduje „věčnou bdělost". Udržení soukromí a bezpečnosti ve společnosti, kde se informace přepočítávají na peníze, od nás vyžaduje nemenší úsilí.

Pozor na viry

A ještě zvláštní poznámka týkající se antivirového softwaru: je nezbytný pro firemní intranet a pro každého pracovníka, který používá počítač. Kromě instalace samotného antivirového programu na počítači je nutné tento program samozřejmě ještě spouštět (což mnoho lidí nemiluje, protože to zpomaluje činnost některých aplikací).

Existuje ještě jedna záležitost spojená s antivirovým programem — aktualizace definic virů. Pokud firma nemá vytvořen systém distribuce nových definic po síti ke každému uživateli, pak se každý uživatel musí starat o nahrávání nejnovějších aktualizací sám. Osobně doporučuji takové nastavení antivirového programu, aby se nové definice instalovaly automaticky každý den.

Na rovinu — jestliže pravidelně neaktualizujeme definice virů, vystavujeme se nebezpečí. Dokonce i když aktualizujeme pravidelně, stále existuje jisté riziko nových virů, o kterých výrobce antiviru ještě neví nebo dosud nestačil vytvořit procedury, které by nové viry odhalovaly.

Všichni pracovníci, kteří mají vzdálený přístup k firemním serverům ze svých notebooků či domácích počítačů, musí aktualizovat svůj antivirový software a používat na svých počítačích firewally jako nezbytné ninimum. Prvním krokem rafinovaného útočníka je celková prohlídka objektu, aby našel nejslabší bod, na který by potom zaútočil. Odpovědnost za firmu vyžaduje neustálé pripomínání pracovníkům, že musejí používat firewally a aktualizovat antivirový software. Nelze očekávat ode všech manažerů, obchodních zástupců a dalších pracovníků, že budou pamatovat na nebezpečí, které s sebou nese nezabezpečený počítač.

Kromě těchto kroků doporučuji používání méně známých, ale neméně důležitých balíčků, které nás chrám před trojskými koňmi. V době psaní této knížky byly dva nejznámější Cleaner (*www.moosoft.com*) a Trojan Defense Sweep (*www.diamondc.com.au*).

A konečně nejdůležitější záležitost spojená s bezpečností firem, které neskenují všechnu poštu přicházející zvenku: protože máme tendenci přikládat menší váhu věcem nesouvisejícím bezprostřední s naši, je třeba neustále připomínat pracovníkům, aby neotevírali přílohy, ledaže by si byli jisti osobou nebo organizací, která ji poslala.

Vedení musí také stále připomínat pracovníkům nutnost používat antivirový program a odhalovač trojských koní — neocenitelná ochrana před e-maily, které vypadají důvěryhodně, ale obsahují destruktivní náklad.

8

Soucit, vina a zastrašení

V patnácté kapitole je popsáno, jak sociotechnik využívá znalost lidské psychiky, aby si podmanil oběť. Zkušení sociotechnici jsou zběhlí ve vytváření situací, stimulujících takové emoce jako strach, vzrušení nebo pocit viny. Za tímto účelem využívají vnitřních mechanismů osobnosti, které velí lidem reagovat na prosby, aniž by se nad situací pořádně zamysleli.

Všichni se snažíme vyhýbat se těžkým situacím, které se týkají nás samotných či jiných osob. Útočník, který se opírá o tuto pozitivní vlastnost, může využívat soucit oběti, zařídit, aby se cítila provinile nebo ji zastrašit.

Zde je několik příkladů ukazujících, jak je možné si zahrávat s emocemi.

Návštěva ve studiu

Někteří lidé dokáží projít okolo osoby hlídající vstup například do hotelového sálu, kde se odehrává nějaká soukromá recepce nebo setkání, takovým způsobem, že se jich nikdo neptá na pozvánku či vstupenku. Na podobném principu se dokáže sociotechnik chytře vedeným rozhovorem vetřít do míst, kde bychom to považovali za nemožné, jako v následujícím příběhu.

Telefonát

„Kancelář Rona Hillarda, u telefonu Dorothy."

„Dobrý den, Dorothy. Jmenuji se Kýle Bellamy. Jsem nový pracovník firmy a mám pracovat při animaci ve skupině Briana Glassmana a mnoho věcí se tu dělá jinak."

„Asi ano, nikdy jsem nepracovala v jiné společnosti, tak to můžu těžko posoudit. Jak ti můžu pomoci?"

„Abych řekl pravdu, cítím se trochu trapně. Dnes odpoledne přijde na setkání scenárista a já ani nevím, s kým mám mluvit o jeho uvedení do studia. Lidé z Brianova sekretariátu jsou sice velmi milí, ale nechci je pořád otravovat otázkami typu: „Jak se dělá to?", „Jak se dělá tamto“ Cítím se, jako bych byl první den na základce a neuměl najít cestu na záchod, jistě znáš ten pocit."

Dorothy se rozesmála.

„A když už najdeš záchod, tak nevíš, jak se potom vrátit."

Znovu se zasmála při nějaké vzpomínce z minulosti a řekla: „Musíš obrátit na ostrahu. Vytoč 7 a potom 6138. Jestli to zvedne Lauren, řekni že Dorothy prosí, aby se o tebe postarala."

„Díky Dorothy. Jestli netrefím na pánskou toaletu, možná ještě volám."

Ještě se společně zasmáli a zavěsili.

Příběh Davida Harolda

Miluji kino, a když jsem se stěhoval do Los Angeles, myslel jsem si, tu každou chvíli budu potkávat nějaké lidi z filmové branže a oni mne budou brát na párty nebo zvát na lunch do studia. Po ročním pobytu ve městě se blížily mé šestadvacáté narozeniny a mým nejdůvěrnějším setkáním s filmovým průmyslem

byla exkurze do Universal Studios s milými lidmi z Phoenixu a Clevelandu. Nakonec jsem došel k závěru, že když mě nechtějí pozvat, pozvu se sám. A tak jsem to také udělal.

Koupil jsem si výtisk *Los Angeles Times*, pročetl jsem rubriku „zábava“ a zapisoval jsem si jména producentů z různých studií. Rozhodl jsem se pro začátek atakovat jedno z největších.

Zavolal jsem na ústřednu a poprosil jsem o spojení se sekretariátem producenta, jehož jméno jsem si přečetl v novinách. Hlas sekretáři která zvedla sluchátko, patřil nějaké ženě mateřského typu, dobře jsem se tedy trefil. Kdybych narazil na jednu z těch mladých holek, které tam pracují s nadějí, že „budou objeveny", asi by nebyla příliš náchylná k pomoci.

Zato Dorothy vypadala na jednu z těch osob, které si domů přinášejí opuštěné kočky a dokážou soucítit s novým zaměstnancem, který je v novém prostředí zmatený, a tak se mi podařilo brzy s ní navázat blízký kontakt. Nestává se každý den, aby vám osoba, kterou se snažte oklamat, dala víc, než od ní očekáváte. Nejen že mi dala jméno jedné z pracovnic ostrahy, ale ještě mi řekla, že se na ni mám odvolat.

Samozřejmě jsem tak jako tak plánoval její jméno využít. Tohle mi jen zjednodušilo práci. Lauren se mi otevřela hned a ani se neobtěžovala podívat, jestli je jméno, které jsem jí řekl, uvedeno na seznamu pracovníků.

Když jsem odpoledne přijel k bráně, nejenže moje jméno figurovalo na seznamu hostů, ale bylo pro mne připravené i parkovací místo. V jídelně jsem snědl pozdní oběd a až do večera jsem se potuloval po studiích, podařilo se mi dokonce vklouznout do několika studií, kde se zrovna točily nějaké scény do filmů. Byl jsem tam až do sedmi večer. Ten den jsem si opravdu užil.

Analýza podvodu

Každý byl někdy novým zaměstnancem. Všichni máme vzpomínky na první dny v práci, zejména z dob, kdy jsme byli mladí a nezkušení. Když nový pracovník prosí o pomoc, dá se očekávat, že mnoho lidí — zejména níže postavených — si připomene vlastní zážitky z prvních dní v práci a podá mu pomocnou ruku. Sociotechnik si to uvědomuje a ví, že tímto způsobem může využívat soucit svých obětí.

Právě tímto způsobem ulehčujeme cizím osobám, aby se dostaly na území našich firemních pracovišť a kanceláří. A co když je v naší firmě povinná zásada doprovázení cizích lidí? Princip samotný je dobrý, ale funguje jen tehdy, jestliže mají všichni zaměstnanci zakořeněný zvyk zastavit každého, kdo má cedulku hosta nebo kdo nemá vůbec žádnou cedulku a pohybuje se po prostorách firmy, a klást mu příslušné otázky. Jestliže se odpovědi zdají podezřelé, pracovník by měl zavolat ochranku.

Za situace, kdy je možné se do prostor firmy velmi jednoduše dostat, jsou její důvěrné informace v nebezpečí. A navíc, bereme-li dnes v úvahu nynější hrožení teroristickými útoky, jsou nebezpečí vystaveny nejen informace.

Udělej to teď hned!

Ne každý, kdo používá sociotechnické metody, je opravdovým sociotechnikem. Libovolná osoba, která zná strukturu firmy, se může ukázat nebezpečná. Riziko se zvyšuje, jestliže firma vede ve svých spisech informace o zaměstnancích. A to, jak známo, dělá většina podniku.

V situaci, kdy zaměstnanci nejsou vyškoleni v rozeznávání sociotechniků, mohou odhodlané osoby, jako je například opuštěná slečna popsaná v následujícím příběhu, udělat věci, které se poctivým lidem zdají nemožné.

Příběh Douga

S Lindou se věci nevyvíjely moc dobře, takže když jsem poznal pocítil jsem, že právě ona je stvořená pro mě. Linda je trochu jakoby ... možná není slovo „nevyrovnaná" docela výstižné, ale když se rozčílí, tak to opravdu stojí za to.

Řekl jsem ji nejšetrněji, jak jsem jen svedl, že se musí vystěhovat, pomohl jsem jí sbalit se a dokonce jsem jí dal několik cédéček *Queenstryche* které byly ve skutečnosti moje. Jen co se vystěhovala, šel jsem do obchodu koupit novou vložku do vstupních dveří a vyměnil jsem ji ještě ten večer. Ráno jsem zavolal na telekomunikace a požádal je o změnu telefonního čísla a jeho utajení.

Nyní jsem se mohl věnovat Erin.

Příběh Lindy

Tak jako tak jsem byla připravena se odstěhovat. Nevěděla jsem jenom kdy. Ale nikomu se nelíbí, když dostane kopačky. Přemýšlela jsem, udělat, aby pocítil, jaký je blbec.

Bylo lehké domyslet si, o co jde. V jeho životě se objevila nějaká jiná ženská, jinak by po mně nechtěl, abych se tak rychle pakovala. Trošku počkám a začnu mu pozdě večer telefonovat. Poslední věc, kterou bude chtít v tu hodinu slyšet, je vyzvánění telefonu.

Vyčkala jsem do víkendu a zavolala jsem v sobotu okolo jedenácté večer. Ukázalo se však, že si nechal změnit telefonní číslo a nové nenechal zveřejnit. To jen dokazuje, jaký to byl mizera.

Už jsem to chtěla vzdát, ale jak jsem se hrabala v papírech, které mi podařilo vzít domů, než jsem skončila s prací v telekomunikační firmě, tak jsem našla potvrzenku na opravu Dougova telefonu zároveň s výpisem, na kterém bylo napsáno číslo kabelu a páru jeho příštroje. Telefonní číslo je možné kdykoli změnit, ale kabel od ústředny do baráku je pořád stejný. A když něco vím o fungování telekomunikační firmy, tak tyhle údaje stačí na získání telefonního čísla.

Měla jsem také seznam všech ústředen ve městě spolu s jejich adresami a telefonními čísly. Našla jsem číslo na centrálu blízko místa, kde jsem bydlela s tím pitomcem Dougem. Zavolala jsem tam, ale nikdo to samozřejmě nezvedl. Nikdy, když je člověk potřebuje, tak tam nejsou.

Po dvaceti sekundách mne napadl plán. Začala jsem obtelefonovávat všechny telefonní ústředny a nakonec jsem se dozvěděla, kde je operátor.Byl ale někde daleko od Dougovy ústředny, pravděpodobně s nohama na stole. Věděla jsem, že by nejspíš neudělal to, o co jsem ho chtěla požádat. Přišel tedy čas, abych zrealizovala nový plán.

„Tady je Linda, servisní centrum," ohlásila jsem se. „Máme tu neodkladno věc, přerušilo se spojení s nemocnicí. Poslali jsme tam technika, ale nemůže nic najít. Potřebujeme, abyste ihned zajel na ústřednu ve Websteru a zkontroloval, jestli jde tón ven z ústředny."

„Zavolám vám, až tam budete," dodala jsem ještě, protože jsem nemohla dopustit, aby telefonoval do servisního centra a sháněl se tam pomně.

Věděla jsem, že se mu nechce opustit vyhřáté místečko, vyjít na mráz, seškrabat led z předního skla a jet v noci po zledovatělých silnicích. Ale věc hořela a nemohl se příliš vymlouvat na jiné povinnosti.

Když jsem ho zastihla o tři čtvrtě hodiny později na ústředně ve Websteru, řekla jsem mu, aby zkontroloval kabel 29, pár 2481. Přistoupil k pultu, zkontroloval a řekl, že je signál. To mi říkat nemusel, věděla jsem to sama.

Povídám tedy: „Dobrá, tak zkuste VL" — tato zkratka znamená verifikace linky, což v podstatě znamená dotaz na číslo. To se dělá tak, že se volá na zvláštní číslo, které odečítá telefonní číslo na opačném konci drátu. Nemohl vědět, že toto číslo je chráněné nebo že bylo právě změněné, a tak udělal, o

co jsem ho požádala. A nadiktoval mi to číslo. Uslyšela jsem ve sluchátku, jak automat recituje další číslice. Perfektní — plán zafungoval.

„Problém tedy musí být někde venku, když na jejich dráty jde signál," říkám, když už mám číslo.

Poděkovala jsem mu a řekla, že na tom budeme ještě pracovat a popřála mu dobrou noc.

Tak skončil Dougův pokus ukrýt se přede mnou tím, že si nechá utajit číslo. Ted teprve začne zábava!

Analýza podvodu

Mladá žena — hrdinka příběhu — byla schopna získat hledanou informaci, aby se mohla pomstít, protože znala strukturu organizace: čísla telefonů, procedury a žargon telekomunikační firmy. Když toto všechno znala, byla schopna nejen získat neveřejný telefon, ale udělat to dokonce uprostřed zimní noci a vyslat přitom operátora na vynucenou jízdu přes město.

Poznámka Mitnicka
****
Když sociotechnik pozná pravidla, kterými se firma řídí, muže s uspěchem navázat kontakt s jejím zaměstnancem. Firma musí být přippravena na případné sociotechnické útoky ze strany stávajících nebo bývalých pracovníkú. Vnitřní kontroly mohou pomoci při zbavování se osob, které mají sklony k takovému chování. Ve většině případu bude neobyčejně těžké je odhalit. Jedinou smysluplnou ochranou je v tomto okamžiku zlepšení procedur ověřování totožnosti a zejména kontrola postavení pracovníka ve firmě, než se mu zpřístupní jakákoliv informace. Jde o ověření osoby, u které si nejsme jisti, že je v současnosti v naší firmě zaměstnaná. Organizace musí školit své zaměstnance, aby se dokázali ubránit takovému uskoku.
****

Pan generální chce...

Oblíbenou a vysoce účinnou formou zastrašení (zajisté díky její jednoduchosti) je ovlivňování lidí pomocí autority.

Už samotné jméno asistenta ze sekretariátu ředitelství může být dostačující. Soukromí detektivové a dokonce i lovci mozku to dělají často. Telefonují na ústřednu a žádají o spojení se sekretariátem. Když sekretářka zvedne telefon, říkají, že mají ten dokument, o který žádal pan ředitel, nebo když pošlou e-mail, jestli by ho mohla vytisknout, nebo ptají na číslo faxu. A jen tak mimochodem, jak že se jmenujete?

Pak telefonují jiné osobě a říkají: „Jeannie z kanceláře ředitele mi že vy byste mi mohla v té věci pomoci."

Uvádění jmen jiných zaměstnanců je obvykle používáno pro dojmu, že máme blízké kontakty s osobou ve firmě vysoce postavenou. Oběť ochotněji něco udělá pro člověka, který zná někoho, koho ona zná.

Pokud je cílem útočníka získání velmi důvěrné informace, může v průběhu rozhovoru použít podobnou metodu s úmyslem vyvolat u oběti určité emoce, například obavu před důtkou od šéfa. Zde je příklad.

Příběh Scotta

„Scott Abrams."

„Scotte, tady je Christopher Dalbridge. Právě mi telefonoval pan Biggley a byl, řekněme, poněkud nespokojený. Říkal, že před deseti dny poslal příkaz všem vašim lidem, aby shromáždili všechny výsledky průzkumu trhu pro naši analýzu. Nic jsme ještě nedostali."

„Průzkum trhu? Nikdo mi nic neříkal. Ze kterého jste oddělení?"

„Jsem z poradenské firmy, kterou si najal pan předseda a už máme velké zpoždění."

„Právě jdu na jednání, dejte mi telefonní číslo a ..."

Útočník ho nespokojeně přerušil: „Tohle mám říct panu Biggleymu? Heleďte, on potřebuje naše analýzy do zítřejšího rána a my nad nimi budeme muset sedět přes noc. Copak mu mám říct, že nemůžeme udělat analýzy, protože od vás nemáme podklady? Nebo mu to řeknete sám?"

Zloba šéfa může zkazit celý týden. Oběť nejspíš změní názor a rozhodne se, že bude možná lepší se tomu věnovat, než půjde na to jednání. Sociotechnik opět zmáčkl to pravé tlačítko, aby dostal to, co chtěl.

Analýza podvodu

Zastrašení pomocí odvolávání se na autority funguje zejména tehdy, když oběť zaujímá poměrně nízké postavení v podniku. Použití jména důležité osoby nejenže oslabuje přirozený odpor a podezíravost, ale ještě posiluje ochotu pomoci. Přirozená potřeba být užitečný roste, když se nám zdá, že osoba, které pomáháme, je důležitá nebo vlivná.

Sociotechnik ví, že tento podvod funguje nejlépe, když používá jméno osoby s vyšším postavením než bezprostředm nadřízený dané osoby. Tento trik je obtížný v případě malých firem. Útočníkovi se nehodí, když existuje velká pravděpodobnost, že jeho oběť bude mít příležitost poznamenat šéfovi marketingu: „Poslal jsem ten marketingový plán podniku tomu chlápkovi, co jste to po něm vzkazoval."

Což samozřejmě vyvolá reakci typu: „Jaký marketingový plán? Jaký chlápek?", která útok na firmu brzy odhalí.

Poznámka Mitnicka
****
Zastrašování způsobuje strach před trestem, což ještě více zvyšuje ochotu spolupracovat. Zastrašení muže rovněž zvyšovat obavy před zesměšněním nebo ztrátou šance na povýšení.
Je nutné lidi naučit, že pochybování o autoritách je nejen dovolené, ale v záležitostech, kdy může jit o bezpečnost firmy, dokonce potřebné. Školení o bezpečnosti informací by mělo učit lidi, jak zdvořile zpochybňovat autoritu tak, aby to nevyvolávalo konflikty. Co víc, samo vedení musí ostatní stále přesvědčovat k tomuto zpochybňování autorit. Jestli pracovník nebude mít istotu, že právě to se od něj očekává, brzy to přestane dělat.
****

Co o nás ví pojišťovák?

Rádi si myslíme, že státní úřady přechovávají informace o nás pod zámkem a mimo dosah lidí, kteří nemají oprávněnou potřebu jejich využívání. Ve skutečnosti ani federální úřady nejsou tak imunní proti průnikům jak bychom si to rádi představovali.

Telefon pro May Linn

Místo: Regionální pobočka Úřadu sociálního zabezpečení
Čas: úterý, 10:18
„Druhé oddělení, u telefonu May Linn Wang."
Hlas ze sluchátka zněl omluvně, skoro bázlivě.
„Paní Wang, tady je Arthur Arondale z kanceláře generálního inspektora. Mohl bych vás oslovovat paní May?"
„Jmenuji se May Linn," odpověděla.
„Tak tedy, May Linn, mám takovou záležitost. Mám tu nového pracovníka, který ještě nemá počítač a ted má udělat něco, co spěchá, a proto pracuje na mém. Dokážete si to představit? Vláda Spojených státu nemá v rozpočtu peníze, aby mohla tomu člověku koupit počítač. A můj šéf si teď myslí, že jsem si našel dobrou výmluvu a nenechá si to ani vysvetlit. Víte, jak to chodí."
„Vím, jak to chodí."
„Mohla byste mi pomoci a zadat rychlý dotaz do MCS?" zeptal a použil přitom název počítačového systému sloužícího k vyhledávání údajů o poplatníkovi.
„Samozřejmě, co byste potřeboval?"
„Potřeboval bych *alphadent* na jméno Joseph Johnson, narozený 7.4.1969" (*Alphadent* znamená hledání konta podle jména daňového poplatníka a data narození.)
Po krátké pauze se zeptala: „Co byste konkrétně potřeboval?"
„Jaké má číslo konta," zeptal se. Použil přitom žargonovou zkratku označující číslo sociálního pojištění.
May Linn přečetla číslo.
„Dobrá a teď bych potřeboval *numident* na toto číslo," řekl volající.
Byla to žádost o přečtení základních údajů o poplatníkovi. May Linn diktovala místo narození, dívčí jméno matky, jméno otce. Volající trpělivě poslouchal, když mu sdělovala také datum, kdy byla vydána karta a oblastní úřad, kde byla vystavena.
Potom poprosil o DEQY (zkratka označující „podrobný dotaz na příjmy") Namísto odpovědi uslyšel otázku: „Na jaký rok?"
„Rok 2001," odpověděl.
"celkem 190 286 dolarů, plátcem je Johnson MicroTech," odpověděla May Linn.
Jiné zdroje příjmů?"
„Ne, nejsou." Děkuji," řekl. „Moc jste mi pomohla."
Ještě se s ní pokusil dohodnout tak, aby mohl kdykoliv zavolat, když bude potřebovat informace a nebude mít přístup ke svému počítači. To je oblíbený trik sociotechniků: když najdou dobrý zdroj informací, pokoušejí se navázat takový kontakt, který by jim dovolil vrátit se ke stejné osobě. Díky budování vztahů se vyhýbají nutnosti vyhledávám nového záchytného bodu.
„Ale ne příští týden," řekla, protože jede do Kentucky na svatbu své sestry. Kdykoli jindy udělá, co bude moci.
Když pokládala telefon, May Linn se cítila dobře, že mohla kolegovi od fochu trochu pomoci.

Příběh Keitha Cartera

Soudě podle filmů a detektivních románů, je možná soukromý detektiv na štíru s etikou, ale zato má velké znalosti o způsobech dobývání informací, které ho zajímají, od různých lidí. Za tímto účelem používá nelegální metody a obvykle o vlásek uniká zatčení. Pravda je taková, že většina soukromých detektivů provozuje svojí činnost úplně v souladu s právem. Protože mnozí z nich začínali kariéru jako policisté, dokonale si uvědomují, co je zákonné a co naopak ne a nemají velké pokušení překračovat tuto hranici.

Je tu však jedno „ale". Někteří detektivové opravdu odpovídají vzoru představovanému v detektivkách. V branži jsou známí jako „obchodníci s informacemi" — je to eufemistické označení lidí, kteří za vás ochotně poruší zásady. Vědí, že některé zakázky lze vykonat rychleji a snáze, když se půjde zkratkou. Skutečnost, že tyto zkratky nejsou v souladu se zákony a mohou je stejně tak dobře přivést na pár let za mříže, se je nezdá příliš odrazovat.

Zato renomovaní detektivové — ti, kteří si pronajímají honosné kanceláře v bohatých městských čtvrtích — takové úkoly nevykonávají osobně. Obvykle si na to najmou nějakého obchodníka s informacemi.

Člověk, kterého budeme nazývat Keith Carter, se jako detektiv otázkami etiky příliš nezatěžoval.

Byla to typická záležitost druhu: „Kam schoval peníze?". Otázka tohoto typu zazněla z úst bohaté dámy, která chtěla vědět, kam její muž ukryl její hotovost. Keith Carter si vždycky kladl otázku, proč se ženy s penězi vdávají za muže, kteří je nemají, ale nikdy si nedokázal odpovědět.

Tentokrát se muž jmenoval Joe Johnson a s penězi uměl zacházet. Byl to velmi inteligentní člověk, který založil firmu působící v oblasti moderních technologií. Investoval do ní deset tisíc dolaru půjčených od rodiny své ženy, přičemž vybudoval firmu, která měla hodnotu milionů dolarů. Podle manželčina právníka, který se zabýval jejich rozvodem, byl majetek pečlivě ukryt a bylo třeba ho nalézt.

Keith si vybral za startovní místo Úřad sociálního zabezpečení, kde si dal za cíl získat zde uložená data na jméno Johnson. Mezi nimi se mohlo nacházet mnoho užitečných informací. Když už měl tyto údaje, mohl se vtělit do sledovaného muže a zaútočit na banky, makléřské kanceláře a podobné instituce, aby se dozvěděl, co bylo třeba.

Keith si tentokrát nastavil laťku trochu výš, chtěl nejen získat z Úřadu sociálního zabezpečení informace o Joe Johnsonovi, ale zařídit si žádežitosti takovým způsobem, aby měl v oddělení stálý zdroj informací, ze kterého by mohl kdykoli čerpat.

> Sociální nezabezpečení
> **********
> Je to neuvěřitelné, ale Úřad sociálního zabezpečení uveřejnil na síti kopii dokumentace programu, který používají jeho pracovníci, plnou informací, které kromě toho, že jsou užitečné pro úředníky, mají ohromnou cenu pro sociotechniky. Dokumentace obsahuje zkratky, žargon a způsoby formulace dotazů, které byly využity v tomto příběhu.
>
> Má někdo ze čtenářů zájem dozvědět se, jak pracuje Úřad sociálního zabezpečení? Stačí si vyhledat tyto informace přes Google nebo vyťukat adresu *http://policy.ssa.gov/poms.nsf/* do prohlížeče. Pokud si ještě nikdo z úřadu nepřečetl tuto knížku a obsah stránky nebyl odstraněn, lze tam nalézt podrobné informace o tom, jaké údaje smí úředník zpřístupnit policistovi, nebo, prakticky vzato, každé osobě, která je schopna úředníka přesvědčit, že je policista.
> **********

První telefonát uskutečnil do místního oblastního úřadu na bezplatnou linku 0800, na kterou obvykle volají všichni normální klienti a která je uvedená v místním telefonním seznamu. Když úředník přijal hovor, Keith ho poprosil o spojení s oddělením reklamací. Po chvilce čekání uslyšel na druhé straně hlas. V tom okamžiku si nasadil novou masku:

„Ahoj," řekl. „Tady je Gregory Adams, oblastní úřad 329. Zkouším se dovolat inspektorovi, ke kterému patří konto končící na 6363, ale ozývá se mi tam fax.

„To je druhé oddělení," odpověděl úředník, vyhledal číslo a sdělil ho Keithovi.

Keith vytočil číslo. Když May Linn zvedla telefon, představil se jako úředník z kanceláře hlavního inspektora a pověděl ji historku o tom, jak byl

pozbaven počítače. May Linn mu sdělila informace, které hledal a přislíbila mu pomoc, kdyby něco podobného ještě někdy potřeboval.

Analýza podvodu

Účinnost představené metody se opírá o hru s pracovníkovým soucitem, který byl vyvolán historkou o tom, jak osoba představující se jako úředník byla zbavena počítače a že „mého šéfa nezajímají takové výmluvy". Lidé v práci nedávají moc často najevo své pocity. Když už to ale udělají, mohou zapomenout na používání standardních obranných mechanismů zabraňujících sociotechnickým útokům. Emocionální finta stylu „mám potíže, mohl bys mi pomoci?" stačila, aby byla partie vyhraná.

Útočníkovi by se nemuselo podařit získat informace od jednoho u úředníků, kteří vyřizují telefonáty zvenku. Tento typ útoku, který použil Keith, funguje jedině tehdy, když číslo osoby uvnitř není všeobecně dostupné. Taková osoba očekává, že volající je osoba „odsud". To je další příklad zabezpečení z dob prohibice.

Zde jsou kroky, které učinily tento útok účinným:

- znalost telefonního čísla do oddělení,
- znalost terminologie — *numident*, *alphadent* a *DEQY*,
- prezentace sama sebe jako úředníka z kanceláře hlavního inspektora, která je známá všem pracovníkům federální správy jako vlivný vládní vyšetřovací úřad.
  Díky tomu se útočník jevil jako spojený s mocí.

Sociotechnici, zdá se, vědí, jakým způsobem formulovat své žádosti, aby se jich nikdo neptal: „A proč telefonujete právě mně?" — dokonce ani tehdy, když by bylo logické zatelefonoval úplně jiné osobě v úplné jiném oddělení. Možná už samotná skutečnost přerušeni rutiny takovýmto telefonátem a chvilkové odtrženi od povinností, aby se mohlo někomu pomoci, odsouvá postřehy tohoto druhu do pozadí.

útočníka z tohoto incidentu neuspokojuje pouhé získání právě potřebné informace, ale chtěl by navázat kontakt, aby mohl získaný zdroj informací využívat i v budoucnu. Jinak by mohl použít obvyklou záminku hrající na soucit, například: „Vylila se mi káva na klávesnici.“ To by zde nestačilo. Klávesnici je možné vyměnit během jednoho dne. Proto ta historka o kolegovi, který pracuje na jeho počítači, kterou by mohl uplatňovat několik týdnů, aniž by vzbuzoval podezření. „No už jsem si myslel, Že včera dostane svůj počítač. Přivezli jeden, ale dali ho někomu jinému, komu se podařila nějaká transakce. Takže ten blbec stále chodí na můj počítač."

Ó já chudáček! Stále potřebuji pomoci — funguje to vždycky.

Jeden prostý telefonát

Jeden z hlavních problémů útočníka je zdůvodnění své žádosti — musí vymyslet něco typického, něco, co je součástí normálního pracovního dne oběti, něco, co od ní nevyžaduje přílišného úsilí. Podobně jako u jiných věcí ze života to jednou může být hračka, ale jindy může vymyšlení rozumného důvodu zabrat celý den.

Telefon Mary H.

Místo: Účtárna firmy Mauserby & Storck, New York
Čas: pondělí, 23. listopadu, 7:49

Pro většinu lidí je práce v účtárně dřina. Hledění do sloupců čísel je obvykle pokládáno za asi tak příjemné jako vrtám zubů. Naštěstí to tak nebere každý. Příkladem budiž Mary Harris, která je samostatnou účetní a považuje svou práci za poutavou a určitě je částečně z tohoto důvodu považovaná za nejoddanějšího pracovníka tohoto oddělení ve firmě.

Jednoho pondělka se objevila v práci dříve, protože ji čekalo hodně práce. K jejímu překvapení zazvonil telefon; když zvedla sluchátko a představila se, ozval se mužský hlas:

„Dobrý den, tady je Peter Sheppard. Jsem z Arbuckle Support - firmy, která zajišťuje technickou správu vaší společnosti. Záznamenali jsme během víkendu několik stížností od lidí, kteří u vás měli problémy s počítači. Tak jsem si řekl, že bych se na to mohl podívat, ještě přijdou ráno lidi do práce. Měla jste nějaké problémy s počítačem s připojením do sítě?"

Odpověděla, že ještě neví. Zapnula počítač a zatímco nabíhal, volající vysvětloval, o co mu jde.

„Chtěl bych provést s vaší pomocí několik testů," řekl. „Na své obrazovce vidím, jaké klávesy mačkáte a chci se ujistit, jestli to síť interpretuje správně. Proto mi vždycky, když stisknete nějakou klávesu, prosím, řekněte, jakou, abych si to mohl zkontrolovat, jestli se u mne objeví stejný znak, ano?"

Představila si poruchu počítače a den plný frustrace, kdy by s prací nepohnula ani o píď dopředu, proto ji potěšilo, že jí ten muž chce pomoci. Po chvíli řekla:

„Mám obrazovku s přihlašováním a za chvíli napíšu své uživatelské jméno.Píši:M...A...R...Y...D..."

„Zatím je všechno v pořádku," odpověděl. „U mě je to stejné. A teď, prosím, napište heslo, ale neříkejte mi ho. Nikdy nesmíte nikomu říct své heslo. Dokonce ani lidem z technické pomoci. Já vidím jen hvězdičky — vaše heslo je chráněné, proto ho nemohu vidět."

Nic z toho nebyla pravda, ale Mary to znělo rozumně. Potom ještě řekl:

„Dejte mi, prosím, vědět, až počítač nastartuje."

Když mu řekla, že už jede, poprosil ji, aby spustila dvě aplikace, které obvykle používá. Nastartovaly bez problémů.

Mary si oddechla, že se zdá všechno v pořádku. Peter řekl:

„Zatím je všechno v pořádku. Jsem rád, že budete dnes moct bez potíží pracovat. Ještě jedna věc," pokračoval. „Právě jsme nainstalovali aktualizaci programu na změnu hesla. Mohla byste mi ještě věnovat pár minut, abych si mohl ověřit, že funguje?"

Mary mu byla vděčná za pomoc, kterou jí poskytl a bez rozmyslu souhlasila. Peter ji provedl kroky instalace aplikace, která umožňuje uživateli změnu hesla — to je standardní prvek operačního systému Windows 2000.

„Teď tam napište heslo," řekl jí. „Jen ho, prosím, neříkejte nahlas."

Když to udělala, Peter poprosil:

„Až se zeptá na nové heslo, napište tam zatím „test123" a potom)estě jednou do druhého kontrolního okénka a stiskněte Enter."

Pottom ji provedl přes odhlášení se od serveru. Poprosil ji, aby několik minut počkala a přihlásila se, tentokrát s novým heslem. Všechno fungovalo perfektně. Peter se zdál být velmi spokojený a provedl ji znovu změnou hesla na původní nebo úplně nové. Ještě jednou ji upozornil, aby mu heslo neříkala.

"Výborně," řekl Peter. „Jsem rád, že je všechno v pořádku. Kdyby byly nějaké problémy, klidně nám zavolejte do Arbuckle. Já jsem obyčejně v terenu, ale každý, kdo zvedne sluchátko, vám bude schopen pomocí."

Mary poděkovala a rozloučila se.

Příběh Petera

Drby o Peterovi se rozšířily rychle, několik lidí z jeho čtvrti, kteří s ním chodili do školy, slyšelo, že se stal něčím jako počítačovým

kouzelníkem a častokrát dokázal najít užitečné informace, které obyčejný člověk nemohl nijak získat. Když za ním přišla Alice Conrad s prosbou o službičku, nejprve odmítl. Proč by jí měl pomáhat? Kdysi se ji pokusil pozvat na schůzku, ale chladně ho odbyla.

Jeho odmítnutí ji vůbec nepřekvapilo, prohlásila, že i tak moc nevěřila že by byl schopný něco takového udělat. To byla výzva. Protože si byl jistý, že je schopný to dokázat, změnil názor a souhlasil.

Alici byla nabídnuta smlouva na poradenství pro marketingovou agenturu, ale podmínky se jí nezdály příliš dobré. Než však půjde zádat o lepší, chtěla se dozvědět, jaké podmínky jsou napsané v jiných smlouvách.

Takto popisuje události sám Peter:

* * *

Neřekl jsem Alici, že obvykle posílám pryč lidi, kteří chtějí, aby ně něco udělal a nevěří, že se mi to podaří, ačkoliv já jsem přesvědčen že úkol je jednoduchý. Nebo aspoň proveditelný — tento úkol totiž snadný nebyl.

Zato jsem jí mohl ukázat své schopnosti.

Hned v pondělí po půl osmé ráno jsem zatelefonoval do agentury, zvedla to recepční. Řekl jsem jí, že jsem z firmy, která se stará o jejich penzijní plány a musím mluvit s někým z účtárny. Zeptal jsem se, jestli se už někdo z tohoto oddělení objevil v práci. Odpověděla:

„Myslím, že jsem před pár minutami viděla Mary, jak přicházela. Zkusím vás na ni přepojit."

Když Mary zvedla sluchátko, moje historka s počítači ji měla vystrašit tak, aby byla ochotna ke spolupráci. Jakmile jsem ji provedl změnou hesla, rychle jsem se nalogoval do systému pomocí stejného dočasného hesla které jsem jí doporučil napsat: „test123".

Přišel čas na mistrovský kousek — nainstaloval jsem malý prográmek který mi umožnil přístup do firemního systému v libovolnou chvíli pomocí mého vlastního hesla. Po ukončení rozhovoru s Mary bylo mým prvním krokem vymazání stop po mé přítomnosti v systému. To bylo jednoduché. Jakmile se mi podařilo rozšířit práva v systému, stáhl jsem si program *clearlogs*, který jsem našel na adrese věnované otázkám bezpečnosti www.ntsecurity.nu .

Nyní bylo třeba trochu zapracovat. Spustil jsem vyhledávání všech dokumentů, které obsahovaly slovo „smlouva" v názvu souboru a stáhl jsem si nalezené soubory. Když jsem hledal dál, narazil jsem na zlatou žílu. Adresář obsahující zprávy o příjmech poradců. Podařilo se mi stáhtnou všechny soubory se smlouvami a seznam platů.

Alice si teď mohla prohlédnout smlouvy a ověřit si, jaké částky byly vypláceny jiným konzultantům. Ostatně, ať si tu otročinu udělá sama. Já jsem zařídil to, o co mně žádala.

Z cédéček, kam jsem data zapsal, jsem vytiskl část souborů, abych jí dokázal, co se mi podařilo získat. Pozvala mne na oběd. Měli byste vidět její výraz, kdy si prohlížela štos papírů.

„To není možné," říkala. „To není možné."

Nevzal jsem s sebou cédéčka. Nechal jsem je u sebe jako návnadu. Řekl jsem jí, aby se pro ně někdy stavila. Doufal jsem, že mi možná bude chtít projevit vděčnost za to, co jsem pro ni udělal.

Analýza podvodu

Peterův telefon do marketingové agentury je příklad nejzákladnější sociotechnické strategie — jednoduchá akce, která nevyžaduje skoro žádnou přípravu. Jak bylo vidět, zafungovalo to napoprvé a trvalo to pouze několik minut.

Navíc Mary, oběť útoku, neměla žádný důvod si myslet, že byla nějakým způsobem podvedena a psát hlášení nebo vyvolat poplach.

Plán zafungoval díky třem sociotechnickým taktikám. Nejprve získal Maryinu ochotu ke spolupráci, když v ní vyvolal strach před možnou havárií počítače. Potom ji věnoval trochu času, když jí řekl, aby spustila dvě aplikace, aby měla jistotu, že všechno funguje a při té příležitosti s ní navázal kontakt a pocit sounáležitosti. A nakonec získal její další ochotu pomoci, když využil její vděčnost za pomoc projevenou během kontroly počítače.

Když jí Peter opakoval, že by neměla prozrazovat své heslo nikomu, dokonce ani jemu, Peter ji účinně a zároveň nenápadně přesvědčil, že on sám dbá o bezpečnost firemních dat. To zvýšilo její jistotu, že byl tím, za koho se prohlašoval. Vždyť chránil ji i její firmu.

> *Poznámka Mitnicka*
> **********
> Je ohromující, jak jednoduše dokáže sociotechnik přesvědčit lidi, aby udělali různé věci vzbuzováním emocionálních reakcí. Opírá se přitom o vyvolávání automatických reakcí, vycházejících z psychologických zásad, a využívá myšlenkové zkratky, které používají lidé, když si myslí, že osoba, se kterou hovoří, je na jejich straně.
> **********

Razie

Představme si takovou situaci: Vláda se chystá nastražit past na člověka jménem Arturo Sanchez, který přes Internet zadarmo distribuuje filmy. Hollywoodská studia tvrdí, že porušuje jejich autorská práva. Sanchez odpovídá, že se je pouze pokouší přesvědčit, aby rozpoznali v Internetu cenné odbytiště a učinili nějaké kroky s cílem zpřístupnit tímto způsobem filmy lidem, kteří by je chtěli vidět. Upozorňuje — správně — že by to mohl být pro studia gigantický zdroj příjmů, dosud jimi úplně přehlížený.

Máte povolení k prohlídce?

Jednoho večera, když se vracel pozdě večer domů, pohlédl na okna svého bytu a všiml si, že světla jsou zhasnutá, přestože vždy, když odchází nechává některá rozsvícená.

Bušil na sousedovy dveře tak dlouho, až ho vzbudil. Dozvěděl se od něj, že v budově byla policie, ale nařídili mu stát dole a on si není jistý, do kterého bytu vešli. Věděl jen, že při odchodu vlekli nějaké těžké předměty, ale těžko říct co, protože byly zabalené. Nikoho nezatkli.

Arturo zkontroloval svůj byt. Špatná zpráva byla, že tam ležel dopis od policie nařizující mu, aby během tří dnů zavolal na policii a domluví se k výslechu. Ještě horší zpráva byla, že zmizely jeho počítače.

Arturo vypadl ze svého bytu. Chtěl zůstat u kamaráda. Po celý čas ho trápila nejistota: kolik toho policie ví? A nejde snad o něco jiného, o něco, co může snadno vysvětlit, aniž by musel opustit město?

Než začneme číst dál, zamysleme se: Je možné si představit způsob, jak poznat, co o nás ví policie? Za předpokladu, že nemáme žádné známé ani na policii ani na prokuratuře? Je nějaký způsob, jak by obyčejný občan mohl získat takovou informaci? I když je sociotechnikem?

Jak přechytračit policii

Atruro uspokojil svůj hlad po informacích následovně. Nejprve našel číslo nejbližší pošty, zavolal tam a poprosil o číslo faxu.

Potom zatelefonoval na oblastní prokuraturu a požádal je o spojení s archivem. Zde se představil jako vyšetřovatel z Lake County a řekl, že by chtěl hovořit s osobou, která má na starosti aktuální povolení k domovní prohlídce.

„To jsem já," řekla úřednice na druhé straně.

„Skvělé," odpověděl. „Protože minulou noc jsme dělali prohlídku u jednoho podezřelého a hledám přísežné prohlášení."

„Řadíme je podle adresy," řekla.

Uvedl jí adresu, na což mu vzrušeně řekla:

„Aha! Znám ho! To je ten s těmi filmy."

„Ano, to je on," odpověděl. „Hledám to prohlášení a kopii povolení."

"Mám je v ruce."

"Výborně," řekl. „Jsem v terénu a za čtvrt hodiny mám schůzku se zvláštními službami (Secret Service) kvůli této záležitosti. Byl jsem poslední dobou nějak roztržitý, že jsem zapomněl ty papíry doma a nijak už mestihnu si tam pro ně dojet. Mohl bych od vás dostat kopii?"

„Samozřejmě. Žádný problém. Udělám kopie a můžete se pro to stavit."

„Skvělé," řekl. „To je bezva, ale je tu ještě jedna malá potíž. Jsem na druhém konci města. Mohla byste mi to odfaxovat?"

To trochu problém byl, ale dal se vyřešit.

„Nemáme tu na oddělení fax," řekla. „Ale jeden, který mohu používat, je dole v kanceláři zapisovatelů."

„Tak já tam zavolám a domluvím to s nimi."

Úřednice od zapisovatelů řekla, že to s radostí udělá, ale musí vědět, kdo to zaplatí. Potřebovala účetní kód.

„Zjistím kód a hned zavolám," přislíbil.

Pak zavolal na sekretariát oblastní prokuratury, představil se jako policejní důstojník a zeptal se přímo recepční:

Jaký je účetní kód kanceláře oblastní prokuratury?"

Bez váhání mu ho sdělila.

Další telefonát úřednici u zapisovatelů a sdělení účetního kódu bylo dobrou záminkou k další manipulaci: poprosil úřednici, aby skočila nahoru a vyzvedla xerokopie dokumentů, které měly být odfaxovány.

> *Poznámka Mitnicka*
> **********
> Jak je to možné, že sociotechnici znají podrobnosti fungování tolika institucí, včetně policie a prokuratury, praktiky telekomunikačních firem, organizaci různých podniku a detailní údaje týkající se oblastí, které se hodí během útoků, tedy telekomunikací a počítačů? Protože to je jejich práce. Tyto znalosti rozhodují o hodnotě sociotechnika, protože ho dělají přesvědčivým.
> **********

Zametání stop

Arturo musel ještě udělat pár věcí. Vždycky existuje možnost, že někdo podfuk vycítí a až přijede na poštu, setká se tam se dvěma detektivy v civilu, kteří předstírají, že se zabývají něčím úplně jiným až do chvíle, kdy se někdo zeptá na ten fax. Počkal chvíli a pak zavolal znovu do kanceláře zapisovatelů, aby se ujistil, že fax byl vyslán. Zatím šlo všechno podle plánu.

Pak zavolal na jinou poštu a povídal historku o tom, jak je „...spokojený se službami a že by v této souvislosti chtěl napsat vedoucímu poděkování. Mohli byste mi říci, jak se jmenuje?" Když měl tuto informaci, zavolal na první poštu a řekl, že chce mluvit s vedoucím směny. Když se ve sluchátku ozval mužský hlas, Arturo řekl:

„Dobrý den, tady je Edward z pobočky 628 v Hartfieldu. Naše vedoucí, paní Anna, mi řekla, abych vám zavolal. Máme tu jednoho zákazníka, který je už dost rozčilený. Někdo mu totiž sdělil číslo faxu jiné pošty. Čeká tu na důležitý dokument, ale číslo, které obdržel, je vaše."

Vedoucí slíbil, že někdo z jeho lidí ihned ten fax najde a odešle do Hartfieldu.

Když došel fax, Arturo už čekal na druhé poště. Jakmile ho měl v rukou, zavolal zapisovatelům, aby poděkoval úřednici a řekl:

„Ty kopie nemusíte nosit zpátky nahoru. Můžete je klidně vyhodit.“

Potom zatelefonoval vedoucímu směny první pošty a také řekl, že je možné kopie faxu vyhodit. Tak nezůstanou žádné stopy po tom, co se stalo, kdyby se tam snad náhodou někdo objevil a kladl otázky. Sociotechnici vědí, že opatrnosti nikdy nezbývá.

Když věc takto zařídil, Arturo dokonce nemusel platit na první poště za příjem faxu a jeho vyslání na druhou poštu. Kdyby se ukázalo, že se v první pobočce objevila policie, Arturo by stihl vyzvednout fax v druhé pobočce a zmizet, než by stačili někoho poslat.

A konečně závěr. Přísežné prohlášení a povolení k domovní prohlídce ukazovaly, že policie má dobře zdokumentované důkazy o tom, že Arturo nelegálně kopíroval filmy. Právě to chtěl vědět. O půlnoci dne už překračoval hranice státu. Utíkal, aby na jiném místě a s novou totožností začal znovu svou činnost.

Analýza podvodu

Lidé, kteří pracují v kancelářích oblastních prokuratur, mají stálý kontakt s policejními důstojníky. Odpovídají na jejich dotazy, zařizují pro ně různé věci, přebírají zprávy. Osoba, která má dost drzosti, aby zavolala a představila se jako policejní důstojník, zástupce šerifa apod. je většinou uznána za „naši". Pokud se příliš brzy neprozradí neznalostí terminologie, nervozitou, váháním při rozhovoru nebo není jiným způsobem nepřesvědčivá, dokonce nebude obvykle muset ani odpovídat na nejakou ověřovací otázku. To se právě stalo v popisovaném příběhu u dvou různých pracovníku.

Jako obvykle vyžadovalo získám účetního kódu jeden telefonát. Arturo hrál na city, když vyprávěl pohádku, že „za čtvrt hodiny mám schůzku se zvláštními službami kvůli této záležitosti. Byl jsem poslední dobou nějak roztržitý, že jsem zapomněl ty papíry doma a nijak už nestihnu si tam pro ně dojet. Mohl bych od vás dostat kopii?" Úřednici se ho zželelo a ochotně mu pomohla.

Másledovně Arturo využil ne jeden, ale rovnou dva poštovní úřady a tím si zajistil dostatečné zabezpečení pří přebírání faxu. Jiná varianta této taktiky by zajistila, že vysledování Artura by bylo ještě obtížnější. Namísto toho, aby nechal fax poslat na druhou poštu, mohl útočník uvést něco, co vypadá jako číslo faxu, ale ve skutečnosti je to bezplatná internetová služba umožňující příjem faxů a jejich zasílání na uvedenou e-mailovou adresu. Tímto způsobem mohl fax dorazit přímo na počítač útočníka, který by se tak vyhnul nutnosti osobní přítomnosti na místě, kde by mohl být později identifikován. E-mailovou adresu a použité číslo faxu by bylo možné po skončení záležitosti zrušit.

> Poznámka Mitnicka
> **********
> Skutečnost je taková, že nikdo z nás není imunní proti úskokům dobrého sociotechnika. V každodenním životě nemáme vždy dost času na rozhodování, dokonce ani v záležitostech, které jsou pro nás důležité. Komplikované situace, nedostatek času, emocionální stav nebo duševní vyčerpání nás mohou snadno rozptýlit. Používáme tedy myšlenkové zkratky, kdy se rozhodujeme bez důkladné a úplné analýzy informací, reagujeme

automaticky. Týká se to hlavně federálních úředníků a policistů. Jsme jenom lidé.
****

Záměna rolí

Mladík, kterého nazvěme Michael Parker, byl jedním z těch, kteří si příliš pozdě uvědomili, že šanci na lépe placenou práci mají jen lidé s vyšším vzděláním. Měl sice možnost chodit na místní univerzitu za snížené školné a vzít si půjčku na vzdělání, ale znamenalo by to pracovat po nocích a o víkendech, aby bylo z čeho zaplatit činži, jídlo, benzín a pojistní auta. Michael však vždy hledal nějakou zkratku, takovou, která by ho rychleji dovedla k cíli při menší námaze. Protože ho odmalička fascinovaly počítače a zkoumal, jak fungují, napadlo ho, že by si sám mohl "vytvořit" diplom inženýra — informatika.

Absolvent

Vymyslel, že by se mohl nabourat do počítačového systému státní univerzity, najít data někoho, kdo právě ukončil studia s dobrým průměrem, zkopírovat je, zaměnit osobní údaje za své a vrátit zpátky do dat absolventů daného roku. Po chvilce si uvědomil, že přece musejí existovat ještě jiné dokumenty studentů, kteří prošli školou — dokumenty o výplatách stipendií, zápisy na kolejích a kdoví, co ještě. Samotné stvoření dat dokumentujících průběh studia nemusí stačit.

Když o tom nějakou dobu přemýšlel, došel k závěru, Že by mohl dosáhnout svého cíle, kdyby našel studenta stejného jména, který získal titul inženýra informatiky někdy během posledních deseti let. Pokud se někdo takový najde, bude stačit na přihláškách vyplňovat číslo sociálního zabezpečení druhého Michaela Parkera. Pak každá firma, která si bude ověřovat, jestli osoba toho jména a čísla sociálního zabezpečení získala titul inženýra, obdrží kladnou odpověd.

(Možná to není každému zřejmé, ale Michael věděl, že může klidně uvést číslo pojištění nalezeného absolventa v přihlášce. Později, až bude přijatý, uvede na formulářích, které vyplňuje nově přijatý pracovník, své vlastní číslo. Ve většině firem nikoho nenapadne zkontrolovat, jestli nový pracovník udával stejné číslo během ucházení se o práci.)

Počítač

Jak najít Michaela Parkera v univerzitních dokumentech? Náš hrdina to udělal následovně:

Šel do hlavní knihovny univerzitního kampusu, usedl k počítači a otevřel si hlavní intemetovou stránku univerzity. Potom zavolal na studijní oddělení. Vůči osobě, která vzala telefon, použil jeden z nám už známých sociotechnických triků.

„Volám z výpočetního centra, děláme změny v konfiguraci sítě a chceme se ujistit, jestli u vás nezpůsobily potíže s přístupem. K jakému serveru jste připojeni?"

„Serveru?" zeptal se hlas ve sluchátku.

„K jakému počítači se hlásíte, když chcete vyhledávat informace o studentech?"

Obdržel odpověď: *admin.rnu.edu*. Už měl jméno počítače, na kterém jsou uloženy dokumenty o studentech. Byl to první střípek do mozaiky – věděl už, kam se musí dostat.

Vložil tuto adresu do počítače a obdržel odpověď, kterou očekával - firewall blokoval přístup. Spustil tedy program, který zjišťoval, jestli je možné spojit se na tomto serveru alespoň s nějakou službou, a našel otevřený port služby Telnet. Ta umožňuje připojení jednoho počítače k druhému tak, jako by ten první byl vzdáleným terminálem druhého. Teď potřeboval pouze standardní uživatelské jméno a heslo.

Znovu zavolal na studijní a všímal si, jestli telefon nezvedne stejná osoba. Tentokrát to byla nějaká žena. Opět se představil, jako že volá z univerzitního výpočetního centra. Řekl, že instalují nový systém studentské evidence. Poprosil o službičku, která měla spočívat v tom, že se pokusí přihlásit k novému systému a vyzkoušet, jestli správně funguje přístup k záznamům o studentech. Sdělil jí IP adresu, na kterou se měla připojit a provedl ji celým procesem.

Ve skutečnosti to byla adresa počítače, u kterého Michael seděl v univerzitní knihovně. Použil fintu popsanou v sedmé kapitole a vytvořil falešnou přihlašovací obrazovku, která vypadala podobně jako ta, na kterou byla žena zvyklá při vstupu do systému obsahující dokumenty o studentech.

„Nefunguje to," oznámila. „Po celou dobu to říká *login incorrect*." Simulátor však zaznamenal údaje o klávesách, které stiskla při psaní uživatelského jména a hesla přímo do počítače, u kterého seděl Michael. Povedlo se. Řekl:

„Aha. Některá konta nebyla ještě v novém systému založena. Udělám to za chvíli a ještě vám brnknu."

Protože si dával pozor, aby celá věc skončila hladce, nezapomněl jí později znovu zatelefonovat, jak slíbil, a povědět, že pokusný systém nefunguje tak, jak by měl a že se ozvou buď jí nebo někomu jinému z jejich oddělení, až se jim podaří problém vyřešit.

Studijní oddělení přichází s pomocí

Ted už Michael věděl, na jaký systém se musí dostat a měl na něj uživatelské jméno i heslo. Jaké má však zadat příkazy, aby našel soubory týkající se absolventů informatiky, odpovídajícího jména a data ukončení studií? Studijní evidence byla vytvořená na škole a přizpůsobená speciálním požadavkům školy a studijního oddělení. Byl s tím spojený nestandardní způsob zadávání dotazů.

První krok při odstraňování poslední překážky znamenal najít osobu, která by mohla provést vyhledávání v databázi. Znovu zavolal do studijního oddělení a znovu jinému pracovníkovi. Tentokrát řekl, že volá z děkanátu a zeptal se:

„Komu mám zavolat, když mám problémy s přístupem do databáze studentů?"

O několik minut později už hovořil se správcem databáze a hrál scénu se soucitem v hlavní roli: „Tady je Mark Sellers ze studijího oddělení. Jsem tu nový a potřeboval bych trochu pomoci. Omlouvám se, že vám volám, ale všichni šli na nějakou poradu a já jsem tu zůstal sám. Potřeboval bych seznam všech absolventů informatiky s titulem inženýra z let 1990 až 2000. Musím to mít hotové do konce dne a pokud se mi to nepovede, možná tu nebudu pracovat dlouho. Pomohl byste mi v nouzi?"

Pomáhání lidem bylo součástí obvyklých povinností administrátora, proto se vybavil velkou dávkou trpělivosti a provedl Michaela celým procesem.

Ke konci rozhovoru už měl Michael úplný seznam absolventů z posledních jedenácti let. Během několika minut našel dva Michaely Parkery. Vybral si jednoho z nich a přečetl si jeho číslo sociálního pojištění i ostatní informace o něm z databáze.

Od této chvíle byl Michaelem Parkerem s titulem inženýra informatiky, získaným po ukončení studia s vyznamenáním v roce 1998.

Analýza podvodu

Při tomto útoku byl použit úskok, který jsme ještě neprobírali: útočník prosí správce databáze, aby s ním prošel proces obsluhy programu, který neznal. Neobyčejně účinné obrácení rolí. To je, jako kdyby poprosil prodavače, aby mu pomohl do auta s krabicí, ve které jsou zabalené věci ukradené v obchodě.

Poznámka Mitnicka
****
Uživatelé často nemají ponětí o nástrahách spojených s používáním sociotechniky ve světě technologií. Mají přístup k informacím, nemají však znalosti o ohrožení bezpečnosti. Sociotechnik si vybírá jako oběť osobu, která nezná cenu hledané informace. Taková osoba pro nás ochotněji něco udělá..
****

Prevence

Soucit, pocit viny a zastrašení jsou emoce často využívané sociotechniky. Způsob jejich využívání demonstrují zde uvedené příběhy. Co můžeme udělat, abychom se vyhnuli útokům tohoto typu?

Ochrana dat

Některé příběhy této kapitoly podrobně ukazují nebezpečí spojené s posíláním souborů osobě, kterou neznáme, dokonce i když je ta osoba zaměstnancem (nebo se nám to tak alespoň zdá) a dokument je posílán uvnitř na e-mailovou adresu patřící do firemní domény nebo na fax, který je umístěn ve firmě.

Bezpečnostní pravidla firmy musí jednoznačně definovat prostředky ochrany během zpřístupňování cenných dat osobě, kterou odesílatel nezná osobně. Musí být určeny procedury, jak předávat soubory s důvěrnými daty. Když žádost o data přijde od osoby, kterou osobně neznáme, musejí být stanoveny kroky, které musí pracovník uplatnit v souvislosti s verifikací této osoby, s ohledem na různé úrovně verifikace v závislosti na stupni citlivosti dat. Zde je pár řešení k posouzení:

- zavést zásadu poskytování informací pouze známým osobám;
- uchovávat záznamy o transakcích pro každou osobu nebo oddělení;
- udržovat seznam osob, které byly proškoleny v oblasti procedur a mají výhradní oprávnění posílat ven důvěrné informace;
- jestliže má žádost o údaje písemnou formu (e-mail, fax nebo pošta), uplatňovat dodatečné kroky, aby se ověřilo, jestli tato žádost skutečně pochází od toho odesílatele, který je uveden.

0 heslech

Pracovníci, kteří mají přístup k důvěrným informacím — což je dnes prakticky každý, kdo má přístup k počítači — si musejí uvědomit, že dokonce i chvilková změna hesla může vést k velkému ohrožení bezpečnosti.

Skolení v oblasti bezpečnosti se musí zabývat také hesly, zejména tím, kdy a jak je měnit, z čeho se skládá přípustné heslo a jaké riziko se srývá v angažování jiných osob do tohoto procesu. Skolení musí pracovníky důrazně upozorňovat na skutečnost, že každý požadavek spojený s jejich heslem je podezřelý.

Zdálo by se, že to jsou jednoduché pokyny, které se dají zaměstnancům snadno sdělit. Jenže samotné sdělení není nic platné. Aby totiž pracovník pochopil jeho význam, musí se dozvědět, jak může například chilková změna hesla vést k narušení firemní bezpečnosti. Můžeme říci dítěti: „Před vstupem na vozovku se vždycky rozhlédni na obě strany", ale dokud nepochopí, proč je to tak důležité, můžeme se spoléhat pouze na slepou poslušnost. Všechna pravidla vyžadující pouze slepou poslušnost jsou obvykle ignorována a zapomínána.

Poznámka
****
Hesla jsou hlavním předmětem sociotechnických útoků, proto je této oblasti věnována část 16. kapitoly, kde je možné nalézt doporučované procedury k zacházení s nimi.
****

Místo ohlašování incidentu

Bezpečnostní pokyny by měly určovat osobu nebo skupinu osob, které by se měla hlásit všechna podezření na pokusy o infiltraci do organizace. Všichni zaměstnanci musejí vědět, komu zatelefonovat v situaci, kdy mají podezření na fyzické či elektronické narušení. Číslo telefonu na místo ohlašování incidentů by mělo být vždy při ruce.

Ochrana sítě

Je nutné opakovat zaměstnancům, že názvy serverů nebo podsítí nejsou bezvýznamnými informacemi a mohou pro vetřelce znamenat důležitý údaj, užitečný při získávání důvěry a hledání místa, kde jsou uložené jisté informace.

Zejména správci databází, kteří disponují velkým množstvím informací, musejí postupovat podle přísných pravidel a prověřovat lidi, kteří volají o informace nebo pomoc.

Lidé, kteří stále poskytují pomoc a rady spojené s počítači, musejí být dobře vyškoleni v tom, jaké dotazy by v nich měly vzbuzovat podezření, že se jedná o sociotechnický útok.

Na druhou stranu z pohledu administrátora databáze představeného v posledním příběhu splňoval volající všechna kriteria věrohodnosti: telefonoval z kampusu a měl přístup ke stránce, která byla chráněná heslem. To jenom znovu dokazuje, jak je nezbytné používám standardních procedur ověřujících osoby žádající o informace, zvlášť když volající žádá o pomoc se získáním přístupu k důvěrným údajům.

Tato doporučení jsou nutná zejména pro školy. Jak známo, mnoho hackerů se rekrutuje z prostředí studentů. V této situaci se dá očekávat, že studentské spisy pro ně budou lákavým soustem, jednání tohoto typu se natolik rozšířilo, že některé firmy považují kampusy za nepřátelská prostředí a konfigurují firewally tak, aby blokovaly přístup ze strany jakékoliv vzdělávací

instituce.[19] V této souvislosti by všechny spisy studentů i personálu měly být považovány za hlavní potenciální cíl útoku a měly by být adekvátním způsobem chráněny.

Tipy na školení

Většinu sociotechnických útoků může snadno odrazit každý, kdo ví, na co si dávat pozor.

Z hlediska firmy existuje fundamentální potřeba dobrého školení. A je též potřeba nalézt řadu způsobů, jak připomínat lidem věci, které se naučili.

Za tímto účelem lze používat v systému okna připomínající různé zásady bezpečnosti. Měla by být naprogramována tak, aby zmizela teprve po stisknutí tlačítka potvrzujícího přečtení.

Dobrou metodou je používání krátkých poznámek ve firemním informačním bulletinu. Nejde tu o celý článek, ačkoliv na druhou stranu takový sloupek věnovaný bezpečnosti by nebyl od věci, ale o krátké poznámky podobné reklamám v časopisech. Takto by bylo možné v každém vydání zpravodaje představit novou otázku z bezpečnostní oblasti formou, která by přitahovala pozornost čtenáře.

[19] Pozn. překl.: V USA je to snadné, tam stačí filtrovat doménu .edu, ale u nás nejde poznat, jestli daná doména patří nějaké škole nebo ne.

9

Obrácený „Podraz"

Podraz (The Sting), zmiňovaný na jiném místě této knihy, je podle mě snad nejlepší film, jehož námětem je sociotechnická operace. Představuje intriku v bohatých a zajímavých detailech. Předvedená akce ukazuje, jak profesionální podvodníci provádějí jeden ze tří typů švindlů, který naleží do skupiny tzv. „velkých podvodů". Jestli chcete vidět, jak skupina profíku shrábne velké peníze, měli byste se na ten film jít podívat.

Tradiční podvody — pomineme-li detaily — probíhají podle určité šablony. Občas se však situace obrátí — útočník aranžuje události tak, aby se na něj s prosbou o pomoc obrátila samotná oběť.

Jak to funguje? Hned si to povíme.

Umění přátelského přesvědčování

Když průměrný člověk uslyší pojem „počítačový hacker", obvykle si vytvoří negativní představu osamělého, introvertního jedince, který nedovede hovořit s lidmi a komunikuje se světem jen pomocí e-mailů. Hacker-sociotechnik spojuje znalost technologií se společenskými schopnostmi se stále zdokonalovanými dovednostmi využívat lidi a manipulovat s nimi, které mu dovolují získávat informace zcela neuvěřitelnými cestami.

Telefon Angele

Místo: Industrial Federal Bank, pobočka ve Valley
Čas: 11:27

Angela Wisnowski měla telefonát. Nějaký muž říkal, že očekává dost velké dědictví a zajímají ho informace o různých typech spořících účtů, depozit a jiných bezpečných a poměrně výnosných forem investicí, které by mu mohla Angela nabídnout. Vysvětlila mu, že je na výběr několik možných řešení a zeptala se, jestli by nechtěl někdy banku navštívit a popovídat si o podrobnostech. Říkal, že hned jak peníze dostane odjíždí na prázdniny, a má kromě toho ještě mnoho dalších věcí k zařizování. Začala tedy po telefonu navrhovat některá řešení s různými detaily o úrocích, možnosti předčasného výběru vkladu a podobně, a snažila se dozvědět se zároveň něco o jeho očekáváních.

Zdálo se, že už k něčemu směřují, když řekl:

„Ach, omlouvám se, musím vzít druhý telefon. Kdy bych mohl znovu zavolat, abychom dokončili rozhovor a udělali nějaké rozhodnutí? Jdete někdy na oběd? "

Řekla, že odchází na oběd v půl jedné. Muž řekl, že zkusí zavolat do té doby nebo zítra.

Telefon Louisovi

Větší banky používají vnitřní bezpečnostní kódy, které se mění každý den. Když osoba z jedné pobočky potřebuje informaci z jiné, musí dokázat, že je oprávněna odpověd dostat tím, že uvede příslušný denní kód. Kvůli zvýšení bezpečnosti používají některé banky větší počet kódů. V Industrial Federal

Bank se na počítači každého pracovníka objevuje každé ráno seznam pěti kódů označených písmeny A až E.

* * *

Místo: Industrial Federal Bank, pobočka ve Valley
Čas: 12:48

Telefon, který vzal Louis Halpburn, se mu nezdál podezřelý. Takové záležitosti zařizoval pravidelně několikrát týdně.

„Dobrý den," řekl volající. „Tady Neil Webster, volám z pobočky 3182 v Bostonu. Chtěl bych mluvit s Angelou Wisnowski."

„Šla na oběd. Mohu vám nějak pomoci?"

„Zanechala nám tu vzkaz. Žádá o vyslání faxu s údaji o klientovi.“

Tón volajícího prozrazoval, že má špatný den.

„Člověk, který se tím u nás obvykle zabývá, je nemocný," řekl. „Mám tu ještě hromadu takových faxů a už budou za chvíli čtyři hodiny. Měl jsem už dávno jít, protože jsem za půl hodiny objednaný u doktora."

Manipulace, kdy se uvedly všechny důvody, proč by se s ním mělo cítit, měla za úkol docílit „změknutí," oběti.

„Nevím, kdo tu zprávu zapsal," pokračoval, „ale číslo faxu je nečitelné. Začíná na 213 a pak nemám tušení, co je dál."

Louis sdělil číslo faxu a volající řekl:

„Díky moc. Než to ale pošlu, musím se ještě zeptat na kód B."

„Ale to přece vy mi telefonujete," řekl Louis tak chladně, aby to mohl úředník v Bostonu vycítit.

„*To je dokonce dobře*," řekl si volající. „*Kdybych necítil z druhé strany alespoň smítko odporu, práce by se stala příliš lehká a mohl bych zlenivět.*"

Louisovi řekl: „Náš šéf propadl paranoi a vyžaduje ověřování všech osob, kterým něco posíláme, ať už je to cokoli. Ale žádný problém, nikdo neříká, abyste se prokazoval a nikdo neříká, abych poslal ten fax."

„Angela se vrátí za půl hodiny," řekl Louis. „Řeknu jí, aby vám zavolala."

„A já jí pak řeknu, že jsem dnes nemohl poslat informace, protože jste nechtěl uvést kód. Jestli mi doktor nedá neschopenku, tak možná zítra zavolám."

„Jak račte."

„Na tom faxu je napsáno „spěchá". Ale na tom nezáleží, bez verifikace i tak nemůžu nic udělat. Vvřidte jí, prosím, že jsem to opravdu chtěl poslat, ale vy jste mi neuvedl kód, ano?"

Louis konečně ustoupil. Bylo slyšet jeho rezignovaný povzdech.

„No dobrá," řekl. „Dejte mi chvilku, musím jít k počítači. Který jste chtěl kód?"

„B," odpověděl volající.

Louis zaparkoval hovor a za chvíli zvedl jiné sluchátko a uvedl kód:

„3184."

„To není správný kód."

„Jak to že není? Kód B je 3184."

„Já jsem ale neříkal B, ale E."

„Krucinál, tak moment."

Další pauza. Vyhledával kód.

„Kód E, číslo 9697."

„9697. Dobře. Za chvilku posilám fax."

„Děkuji."

Telefon Walterovi

„Industrial Federal Bank, u telefonu Walter."

„Ahoj Waltře, tady Bob Grabowski ze Studio City, pobočka 38" ozvalo se ve sluchátku. „Potřeboval bych kartu podpisových vzorů, mohl bys ji najít a nafaxovat mi ji?"

Na kartě podpisových vzorů je nejen podpis klienta, ale také identifikační informace, tedy číslo sociálního pojištění, datum narození, dívčí jméno matky, a občas dokonce i číslo řidičského průkazu. Lákavé sousto pro sociotechnika.

„Jistěže bych mohl. Řekni mi kód C."

„Někdo sedí na mým počítači," řekl volající. „Ale zato si pamatuju B a E, protože je dneska pořád používám. Zeptej se na některý z těch dvou."

„Dobře, dej mi éčko."

„9697."

Za několik okamžiků Walter faxoval kartu s podpisovým vzorem.

Telefon Donny Plaice

„Dobrý den, tady Anselmo."

„Co pro vás mohu udělat?"

„Jaké je to telefonní číslo 800, kam bych měl zavolat, abych se dozvěděl, jestli můj vklad už přišel na konto?"

„Jste klientem naší banky?"

„Jsem, ale nějaký čas jsem to číslo nepoužíval a ztratil jsem lístek, kde jsem ho měl zapsané."

„To číslo je 800-555-8600."

„Výborně, díky."

Příběh Vince Capelliho

Jako syn policisty z městečka Spokane věděl Vince už od mládí, že nechce strávit život otročinou a nastavováním krku za mizerný plat. Jeho hlavním cílem bylo vypadnout ze Spokane a založit si vlastní firmu. Výsměch jeho kamarádů ze školy jeho touhu jen přižívil – zdálo si jim směšné, že tak moc chtěl založit firmu a ani nevěděl, čím by se měla zabývat.

V duchu Vince věděl, že mají bohužel pravdu. Uplatňoval se pouze jako zadák ve školním basketbalovém mužstvu. Nebyl ani natolik schopný, aby získal stipendium na vysoké škole, ani nebyl natolik dobrý, aby se stal profesionálním basketbalistou. Jaký byznys by tedy měl začít?

5polužáci ze třídy si nikdy pořádně nevšimli jedné jeho vlastnosti: když Vince toužil po něčem, co patřilo některému z nich – ať už to byl nový kapesní nůž, pár teplých rukavic nebo nová sexy holka – brzy to patřilo jemu. Vůbec nemusel krást – vlastníci mu všechno dávali dobrovolně a o chvíli později přemýšleli, jak se to vlastně stalo. Nikam by nás nepřivedlo ani kdybychom se na to vyptávali samotného Vinceho, neuvědomoval si, že má ten dar.

Vince Capelli byl sociotechnik už od dětství, ačkoliv nevěděl, co to slovo znamená.

Po maturitě se jeho spolužáci smát přestali. Zatímco jiní se začínali v okolí poohlížet po práci, který by nespočívala v kladení otázek typu: „Dáte si k tomu hranolky?", Vinceho poslal otec ke svému kolegovi, starému policistovi, který odešel ze služby a založil si v San Francisku soukromou detektivní kancelář. Ten si brzy všiml talentu dřímajícího v mladíkovi a zaměstnal ho.

Od té doby uplynulo šest let. Vince nesnášel zakázky na sbírání důkazů proti nevěrným manželům, což bývalo spojené s mnohahodinovými nudnými pozorováními. Ale zato přímo zbožňoval záležitosti, kdy měl za úkol zjišťovat majetkový stav různých lidí pro advokáty, kteří chtěli vědět, jestli je daný chlápek natolik zámožný, že se vyplatí ho tahat po soudech. Tyto případy mu dávaly hodně příležitostí využívat svůj talent.

Jako například tehdy, kdy měl zjistit stavy účtů jistého Joea Markowitze. Joe nejspíše uzavřel podezřelý obchod s náhodným známým, který se ted chtěl dozvědět, jestli měl Markowitz nějaké peníze, které by bylo možno získat zpátky.

Vinceovým první krokem bylo získat alespoň jeden nebo lépe dva bankovní bezpečnostní kódy pro daný den. Zdá se to téměř nemožné. Co vlastně by mohlo pracovníky banky donutit prozradit základní prvek zajišťující bezpečnost? Položme si otázku — kdybychom chtěli získat kódy, napadl by nás nějaký plán?

Pro lidi, jako je Vince, to je hračka.

* * *

Lidé nám důvěřují, když používáme jejich žargon. Ukazujeme tak, že patříme k „uzavřenému kruhu" — je to skoro jako heslo.

Tentokrát jsem nepotřeboval přílišnou znalost žargonu. Pro začátek mi stačilo číslo pobočky. Zavolal jsem do úřadovny Beacon Street v Buffalu. Člověk, která ho zvedl, vypadal jako mluvka.

„Tady Tim Ackerman," ohlásil jsem se. Každé jméno je dobré, stejně by si ho nezapsal.

„Jaké je číslo vaší pobočky?"

„Číslo telefonu nebo pobočky?" ujišťoval se tázaný, což bylo dost hloupé, když uvážíme, že číslo telefonu jsem znát musel, když jsem mu na něj volal, ne?

„Pobočky."

„3182," řekl. Jen tak. Žádné „a proč to potřebujete vědět?" nebo něco takového. Koneckonců to není důvěrná informace: toto číslo je vidět skoro na každém dokumentu, který posílají.

Krok druhý: zatelefonovat do pobočky, kde měl Markowitz otevřený účet, získat jméno jednoho ze zaměstnanců a dovědět se, kdy má přestávku na oběd. Angela Wisnowski. Odchází v půl jedné. Zatím se mi docela daří.

Krok třetí: zavolat na tu samou pobočku v době, kdy bude Angela na obědě a říci, že telefonuji z té a té pobočky v Bostonu, Angela od nás chtěla nafaxovat nějakou informaci, uveďte kód. To bylo nejtěžší — klíčová otázka v celém utkání. Kdybych měl vést nějakou zkoušku na sociotechnika, musel by se zkoušený vyhrabat z takovéto situace: oběť získává odůvodněné podezření a my nadále naléháme, až informaci získáme. To se nedá dělat podle návodu či scénáře. Zde je nezbytná dovednost čtení psychiky oběti, jejích citových stavů, hraní si s ní jak s rybou na háčku, trošku povolujeme vlasec, zatáhneme, popustíme, abychom znovu zatáhli. A tak dále, dokud se rybka neocitne na dně naší lodky. Plesk!

Tímto způsobem se mi podařilo ulovit denní kód. Velký krok kupředu. Ve většině bank používají pouze jeden a ted už bych měl všechno, co potřebuji. Ale Industrial Federal Bank používá pět kódů, takže získání jednoho je trochu málo. Kdybych měl dva z pěti, měl bych větší šanci postoupit do dalšího kola.

Zbožňuji tento trik: „Neřekl jsem B, ale E." Když funguje, funguje dokonale. A většinou funguje.

Nejlepší by bylo, kdybych měl ještě třetí. Dá se to udělat během jednoho hovoru — „B", „E" a „D" zní tak podobně, že by bylo možné ještě jednou hrát, že mi špatně rozuměl. Osoba na druhém konci však nesmí náležet k těm nejbystřejším. Člověk, se kterým jsem mluvil, působi1 inteligentně, takže jsem raději zůstal na dvou kódech.

S denními kódy jsem měl v ruce trumf, který mi dovolil získat kartu s podpisovými vzory. Telefonuji, chlápek se ptá na kód. On chce C a já znám jenom B a E. To neznamená konec světa. Je třeba držet nervy na uzdě. Zahrál jsem něco na téma: „Někdo mi sedí u počítače. Zepej se mne na kódy, které znám."

Všichni pracujeme pro stejnou firmu, jsme na jedné lodi, tak si vzájemně usnadňujeme život — taková myšlenka se má v takovém okamžiku objevit v hlavě oběti. Můj člověk odehrál svou roli podle scénáře. Vybral si mezi kódy, které jsem mu napověděl. Odpověděl jsem správné, tak mi tedy poslal fax s kartou podpisových vzorů.

Už jsme skoro doma. Ještě jeden telefon, abychom získali číslo automatické služby informující o stavu konta. Když jsem měl Markowitzovu kartu, měl jsem čísla všech jeho kont i jeho PIN — banka pro tento účel používala prvních pět nebo poslední čtyři číslice čísla sociálního pojištění. S tužkou v ruce jsem zavolal na linku 800 a po několika minutách mačkání tlačítek a vybírání voleb jsem sepsal aktuální stavy všech účtů, a pro jistotu i nejčerstvější historii vkladů a výběrů.

Měl jsem všechno, co požadoval můj klient, dokonce více. Vždycky jsem přidával nějaký bonus jako známem dobré spolupráce. Zákazník musí být spokojen. Ostatně základem existence každé firmy jsou stálé zakázky.

Analýza podvodu

Klíčem k věci bylo získání denních kódů. Za tímto účelem použil útočník Vince hned několik technik.

Nejprve verbálně krčil rameny, když mu Louis nechtěl sdělit kód. Louisova podezíravost nebyla bezdůvodná — kódy je potřeba používat obráceně. Věděl, že osoba, která telefonuje, má povinnost uvést kód. Pro Vinceho to byl kritický moment — na tom záleželo všechno.

Tváří v tvář Louisovu podezření provedl soustředěný útok, odvolával se na soucit („jsem objednaný k doktorovi"), vyvolával nátlak („mám tu ještě hromadu takových faxů") a používal manipulaci („vyřidte jí, že jsem to opravdu chtěl poslat, ale vy jste mi neuvedl kód"). Vince přímo nehrozil, ale pouze vsugeroval jistou hrozbu: „Když mi neřekneš bezpečnostní kód, nepošlu informace o klientovi, které potřebuje tvá kolegyně a řeknu jí, že jsem to chtěl poslat, ale ty jsi mi odmítl pomoct."

Nebylo by dobré v tomto příběhu Louise příliš zbrkle obviňovat. Koneckonců osoba, se kterou hovořil po telefonu, věděla (nebo alespoň vyvolávala takový dojem), že jeho kolegyně Angela žádala o fax. Volající věděl o bezpečnostních kódech a znal jejich označení. Říkal, že jejich vedoucí to vyžaduje z bezpečnostních důvodů. Takže neviděl žádný důvod, proč by neměl kód uvést.

Louis není jediný. Vyloudění bezpečnostních kódů od zaměstnanců banky je na denním pořádku. Neuvěřitelné, ale je to tak.

Existuje hranice, po jejímž překročení přestávají být techniky používání sociotechniky legální. Získání čísla pobočky bylo úplně legální. Dokonce i obelstění Louise a vymámení dvou bezpečnostních kódů bylo legální. Hranice byla překročena teprve v okamžiku, kdy Vince požádal o fax s osobními údaji zákazníka.

Čin, který Vince spolu s osobou, která si ho najala, spáchal, není příliš riskantním přestupkem. Když ukradneme peníze nebo nějaké předměty, někdo si toho všimne. Když ukradneme informace, většinou si toho nikdo nevšimne, protože informace zůstávají stále ve vlastnictví právoplatného majitele.

> *Poznámka Mitnicka*
> **********
> Bezpečnostní kódy určené ke sdělování po telefonu jsou podobně jako heslo pohodlným a účinným prostředkem ochrany dat. Zaměstnanci však musejí vědět o tricích, které sociotechnici používají, a musejí být tak vyškolení, aby klíč od pokladny neodevzdávali příliš snadno.
> **********

Policajti jako hlupáci

Soukromému očku nebo sociotechnikovi často přijde vhod znát číslo řidičského průkazu někoho jiného[20] — díky němu je možné se na chvíli převtělit do této osoby, abychom získali informace o stavu jejího konta. Bez krádeže peněženky nebo bez koukám přes rameno se získání tohoto čísla zdá zcela nemožné. Ale pro nikoho s alespoň průměrnými sociotechnickými schopnostmi to není žádný problém.

Jistý sociotechnik, říkejme mu Eric Mantini, musel často zjišťovat čísla řidičských průkazů a registrační značky aut. Eric došel k závěru, že bezdůvodně zvětšoval riziko odhalení, když volal na dopravní policii a používal stejnou fintu pokaždé, když takovou informaci potřeboval. Přemýšlel, jestli by se procedura nedala nějak zjednodušit.

Pravděpodobně na to nikdo před ním nepřišel. Eric vymyslel způsob, jak získat informace hned, jakmile je potřeboval. Za tímto účelem využíval služeb státní dopravní policie. Tato oddělení v mnoha státech zpřístupňují obecně důvěrné informace o řidičích pojišťovnám, soukromým detektivním kancelářím a jiným institucím, kterým státní zákony přístup k těmto informacím povolují v zájmu celé společnosti.

Existuji samozřejmě jistá omezení týkající se typu informací, které mohou být sdělovány. Pojišťovny mohou získat jen část informací, jiné zásady platí pro soukromé detektivy a podobně.

Zcela jiná pravidla platí pro policii a vyšetřovatele. Dopravní policie jim zpřístupňuje všechny informace pod podmínkou, že se správně identifikují. Ve státě, kde Eric žil, spočívala identifikace v uvedení kódu instituce, která informace požaduje, a čísla řidičského průkazu tazatele. Pracovník dopravní policie vždy kontroloval, jestli se řidičský průkaz shoduje s uvedeným jménem a ptal se na jednu dodatečnou věc — obvykle na datum narození — než zpřístupnil data.

Eric se nehodlal stát ničím menším než policejním důstojníkem.

Jak se mu to podařilo? Obrátil intriku z „Podrazu".

Ericův „Podraz"

Nejprve zavolal na informace a požádal o telefonní číslo na státní dopravní policii. Dostal Číslo 503-555-5000, což je samozřejmě číslo pro veřejnost, potom zavolal na nedalekou policejní stanici a požádal o dálnopisnou kancelář — místo, odkud se vysílají a kde se přijímají informace od jiných vládních policejních složek, z národního trestního rejstříku atd. Když tam zatelefonoval, řekl, že potřebuje telefon, který používají vyšetřovatelé při kontaktu s dopravní policií.

„A kdo jste?" zeptal se policista od dálnopisu.

„Tady je AI. Volal jsem na 503-555-5753," řekl. Číslo, které uvedl, bylo vymyšlené, ale jen částečně. Jisté je, že číslo na kontakt s policií bude mít stejný prefix (503), jako číslo pro veřejnost. Téměř jisté bylo také to, že další tři číslice budou stejné. Potřeboval pouze ty poslední čtyři.

Do místnosti s dálnopisem nevolá nikdo zvenku. A kromě toho volající znal větší část čísla. Očividně to byla osoba zevnitř.

„Číslo je 503-555-6127," řekl policista.

Tímto způsobem získal Eric speciální číslo pro vyšetřovatele na kontakt s dopravní policií. Jedno číslo ho však zcela neuspokojovalo. Ten úřad má určité více linek — Eric chtěl vědět, kolik přesně a jaká má každá linka číslo.

[20] Pozn. překl.: Číslo řidičského průkazu má v USA často takovou úlohu jako u nás číslo občanského průkazu.

Ústředna

Aby mohl uskutečnit svůj plán, musel získat přístup k telefonní ústředně, která obsluhovala linky spojující vyšetřovatele s dopraváky. Zatelefonoval na státní telekomunikační úřad a představil se jako někdo, kdo volá z firmy Nortel, která vyrábí DMS-100, jeden z nejrozšířenějších typů ústředen.

„Mohl bych hovořit s někým, kdo se zabývá ústřednami DMS-100?"

Když ho přepojili, řekl, že volá z oddělení technické podpory společnosti Nortel v Texasu a vysvětlil, že právě vytvářejí hlavní databázi za účelem aktualizace firmwaru ve všech ústřednách. Věc se bude odehrávat na dálku — nebude potřeba asistence inženýrů. Potřebuji ale přístupové číslo na ústřednu, aby mohli vykonat aktualizaci přímo od sebe.

Znělo to docela věrohodně. Technik sdělil Ericovi číslo. Teď mohl telefonovat přímo na jednu ze státních telefonních ústředen.

Ústředny tohoto typu jsou před potenciálními vetřelci chráněné heslem, podobně jako firemní počítačové sítě. Každý dobrý sociotechnik zabývající se také phreakingem ví, že ústředny firmy Nortel mají pro aktualizaci softwaru defaultní uživatelské jméno NT AS (zkratka z Nortel Technical Assistance Support, nepříliš důmyslné). Ale co heslo? Jakmile získal číslo, pokusil se Eric několikrát připojit a zkoušel různá typická hesla. Heslo stejné jako uživatelské jméno — NT AS — nefungovalo, Ani další obvyklá hesla „helper" či „patch".

Zkusil ještě „update" (aktualizace) a ... byl tam. Typické. Používání takových zjevných hesel je jen o něco málo lepší než nemít vůbec žádné heslo.

Není nad to jít s dobou. Eric pravděpodobně věděl o této ústředně a jejím programovém vybavení stejně jako inženýři, kteří ji spravovali. Jakmile získal autorizovaný přístup k ústředně, měl plnou kontrolu nad telefonními linkami, které ho zajímaly. Ze svého počítače se připojil k centrále a zadal dotaz na číslo, které obdržel dříve, 555-6127. Ukázalo se, že na stejné místo vede devatenáct linek. Zřejmě bylo zatížení veliké.

Ústředna byla naprogramovaná tak, aby byla každému příchozímu hovoru vyhledána první volná linka.

Zvolil si linku číslo 18 a přesměroval ji na číslo svého nového levného mobilu, který nebude škoda po dokončení práce vyhodit.

Po aktivaci přesměrování na osmnácté lince čekal, až zatížení vzroste natolik, že se bude muset zároveň odehrávat sedmnáct hovorů. Následující telefon už nezazvoní v kanceláři dopravní policie — bude to Ericův mobil.

Telefon na dopravní policii

Krátce před osmou hodinou ráno zazvonil mobil. To byla ta nejrafinovanější část akce. Zde Eric, sociotechnik, hovoří s policistou, s někým, kdo ho může potenciálně zatknout, prohledat jeho byt nebo udělat razii, aby proti němu shromáždil důkazy.

A nebyl to jen jeden takový hovor. Od té doby každou chvíli volal nějaký policista. Později Eric obědval v restauraci s přáteli a každých několik minut přijímal hovor a zapisoval si poznámky na útržek papíru vypůjčenu propisovačkou. Dodnes se při vzpomínce na tuto scénu směje.

Dobrý sociotechnik se ani trochu neobává rozhovoru s policií. Naopak vzrušení z toho, jak obelstil vyšetřovatele, bylo pro Erica dalším zážitkem.

Podle Erica probíhaly hovory následovně: Dopravní policie, co pro vás mohu udělat?" „Tady detektiv Andrew Cole." ‚Dobrý den. Co byste potřeboval?"

„Potřebuji *soundex* na řidičák 005602789," mohl například policista požádat o informaci, která by mu pomohla najít fotografii — hodí se to například v situaci, kdy má policista někoho zatknout, ale neví, jak ten Člověk vypadá.

Žargon
****

Sounndex — systém převedení jmen na takové číselné kódy, kdy podobně znějící slova (v angličtině) dávají stejný kód.
****

„Hned si vyhledám seznam," odpovídal Eric. „Aha, pane Cole, z jaké jste agentury?"

„Jefferson County."

Potom Eric kladl nejdůležitější otázky:

„Uvedte, prosím, kód vaší instituce." „Jaké je číslo vašeho řidičského průkazu?" „Datum narození?"

Volající mu sdělil všechny osobní identifikační informace. Eric mohl nyní předstírat, že si ověřuje údaje a za chvíli říct, že se všechno shoduje a zeptat se na podrobnosti o informacích, které má vyhledat. Eric vytvářel dojem, že hledá uvedené příjmení a dovoloval, aby volající slyšel psaní na klávesnici počítače. O chviličku později říkal něco jako:

„Do háje! Už zas mi to spadlo. Moc se omlouvám, ale celý týden mám něco s počítačem. Mohl byste zavolat ještě jednou, aby to vzal jiný kolega?"

Tímto způsobem končil rozhovor čistě, aniž by budil jakékoli podezření v souvislosti s tím, že nemohl policistovi pomoci. A mezitím Eric získal další totožnost — podrobné údaje, které mohl využít, když chtěl od dopravní policie získat informace.

Po nekolikahodinovém přijímání hovorů a po získání několika de-
kódů institucí se Eric znovu připojil na ústřednu a deaktivoval
přesměrování hovorů.

Po této akci ještě měsíce dostával zakázky od legálních detektivních kanceláří, které nechtěly vědět, jak takové informace získával. Když bylo potřeba, znovu se připojil k ústředně, zprovoznil přesměrování a nasbíral další zásobu totožností policistů.

Analýza podvodu

Přehrajme si podrobně všechny Ericovy uskoky, které se zasloužily o zdar akce. V prvním úspěšném kroku přesvědčil úředníka z kanceláře dálnopisu, aby sdělil tajné číslo na dopravní policii úplně neznámému člověku kterého bez ověřování bral jako policistu.

Podobně postupovala osoba z telekomunikačního úřadu, která uvěřila, že Eric je zástupce firmy vyrábějící telefonní ústředny a poskytla mu přístupové číslo na ústřednu, na kterou je připojena i dopravní policie.

Eric se mohl dostat na ústřednu zejména díky mizernému zabezpečení, které praktikuje výrobce zařízení, když používá stejné jméno účtu ve všech ústřednách. Díky této bezstarostnosti bylo uhodnutí hesla maličkostí pro sociotechnika, který si uvědomuje, že obsluha ústředny nastavuje heslo, které se snadno pamatuje.

Když získal přístup na ústřednu, nastavil přesměrování jedné linky dopravní policie na vlastní mobilní telefon.

A nyní vrcholný kousek celé intriky: klamání jednoho policisty za druhým a sbírání nejen kódů institucí, ale také osobních identifikačních údajů. Díky tomu mohl Eric využívat jejich totožnost.

Přestože celý výkon vyžadoval hodně technických znalostí, nepovedl by se, nebýt pomoci několika osob, které neměly ponětí o tom, že hovoří s podvodníkem.

Tento příběh je další ilustrací jevu, že se lidé neptají „proč zrovna já?". Proč úředník od dálnopisu prozradil tajnou informaci nějakému neznámému policistovi nebo — v tomto případě — cizímu člověku *prohlašujícímu* se za policistu, místo aby mu poradil, že se má zeptat kolegy nebo svého nadřízeného? A zase je jediná odpověď to, že si lidé prostě jen zřídka kladou tuto prostou otázku. Možná je to nenapadá? A možná mají zábrany podezírat volajícího z podvodu a odmítat mu pomoc? Možná. Všechna další vysvětleni jsou

jen dohady. Sociotechnika nezajímá, proč to tak je, zajímá ho pouze, jak tato skutečnost usnadňuje získávání informací, které by bylo obtížné získat, kdyby se lidé chovali jinak.

Poznámka Mitnicka
****
Jestli má vaše firma vlastní telefonní ústřednu, zamyslete se nad následující otázkou: co by udělala osoba zodpovědná za ústřednu, kdyby jí zavolal představitel výrobce a požádal ji o číslo na ústřednu? Dala si ta osoba vůbec tu práci, aby změnila defaultní heslo ústředny? Je její heslo jednoduché slovo, které lze najít ve slovníku?
****

Prevence

Správně používaný bezpečnostní kód tvoří důležitou ochrannou bariéru. Nesprávně používaný kód je horší, než kdyby nebyl žádný, protože vytváří iluzi bezpečí, které ve skutečnosti neexistuje. Nač jsou nám kódy, jestliže je zaměstnanci neudrží v tajnosti?

Firma, která potřebuje verbální bezpečnostní kódy, musí jednoznačně určit, jak a kdy je používat. Kdyby byla osoba z prvního příběhu této kapitoly dobře proškolena, nemusela by se spoléhat na své instinkty a nemusela by se dát tak snadno přemluvit, aby prozradila bezpečnostní kód cizímu člověku. Úředník z tohoto příkladu cítil, že by za těchto okolností neměl být na takové informace dotazovaný, ale protože neměl jednoznačné směrnice, o zdravém rozumu nemluvě, rychle podlehl vůli volajícího.

Bezpečnostní procedury by rovněž měly definovat kroky, jak postupovat, když od nás nějaký zaměstnanec vyžaduje kód v neadekvátních okolnostech. Všichni pracovníci by měli neprodleně ohlašovat všechny dotazy na identifikační údaje, jako je denní kód nebo heslo, kladené za podezřelých okolností. Měli by též ohlašovat všechny pokusy ověřování totožnosti tazatele, které skončily neúspěšně.

Jako minimální ochranný prostředek by si pracovníci měli zaznamenat jméno volajícího, číslo jeho telefonu a kancelář či oddělení, odkud volá a položit sluchátko. Než mu zavolají zpátky, měli by si zkontrolovat, jestli v dané kanceláři pracuje osoba příslušného jména a jestli se telefónní číslo shoduje s podnikovým telefonním seznamem. Ve většině případů tato jednoduchá taktika dovolí ověřit, jestli je volající tím, za koho se prohlašuje.

Verifikace bývá obtížnější, jestliže firma používá tištěný telefonní seznam místo aktualizované počítačové verze. Neustále se přijímají a propouštějí zaměstnanci, lidé mění postavení, oddělení i telefonní čísla. Tištěný seznam může být neaktuální už v době jeho publikace. Na počítačovou verzi seznamu se ale také nelze zcela spoléhat, protože sociotechnik zná cesty, jak tam zanést změny. Jestliže není pracovník schopen porovnat telefonní číslo s nezávislým zdrojem, měl by provést verifikaci jinak, například se zkontaktovat s nadřízeným volajícího.

III

Pozor, vetřelec!

Na půdě firmy
Sociotechnika a technologie
První na ráně
Rafinované triky
Průmyslová špionáž

10

Na půdě firmy

Proč je pro cizího člověka tak snadné vydávat se za zaměstnance firmy, přesvědčivě ho hrát a klamat dokonce i lidi, kteří se v ohrožení tohoto typu vyznají? Proč se dá snadno oklamat i člověk, který si plně uvědomuje bezpečnostní pravidla, který dokonce nedůvěřuje neznámým lidem a který dbá o ochranu firemních zájmů?

Zamysleme se nad výše zmíněnými otázkami při čtení příhod v této kapitole.

Strážný

Čas: úterý 17. října, 2.16 po půlnoci

Místo: Skywatcher Aviation, Inc., výrobní závod na předměstí Tusconu ve státě Arizona

Příběh strážného

Leroy Green se cítil mnohem lépe, když slyšel klapot svých bot na podlaze opuštěných továrních hal, než když trávil dlouhé noční hodiny hleděním na monitory v místnosti ochranky. Tam nemohl dělat nic jiného, než jenom civět na obrazovky. Nesměl si dokonce ani přečíst noviny nebo nahlédnout do své v kůži vázané bible. Musel sedět a koukat na zatuhlý obraz, ve kterém se nikdy nic nechtělo pohnout.

Když procházel halami, mohl si alespoň protáhnout nohy a pokud si připomněl, že má do chůze zapojit více také ruce a ramena, měl náhražku gymnastiky. I když něco takového lze stěží považovat za gymnastiku pro bývalého pravého útočníka nejlepšího fotbalového mužstva ve městě. Ale co, pomyslel si, taková už je práce.

Na rohu změnil směr chůze a šel podél ochozu, odkud se rozprostíral pohled na výrobní halu dlouhou několik set metrů. Pohlédl dolů a všiml si dvou osob procházejících podél řady nedokončených helikoptér. po chvíli se postavy zastavily a začaly si prohlížet stroje. Docela divný pohled, když vezmeme v úvahu, že to bylo uprostřed noci.

„Raději to zkontroluji,“ pomyslel si.

Leroy se vydal směrem ke schodům. Do haly vešel tak, aby se k nim přiblížil zezadu. Nevšimli si ho až do okamžiku, kdy se ozval:

„Dobrý den. Mohl bych vidět vaše identifikátory?"

Leroy se snažil požívat v takových chvílích mírný tón. Uvědomoval si, že jeho úctyhodné rozměry by mohly leckoho vystrašit.

„Ahoj Leroyi," přečetl si jeden z nich jméno z jeho připnutého identifikátoru. „Já jsem Tom Stilton z marketingu z ústředí ve Phoenixu. Mám tady u vás několik jednání a chtěl jsem při této příležitosti ukázat mému kolegovi, jak se stavějí největší helikoptéry na světě."

„Dobrá, pane. Prosím vaše identifikátory," řekl Leroy. Všiml si, že byli velmi mladí. Chlápek z marketingu vypadal, jako by právě dokončil střední školu a ten druhý, s vlasy po ramena, na patnáct.

První z nich sáhl do kapsy pro identifikátor, načež začal nervózně prohledávat všechny své kapsy. Leroy začal tušit, že tu něco nehraje.

„Krucinál," řekl. „Musel jsem ho nechat v autě. Mohu ho přinést, to mi zabere nanejvýš deset minut. Skočím na parkoviště a vrátím se."

Leroy zatím vytáhl svůj notes.

„Mohl bych vás ještě jednou poprosit o vaše jméno?" zeptal se a pečlivě zaznamenal odpověď. Potom je požádal, aby s ním šli do kanceláře bezpečnostní služby. Když jeli výtahem do třetího patra, Tom říkal, že tu pracuje teprve šestý měsíc a doufá, že mu Leroy nebude v souvislosti s tímto incidentem dělat problémy.

V kanceláři ochranky začal Leroy zároveň se svými kolegy klást dvojici otázky. Stilton uvedl své telefonní číslo a řekl, že jeho vedoucí je Judy Underwood a sdělil i její telefonní číslo. Informace souhlasili s údaji v databázi na počítači. Leroy si vzal kolegy stranou, aby se poradili, co dělat. Nechtěli udělat nějakou chybu. Všichni tři se shodli, že bude nejlepší, když zavolají jeho vedoucí, i když to bude znamenat, že ji vzbudí uprostřed noci.

Leroy sám zavolal paní Underwood, vysvětlil jí, kdo je, a zeptal se, jestli u ní pracuje pan Stilton.

„Ano," odpověděla v polospánku.

„Narazili jsme na něj ve výrobní hale o půl třetí v noci bez identifikátoru."

„Dějte mi ho k telefonu," řekla paní Underwood.

Stilton přistoupil k přístroji a řekl:

„Jude, je mi to líto, že tě ochranka musela probudit uprostřed noci. Doufám, že se na mne nebudeš zlobit."

Chvíli poslouchal a pak pokračoval:

„To je kvůli tomu, že tam beztak musím být ráno na jednání kvůli tomu novému tiskovému prohlášení. A mimochodem, dostala jsi e-mail ohledně Thompsona? Musíme se v pondělí setkat s Jimem, abychom to neprošvihli. Aha, a jsme domluveni na ten úterní oběd, že?"

Ještě chvíli poslouchal, rozloučil se a zavěsil.

To Leroye překvapilo, neboť očekával, že mu ještě sluchátko předá a jeho šéfová potvrdí, že je všechno v pořádku. Přemýšlel, jestli jí ještě jednou nezavolá. Pomyslel si však, že už ji jednou vyrušil uprostřed noci. Kdyby zatelefonoval podruhé, mohla by se rozzlobit a stěžovat si jeho nadřízenému.

„*Nebudu dělat vlny*," řekl si v duchu.

„Mohl bych kolegovi ukázat zbytek výrobní linky?" zeptal se Stilton Leroye. „Klidně můžete jít s námi a hlídat nás."

„Jděte si prohlížet," řekl Leroy. „Ale příště si nezapomeňte identifikátor. A prosím předem informujte strážní službu, když budete mít v úmyslu pobývat v areálu podniku po pracovní době. Existuje na to nařízení."

„Budu to mít na paměti, Leroyi," odpověděl Stilton a oba odešli.

Neuplynulo ani deset minut, když v kanceláři zazvonil telefon. Paní Underwood.

„Co to bylo za chlápka?" chtěla vědět. Řekla, že se ho pokoušela vyptávat, ale on jí povídal nějaké divné věci o obědě. Vůbec netuší, kdo to byl.

Strážný zavolal kolegům na chodbě i na bráně u parkoviště. Oba viděli před několika minutami vycházet dva mladíky.

Když Leroy později vyprávěl tuto příhodu, vždycky nakonec dodával:

„Bože, myslel jsem, že mě můj šéf zabije. Mám kliku, že mě nevyhodil z práce."

Příběh Joea Harpera

Sedmnáctiletý Joe Harper se už více než rok vkrádal do různých budov. Někdy ve dne, jindy v noci. Pokaždé se chtěl přesvědčit, jestli mu to projde. Byl synem muzikanta a servírky – oba pracovali po nocích a Joe trávil příliš mnoho času osamocen. Jeho popis těch samých událostí nám dovolí lépe pochopit, co se stalo

* * *

Mám takového kamaráda, Kenny se jmenuje, který chce být pilotem helikoptéry. Zeptal se mně, jestli bych ho mohl zavést do továrny Skywatcher, aby si mohl prohlédnout výrobní linku helikoptér. Věděl, že už jsem se potloukal po různých budovách. Vkradání se do míst, kde je vstup zakázán, to už je slušná dávka adrenalinu.

Nemůžete se jen tak jednoduše sebrat a jít do továrny nebo úřadu. Nejprve je nutné všechno do detailu promyslet, naplánovat a udělat průzkum objektu. Je třeba navštívit jejich internetovou stránku, vyhledávat jména a postavení, strukturu a telefonní čísla. Pročítat novinové výstřižky a články v časopisech. Systematický průzkum je můj vlastní recept na bezpečnost — díky tomu mohu předstírat, že jsem zaměstnanec a mluvit s každým.

Kde tedy začít? Nejprve jsem se podíval na Internet, abych si zjistil, kde se nacházejí kanceláře firmy. Ukázalo se, že hlavní sídlo je ve Phoenixu. Paráda. Zavolal jsem tam a požádal o přepojení na marketingový odbor. Každá firma má takový odbor. Vzala to nějaká paní a já povídal, že jsem z firmy Blue Pencil Graphics a chtěl jsem se pozeptat, jestli by měli zájem využít našich služeb. Ptal jsem se, s kým bych mohl na toto téma mluvit. Řekla, že asi nejlépe s Tomem Stiltonem. Poprosil jsem ji tedy o jeho telefonní číslo, na což mi odpověděla, že takové informace neposkytují, ale že mě na něj může přepojit. Dovolal jsem se na jeho záznamník. Nahraná zpráva zněla takto: „Dobrý den, tady Tom Stilton, odbor marketingu, linka 3147. Prosím, zanechte vzkaz." Super! Prý neposkytují takové informace, a tady ten chlápek si ho nechal na záznamníku. Bomba — měl jsem už jméno a číslo.

Další telefonát na stejnou pobočku.

„Dobrý den, sháním Toma Stiltona, ale není u sebe. Chtěl bych se na něco zeptat jeho šéfa."

Šéfová také nebyla, ale během rozhovoru jsem stačil pochytit, jak se jmenuje. Ona si také laskavě nahrála na záznamník číslo linky — výborně.

Určitě by se mi podařilo provést nás bez zvláštního úsilí okolo strážníka na chodbě, ale kdysi jsem projížděl blízko továrny a měl jsem dojem, že tam byl kolem parkoviště plot. V takovém případě ochranka jistě kontroluje, kdo vjíždí na parkoviště. V noci si určitě ještě zapisují espézetky, takže si budu muset na bleším trhu koupit nějaké staré značky.

Nejprve ale musím získat telefonní číslo do budky strážného. Chvíli jsem počkal, aby můj hlas nebyl povědomý, kdyby to vzala stejná osoba. Pak jsem znovu zatelefonoval a řekl:

„Někdo nám hlásil, že jsou problémy s telefonem v budce strážných na Rodge Road. Ještě to blbne?"

Spojovatelka nevěděla, ale že mně tam přepojí.

Vzal to nějaký muž:

„Vrátnice Ridge Road, u telefonu Ryan."

„Ahoj Ryane, tady Ben. Neměli jste poslední dobou nějaké problémy s telefonem?"

Chlápek byl asi proškolený, protože se hned zeptal:

„Jaký Ben? Jaké je tvoje příjmení?"

„Někdo od vás hlásil nějaké potíže," pokračoval jsem, jako bych přeslechl jeho otázku.

Odvrátil sluchátko a zavolal:

„Hej, Bruci, Rogere, nebyly nějaké potíže s telefonem?"

Znovu se vrátil ke sluchátku a řekl:

„Nevíme o ničem."

„Kolik tam máte telefonních linek?"

Na mé jméno už si nevzpomněl.

„Dvě," odpověděl.

„A ted jsme na které?"

„3140."

A máme to!

„A obě fungují bez problémů?"

„Zdá se."

„Dobrá," řekl jsem. „Hele, Ryane, kdyby se u vás objevily nějaké problémy s telefony, zavolejte nám do Telecomu. Jsme tu proto, abychom vám pomáhali."

Rozhodli jsme se s Kennym, že navštívíme továrnu ještě téže noci. Pozdě odpoledne jsem zavolal do budky strážných a představil se jako pracovník odboru marketingu. Řekl jsem:

„Dobrý den, tady Tom Stilton z marketingu. Hoří nám termín a jedou nam na pomoc dva lidi. Ale nedorazí dříve než v jednu, ve dvě v noci. Bude v tu dobu ještě někdo ve službě?"

Odpověděl radostně, že končí o půlnoci.

„A mohl byste tam zanechat vzkaz pro toho, kdo vás střídá?" zeptal jsem se. „Že až se objeví dva lidé a řeknou, že jdou za Tomem Stiltonem, aby je pustil dovnitř, ano?"

Odpověděl, že bez problémů. Zapsal si moje jméno, odbor a vnitřní lmku a řekl, že to zařídí.

Přijeli sme k bráně něco po druhé. Oznámil jsem, že jsme přijeli za mem Stiltonem. Rozespalý strážník nám ukázal dveře, kterými máme jít a místo na zaparkování.

Po vstupu do budovy jsme narazili na další stanoviště strážných na chodbě a na knihu, kam se měl zaznamenávat pobyt po pracovních hodinách. Řekl)sem strážným, že musím na ráno připravit zprávu a kamarád prostě chtěl vidět továrnu.

„Je do helikoptér blázen," řekl jsem. „Chce se stát pilotem."

Hlídač požádal o můj identifikátor. Sáhl jsem do kapsy, posléze do několika jiných a řekl jsem, že jsem ho asi zapomněl v autě že pro něj hned skočím.

„Deset minut“ řekl jsem.

„Není třeba. Stačí, když se zapíšete," řekl strážný.

Procházka podél výrobní linky byla úžasná. Dokud nás nezastavil ten obr Leroy.

V kanceláři hlídačů jsem si byl vědom toho, že vetřelec by vypadal nervózně a vystrašeně. Když se věc vyostřila, předstíral jsem podráždění, Jako bych byl opravdu tím, za koho jsem se vydával, a z rovnováhy mě vyšinul fakt, že mi nechtěli uvěřit.

Když začali mluvit o tom, že by asi měli zavolat mé šéfové a začali v počítači hledat její telefon domů, stál jsem tam a uvažoval: „Asi je na čase se vypařit. Ale co brána na parkovišti — i kdyby se nám podařilo dostat se z budovy, zavřou bránu a chytí nás."

Když Leroy zavolal paní, která byla Stiltonova vedoucí, a podal mi sluchátko, začala na mě křičet:

„Kdo je tam? Kdo jste?!"

Ale já prostě hovořil tak, jako bychom vedli normální rozhovor a nakonec jsem zavěsil.

Jak dlouho jí bude trvat, než uprostřed noci najde číslo do továrny? Odhadoval jsem, že máme ani ne čtvrt hodiny na to, abychom se odsud dostali, než ta ženská zavolá zpátky a zburcuje strážné.

Vyšli jsme z továrny tak rychle, jak jen to bylo možné, ale tak, aby to nevypadalo, že nějak spěcháme. Oddechl jsem si, když hlídač u brány parkoviště jenom mávl rukou, abychom jeli.

Analýza podvodu

Stojí za připomenutí, že hrdiny pravdivé události, na které je založen tento příběh, byli teenageři. Pro ně to byla skopičina, dobrodružství-chtěli se přesvědčit, jestli se jim to povede. Jestliže se pro dvojici teenagerů ukázal vstup do areálu firmy tak jednoduchý, jakou práci by to as dalo zlodějům, průmyslovým špiónům nebo teroristům?

Jak je možné, že tři zkušení strážní dovolili dvěma vetřelcům jen tak odejít z továrny? Tím spíš, že už jejich nízký věk by měl vzbuzovat velké podezření?

Leroy *měl* na počátku správné pochybnosti. Dobře udělal, když je zavedl do kanceláře a ověřoval mladíka vydávajícího se za Toma Stiltona a také telefony a jména, která uvedl. A zcela jistě byl správný i telefon jeho domnělému nadřízenému.

Nakonec ho ale oklamala mladíkova sebejistota a pobouření. To nebylo chování, které by očekával od zloděje nebo od vetřelce – takhle se mohl chovat pouze zaměstnanec firmy. Tak si to alespoň Leroy myslel. Měl by být proškolen, aby jednal podle identifikačních pokynů nikoliv podle svého úsudku.

Proč jeho pochybnosti nevzrostly, když ten mladík zavěsil sluchátko? Když ho nedal zpátky Leroyovi, aby slyšel na vlastní uši, jak Judy Underwood potvrzuje, že její pracovník má důvod pobývat v továrně v tuto hodinu?

Bylo to šité tak hrubou nití, že je těžké uvěřit, že se Leroy nechal napálit. Podívejme se však na věc jeho očima: jen tak tak vystudoval střední školu, záleželo mu na práci, nebyl si jistý, jestli se nevystavuje přílišnému riziku druhým telefonátem osobě na vedoucí pozici. Rozhodli bychom se, být v jeho kůži, pro opětovný telefonát?

Samozřejmě druhý telefonát nebyl jediným východiskem. Co ještě mohl strážný udělat?

Ještě před uskutečněným telefonátem měl požádat oba mládence o nějaký doklad totožnosti s fotografií. Když přijeli do továrny autem, tak by alespoň jeden z nich měl mít u sebe řidičský průkaz. Pak by se skutečnost s falešnými jmény ihned prokázala (profesionál by se zajisté vykázal falešným dokladem, ale tito chlapci na to určitě nepomyslili). V každém případě měl Leroy zjistit jejich totožnost a zapsat si je. Kdyby oba tvrdili, že u sebe nemají žádný doklad totožnosti, měl jít s nimi do auta pro identifikátor, který tam údajný Tom Stilton prý zapomněl.

Po rozhovoru se šéfovou je měl jeden ze strážných doprovodit a zapsat si poznávací značku. Kdyby byl pozorný, možná by si všiml, že značka (ta koupená na bleším trhu) neměla platnou registrační nálepku – a už to by byl důvod, aby dvojici zadržel za účelem dalšího zjišťování jejich totožnosti.

> *Poznámka Mitnicka*
> **********
> Lidé se schopností manipulace mají často okouzlující osobnost. Jsou to převážně osoby bystré, čilé a výřečné. Sociotechnici se také vyznačují schopností rozptylovat myšlenky lidí, se kterými hovoří, což vede k rychlému navázání spolupráce s obětí útoku. Myslet si, že ne každá osoba podlehne takovéto manipulaci, je podcenění schopností a instinktu sociotechnika.
>
> Na druhou stranu dobrý sociotechnik si nikdy nedovolí podceňovat svého protivníka.
> **********

Smetiště plné informací

Udivující je množství informací, které je možné získat prohledáváním odpadků vyvážených z firmy.

Mnoho lidí si neuvědomuje, co vlastně vyhazuje: účty za telefon, výpisy z bankovního účtu, obaly od léků, materiály svázané s prací a mnoho jiných věcí.

Pracovníci ve firmě si musejí uvědomovat, že existují lidé, kteří hledají v odpadcích využitelné informace. Když jsem byl na gymnáziu chodíval jsem prohledávat popelnice za budovou místní telekomunikační firmy – nejčastěji

sám, občas s kamarády, kteří se také zajímali o telekomunikace. Jako zkušený „smetištní potápěč" jsem se naučil vyhýbat se smetí z různých „nezajímavých" míst a nosit rukavice.

Samo prohrabování se odpadky není možná nejzábavnější, ale to, co tam lze najít, představuje vítaný zisk. Vnitřní telefonní seznamy, dokumentace k programům, seznamy zaměstnanců, nepovedené výtisky, ze kterých bylo možné naučit se programovat ústředny, a tak dále. Stačilo si vzít.

Návštěvy na smetišti jsem plánoval na noci po vytištění nových dokumentací, protože pak byly ty staré exempláře bezstarostně vyhazovány. Chodil jsem tam také občas namátkou hledat nějaké poznámky, dopisy, zprávy a podobné věci, které mohly obsahovat zajímavé informace.

Když jsem přicházel na smetiště, hledal jsem nejprve nějaké krabice a dával je stranou. Jestliže mě někdo načapal, a občas se to stávalo, říkal jsem, že se můj kamarád stěhuje a tak pro něj hledám nějaké krabice, aby se mohl sbalit. Hlídač si obvykle nevšímal dokumentů, kterými jsem krabice plnil, než jsem si je vzal domů. Občas mi řekli, abych zmizel; pak jsem šel k popelnicím konkurenční telekomunikační firmy.

Nevím, jak to vypadá dnes, ale v tehdejších časech bylo snadné poznat pytle, které mohly obsahovat něco zajímavého. Drobné smetí a odpadky z bufetu byly vyhazovány volně ve velkých pytlích, zatímco odpadky z kancelářských košů byly vynášeny v bílých igelitových pytlích zavázaných provázkem.

Když jsme jednou s kamarády prohledávali smetiště, našli jsme několik roztrhaných listů papíru. Roztrhaný je slabé slovo: někdo si dal tu práci, aby je rozcupoval na úplně malé kousíčky. Všechny ty útržky se nacházely v samostatném pytlíku. Vzali jsme pvtlík do nedaleké hospody, vysypali jsme kousky na stůl a začali je skládat.

Všichni jsme měli rádi puzzle, takže skládání útržků byla pro nás dobrá zábava. Za odměnu jsme dostali místo lízátka něco lepšího. Složený dokument obsahoval seznam kont a hesel do jednoho z nejdůležitějších firemných systémů.

Vyplácí se celá ta námaha a riziko spojené s hrabáním se na smetišti? A jak! Dokonce víc, než by muselo, protože riziko je nulové. Bylo to tak tehdy a je tomu tak dodnes: pokud při té příležitosti nevstupujeme na něčí soukromý pozemek, je prohrabávání smetišť stoprocentně legální.

Samozřejmě nejen phreakeři a hackeři se noří do odpadkových košů. Policie rovněž pravidelně nahlíží do popelnic a na základě důkazů nalezených v jejich popelnicích byla obviněna řada lidí, od obyčejných podvodníčků až po mafiánské bossy. Také výzvědné služby léta používají tuto metodu.

Není to možná taktika hodná Jamese Bonda — diváci chtějí zajisté raději sledovat, jak vyzrává nad padouchem nebo svádí další kočku, než aby ho viděli po kolena ponořeného v odpadcích. Opravdoví špióni se ale neštítí, protože mezi slupkami od banánů a kelímky od kávy, starými novinami a roztrhanými seznamy nákupů může být ukryto něco cenného. A kromě toho je tento způsob hledání informací docela bezpečný.

Peníze za odpadky

Korporace si také občas hrají na smetištní potápěče. V červnu roku 2000 otiskly noviny zprávy, že Oracle Corporation (šéf této firmy, Larry Ellison, je asi nejzapřísáhlejším nepřítelem Microsoftu v USA) si najala detektivní firmu, jejíž pracovníci byli přistiženi při činu. Zjevně chtěli získat přístup k odpadkům z ATC (lobbovací skupina podporovaná Microsoftem), ale bez rizika, že budou přistiženi. Podle novinových zpráv poslala firma do ATC ženu, která nabízela uklízečům 60 dolarů za odpadky z ATC. Odmítli. Následující noc se objevila podruhé a zvedla nabídku na 500 dolarů.

Uklízeči to tentokrát nejenom odmítli, ale i nahlásili.

Časopis Time nadepsal svůj článek věnovaný Ellisonovi z Oraclu "Slídil Larry" (Peeping Lany).

Analýza podvodu

Vezmeme-li v úvahu zkušenosti moje i firmy Oracle, možná bychom se měli zamyslet, jestli krádež odpadků není riskantní.

Odpověd bude znít: riziko je nevelké a zisk může být ohromný. Snad jen pokus o koupení osob, které se zabývají úklidem, zvětšuje riziko nesení nějakých důsledků. Je však nepochybné, že kdo se nebojí krapet se ušpinit, měl by si poradit bez úplatků.

Sociotechnik najde v odpadkovém koši hodně zajímavých věcí. Může tam získat informace postačující k zahájení útoku na firmu, například koncepty, harmonogramy, dopisy a podobné dokumenty, kde se objevují jména, oddělení, pracovní postavení, telefonní čísla i názvy realizovaných projektů. Smetí nám může dodat informace o struktuře firmy, plánech výjezdů atd. Tyto detaily se mohou zdát lidem z dané organizace nedůležité, ale pro útočníka jsou velmi cenné.

Mark Joseph Edwards hovoří ve své knížce *Internet Security With Windows NT* o celých zprávách vyhazovaných kvůli překlepům, heslech zapsaných na útržku papíru, poznámkách typu „když jsi byl pryč, volali..." s telefonními čísly, celých šanonech naplněných dokumenty, nezničených disketách a páskách — toto všechno může potenciálnímu vetřelci pomoci.

Autor knížky se také ptá: „A kdo jsou lidé, kteří uklízejí vaše kanceláře? Přijali jste rozhodnutí, že uklízeči nemají přístup do místností s počítači? A co odpadkové koše v ostatních místnostech? Federální úřady provádějí bezpečnostní prověrky lidí, kteří mají přístup k jejich popelnicím a skartovačkám. Neměli byste si z nich vzít příklad?"

> *Poznámka Mitnicka*
> **********
> Vaše odpadky mohou znamenat pro útočníka poklad. Obyčejně si neděláme velké starosti s tím, co vyhazujeme do koše doma, tak proč bychom si měli myslet, že se lidé v prácí chovají jinak? To všechno vede k nutnosti vzdělávat zaměstnance a seznámit je s riziky (všeho schopní lidé hledající informace v popelnicích) i zranitelnými místy (důvěrné informace, které nebyly zničené či řádně vymazané).
> **********

Potupa

Nikdo neviděl nic podezřelého na tom, že Harlan Forris přišel v pondělí ráno do práce na silniční odbor a řekl, že si ve spěchu zapomněl doma visačku. Vrátná ho vídávala dennodenně po celou dobu, co tu pracovala — tedy dva roky — jak přicházel do práce. Řekla mu, aby se podepsal na visačku brigádníka, předala mu ji a pustila ho dovnitř.

Peklo začalo teprve o dva dny později. Historka se rozšířila po celém odboru. Většina lidí, kteří ji slyšeli, tomu nemohla uvěřit, zbytek nevědel, jestli se má smát nebo litovat chudáka George.

Neboť George Adamson byl politováníhodná osoba — byl to nejlepší šéf odboru, jakého kdy měli. Nezasloužil si, aby se něco takového stalo právě jemu. Samozřejmě za předpokladu, že ta historka byla pravdivá.

Potíže začaly, když si George jednoho pátečního odpoledne pozval Harlana do své kanceláře a oznámil mu, jak nejšetrněji mohl, že bude od pondělka přeřazený na odbor hygieny. Pro Harlana to bylo, jako by ho propustili. A vlastně horší — bylo to ponižující. Nedokázal se s tím smířit.

Večer seděl na verandě a pozoroval auta lidí vracejících se z práce domů. Nakonec si všiml kluka, který se jmenoval David, a kterému všichni říkali

„ten kluk od válečných her", jak se na svém mopedu vrací ze školy. Zastavil ho, dal mu novou hru Code Red Mountain, kterou koupil speciálně pro tuto příležitost, a přednesl nabídku: nejnovější herní konzoli plus šest her za trochu počítačové pomoci a závazek mlčení.

Když Harlan objasnil svůj plán — zatím bez podrobností — David souhlasil a řekl, co chce od Harlana. Musel koupit modem, najít v kanceláři počítač poblíž nějaké volné telefonní zásuvky a připojit ho. Potom měl umístit modem pod psacím stolem tak, aby si ho nikdo nevšiml. Následující krok byl riskantní. Harlan musel usednout k počítači, nainstalovat software umožňující vzdálený přístup a spustit ho.

Člověk, který v dané kanceláři pracoval, se mohl každou chvíli vrátit nebo mohl někdo přijít a uvidět ho v cizí kanceláři. Byl tak nervózní, že ani nemohl přečíst instrukce, které mu David napsal. Ale nakonec se mu všechno podařilo udělat a nikým nepovšimnut vyklouzl z budovy.

Kladení miny

Večer se David stavil u Harlana na večeři. Pak oba usedli k počítači a během několika minut se mladíkovi podařilo získat vzdálený přístup na počítač George Adamsona. Úkol to byl jednoduchý, protože George nikdy neměl čas na to, aby si změnil heslo a kromě toho pořád někoho žádal, aby si stáhl soubor z jeho počítače nebo od něj něco poslal. Brzy jeho heslo znali všichni z oddělení.

Po krátkém hledání nalezli soubor *Rozpočet2002.ppt* a stáhli si ho na Harlanův počítač. Harlan pak Davida poprosil, aby ho nechal dvě hodiny o samoté.

Když se David vrátil, Harlan ho požádal o opětovné připojení k počítačové sítí silničního odboru a nahrál soubor zpátky tam, kde ho našli. Tím přepsali původní verzi tou svojí. Harlan ukázal Davidovi konzoli a řekl, že pokud půjde všechno podle plánu, zítra bude jeho.

Překvapení pro George

Zdálo by se, že něco tak nudného jako rozpočtové jednání nebude nikoho zajímat, ale tentokrát byla zasedačka oblastního zastupitelství plná novinářů, představitelů různých zájmových skupin i obyčejných zvědavců. Přijely dokonce i dva televizní týmy.

George vždy cítil, že na těchto schůzích může hodně ztratit. Oblastní zastupitelstvo přidělovalo prostředky a kdyby nebyl schopen uvést přesvědčivé argumenty, bude jeho rozpočet zkrácen a potom si budou všichni stěžovat na díry na silnicích, nefunkční semafory, nebezpečné křižovatky a obviňovat budou právě jeho. Celý rok. Toho večera, když mu bylo uděleno slovo, se cítil pevný v kramflecích. Po šest týdnů si připravoval prezentaci v PowerPointu a dokonce si ji vyzkoušel na ženě, na svých nejbližších spolupracovnících a důvěryhodných přátelích. Všichni se shodovali, že to byla nejlepší prezentace, jakou viděli.

První tři obrázky v PowerPointu splnily svou úlohu skvěle. Všichni členové rady pozorně sledovali plátno. Slajdy ideálně doplňovaly argumentaci řečníka.

Ale potom se něco pokazilo. Čtvrtý obrázek měl ukázat náladovou fotografii nově otevřeného úseku dálnice při západu slunce. Ale místo toho se tam objevilo něco jiného. Něco velmi pohoršlivého. Fotografie jako z *Penthousu* nebo *Hustlera*. Zaslechl šum mezi diváky a rychle přešel na další slajd. To bylo ještě horší. Představivosti už nebylo ponecháno vůbec nic.

Právě chtěl stisknout klávesu pro další obrázek, když někdo ze sálu vytáhl šňůru od projektoru ze zdi. Předsedající zatím bušil dřevěným kladívkem do

stolu a snažil se překřičet vzniklou vřavu oznámením o přeložení schůze na jiný termín.

Analýza podvodu

S pomocí dospívajícího hackera se nespokojený pracovník dokázal dostat do počítače svého šéfa, stáhnout si důležitou prezentaci a zaměnit několik slajdů. Pak uložil prezentaci zpátky na šéfův disk.

Díky modemu připojenému k jednomu z počítačů a telefonní zásuvce byl mladý hacker schopný dostat se na počítač zvenku. Mladík si předtím připravil software na vzdálený přístup, aby měl po připojení plný přístup ke všem souborům v systému. Protože byl počítač připojený k podnikové síti a uživatelské jméno a heslo byly všeobecně známé, přístup k jeho souborům neznamenal žádné úskalí.

Celá práce zabrala pouze pár hodin včetně skenování obrázků z barevných magazínů, škoda způsobená na dobré pověsti vedoucího byla nepředstavitelná.

> *Poznámka Mitnicka*
> **********
> Většina pracovníků, kteří jsou propouštěni, přeřazováni nebo degradováni, nedělá žádné problémy. Stačí však jeden, aby si firma příliš pozdě uvědomila, Že se měly už dříve přijmout kroky, které by předcházely katastrofám.
> Zkušenosti a statistika říkají, že největší nebezpečí hrozí firmě ze strany zaměstnanců. To oni mají detailní znalosti o místech, kde jsou uložené důležité informace, kam udeřit, aby byly způsobeny největší škody.
> **********

V očekávání povýšení

Jednoho teplého podzimního dopoledne vešel Peter Milton do foyer regionální pobočky Honorable Auto Parts v Denveru – firmy, která provozovala velkoobchod s náhradními díly. Čekal u pultu v recepci, zatímco dívka zároveň zapisovala hosta do návštěvní knihy, vysvětlovala po telefonu někomu cestu a vyřizovala kurýrní zásilku.

„Jak jste se naučila dělat tolik věcí najednou?" žasl Peter, když konečně našla čas na něho. Usmála se, zjevně potěšena, že si toho všiml. Řekl jí, že je z marketingu z Dallasu a že je zde domluvený s Mikem Talbotem z odbytu v Atlante.

„Máme dnes odpoledne navštívit zákazníka," vysvětlil. „Prostě na Mika počkám tady ve foyer."

„Marketing," povzdechla si melancholicky.

Peter se na ni usmál, očekávaje, co bude dál.

„Kdybych šla na školu, vybrala bych si právě to," pokračovala. "Sním o prácí v marketingu."

Znovu se usmál.

„Kailo," přečetl si její jméno na cedulce na pultu. „U nás v Dallasu pracovala jako sekretářka jedna holka, která pak přešla do marketingu. To bylo asi před třemi roky a dnes je asistentkou ředitele marketingu vydělává si dvojnásobek toho, co na začátku."

Kaila se zasnila.

"Umíte pracovat s počítačem?"

"Samozřejmě," zněla odpověd.

"A co byste řekla tomu, kdybych vás navrhl na místo sekretářky v marketingu?"

„Kvůli té práci bych se klidně do Dallasu i přestěhovala," rozzářila se

„Dallas si oblíbíte,“ řekl. „Nemohu vám teď nic slíbit, ale uvidím, co se dá dělat."

Pomyslela si, že ten milý a upravený muž v obleku a kravatě by mohl pro její kariéru hodně udělat.

Peter se posadil v hale, otevřel svůj notebook a zabral se do práce. Po čtvrthodince přišel znovu k pultu.

„Zdá se, že Mika něco zdrželo. Nebyla by tu nějaká jednací místnost, kam bych si mohl sednout a zkontrolovat si poštu?"

Kaila zatelefonovala člověku, který měl na starosti rezervace jednacích místností a požádala ho o nějakou volnou pro Petera. Podle módy přicházející z firem v Sillicon Valley (první z nich snad byla společnost Apple) byly některé konferenční salónky pojmenované podle postav z animovaných filmů, jiné názvy řetězců restaurací, jmény filmových hvězd či hrdinu komiksů. Měl hledat salónek Mickeyho Mouse. Kaila ho požádala, aby se zapsal do knihy a ukázala mu cestu.

Našel svou místnost, usadil se a připojil svůj notebook do zásuvky sítě Ethernet.

Máme už jasno?

Přesně tak! Vetřelec se připojil k firemní síti za zády firemního firewallu.

> Poznámka Mitnicka
> **********
> Je vhodné vyškolit personál, že šaty nedělají člověka. To, že je někdo dobře oblečen a má dobré vystupování, ještě neznamená, že je důvěryhodný.
> **********

Příběh Anthonyho

Myslím, že Anthonyho Lakea by bylo možné označit termínem „líný obchodník". I když možná slovo „křivák" by bylo výstižnější.

Místo toho, aby pracoval pro někoho, rozhodl se, že bude pracovat pro sebe. Měl v úmyslu otevřít si obchod, kde by mohl celý den klidně sedět a nemusel se neustále honit z místa na místo. Chtěl dělat pouze takové obchody, ze kterých by měl jisté příjmy.

Jaký obchod si zvolit? To bylo zrovna dost jednoduché. Vyzná se v opravách aut, takže si otevře obchod s náhradními díly.

A záruka úspěchu? Řešení ho napadlo hned: přesvědčit velkoobchod Honorable Auto Parts, aby mu prodával zboží za cenu jejich nákladu.

Samozřejmě to asi sami od sebe nebudou chtít udělat. Anthony ale znal cesty, jak přechytračit lidi, a jeho kamarád Mickey věděl, jak se nabourat do cizích počítačů. Společně vypracovali mazaný plán.

Toho podzimního dne se přesvědčivě představil jako Peter Milton, zaměstnanec firmy, dostal se dovnitř podniku a podařilo se mu připojit svůj notebook do vnitřní sítě. Do této chvíle plán fungoval, ale to byl jen první krok. To, co ještě musel udělat, nebylo jednoduché, zvláště proto, že se Anthony chtěl vejít do patnácti minut — každá sekunda navíc bv zvyšovala riziko jeho odhalení.

Ještě dříve však uskutečnil telefonát, ve kterém se představil jako technik dodavatele počítačů a sehrál malé představení.

„Vaše firma si zaplatila dvouletý servis a chtěli bychom si vás zapsat do databáze, abychom věděli, když se objeví nové verze, jaké programy používáte. Potřebovali bychom tedy seznam aplikací, které používáte."

Jako odpověd dostal seznam programů a jeho kolega určil jako cíl útoku jeden z nich, MAS90. Tento program udržoval seznam odběratelů spolu s rabaty a platebními podmínkami pro každého z nich.

S touto klíčovou znalostí v ruce spustil program, který identifikuje všechny aktivní počítače v síti. Netrvalo dlouho a našel server, který používala účtárna. Z arzenálu hackerských programů, které měl v notebooku, si vybral jeden, který zjistil všechny oprávněné uživatele serveru. Pomocí dalšího programu se pokoušel použít typicky zadávaná hesla jako *nic* nebo *heslo*. Slovo *heslo* zabralo. Nic divného. Lidé jaksi ztrácejí fantazii, když si mají vymyslet heslo.

Uběhlo teprve šest minut a už byl v polovině cesty. Dostal se na server.

Další tři minuty pečlivě vpisoval do seznamu klientů údaje o své firmě: název, adresu, telefon a jméno kontaktní osoby. Posléze v klíčovém políčku, o což vlastně v celé akci šlo, vložil údaj, že mu bude všechno zboží prodáváno s marží jedno procento.

Všechno to stihl za necelých deset minut. Když odcházel, zastavil se na chvíli u Kaily, aby jí poděkoval, že mu umožnila projít si poštu, pověděl jí, že se spojil s Mikem Talbotem, že se plán změnil a jede rovnou ke klientovi na jednání. Dodal, že ji nezapomene doporučit na tu pozici v marketingu.

Analýza podvodu

Vetřelec vydávající se za Petera Miltona použil dvě techniky psychologickě diverze — první byla plánovaná a druhá spočívala v improvizaci na okamžitou situaci.

Oblékl se tak, aby vypadal jako někdo z managementu, kdo si dost vydělává. Oblek, kravata, náležitý účes a dobrý střih — mohlo by se zdát, že to jsou maličkosti, ale právě ty vytvářejí odpovídající dojem.

Přesvědčil jsem se o tom na vlastní kůži. Krátký čas jsem pracoval jako programátor v GTE — již neexistující velké telekomunikační firmě, která sídlila v Kalifornii. Tam jsem objevil, že když jsem někdy přišel do práce bez identifikátoru, dobře, ale neformálně oblečený — řekněme košile a bavlněné kalhoty — hned mne zastavili a ptali se mne, kde mám identifikátor, kdo jsem a kde pracuji. Jiný den jsem se objevil také bez identifikátoru, ale v obleku a kravatě, velmi reprezentativně oblečený. Podle starého triku jsem se vmísil do davu přicházejícího do budovy či procházejícího vrátnicí. „Nalepil" jsem se k nějaké skupince když přicházeli k hlavnímu vchodu, a vešel jsem, jako bych k nim patřil Prošel jsem, a i kdyby si strážný všiml, že nemám identifikátor, určitě by mne nezadržel, protože jsem vypadal jako někdo z vedení a vešel jsem zároveň s osobami, které identifikátory měly.

Tato zkušenost mne poučila, jak moc je chování strážných předvídatelné. Stejně jako my všichni činí odhady na základě vzhledu člověka. Je to slabina, kterou sociotechnici bez milosti využívají.

Druhá psychologická zbraň se objevila v rukou útočníka, když si všiml neobyčejného výkonu recepční. Zabývala se několika věcmi najednou a nejen, že ji to neiritovalo, ale ještě dala každé osobě znát, zejí věnuje plnou pozornost. Vnímal to jako vlastnost osoby, která je zainteresovaná kariérou a rozvojem. Když potom prohlásil, že je z odboru marketingu, pozoroval její reakci, jestli nespatří nějaké znamení bližšího kontaktu mezi nimi. Zřejmě se povedlo. Tak si získal osobu, kterou mohl zmanipulovat slibem pomoci dostat se k lepší práci (samozřejmě, kdyby řekla, že vždycky chtěla pracovat v účtárně, tvrdil by, že má na příslušném odboru kontakty a mohl by se pokusit sehnat jí tam práci).

Vetřelci rádi používají ještě jednu psychologickou zbraň. Budují si důvěru pomocí dvoustupňového útoku. Útočník nejprve zahájil rozhovorem na téma práce v marketingu; příležitostně nadhazoval jména jiných skutečně existujících pracovníků. Jméno, které používal, bylo také jméno jednoho opravdového zaměstnance.

Po takto započaté konverzaci mohl v zásadě ihned přejít k prosbě o zpřístupnění konferenční místnosti. On se však namísto toho na chvíli posadil v hale a dělal, že pracuje a čeká na svého kolegu. Byl to další způsob, jak

zaplašit eventuální podezření — vetřelec by asi spíš nechtěl pobývat delší dobu na takovém místě. Neseděl tam však příliš dlouho, sociotechnici dobře vědí, že je vhodné být „na místě činu" jen tak dlouho, kolik je nutné.

Podle zákonů-nespáchal Anthony zločin, když vstoupil do foyer firmy. Žádost o zpřístupnění konferenční místnosti také nebyla v rozporu se zákonem. Samotné připojení do počítačové sítě a vyhledával serveru také nebylo přestupkem.

Anthony porušil zákon teprve tehdy, když se naboural do firemního počítačového systému.

Poznámka Mitnicka
****
Vpouštění cizích osob do míst, kde je možnost připojit se do firemní sítě, zvyšuje riziko narušení bezpečnosti. Žádost pracovníka o využití konferenční místnosti za účelem stažení pošty je absolutně odůvodněná, zejména když daná osoba přijela z jiné pobočky. Jestliže však toho člověka neznáme osobné a síť není segmentována tak, aby předcházela neautorizovaným připojením, může se ukázat, že je zde slabý článek ohrožující firemní data.
****

Špehování Mitnicka

Když jsem před mnoha lety pracoval v jedné nevelké firmě, všiml jsem si něčeho zvláštního. Vždy, když jsem vcházel do místnosti, kterou jsem sdílel se třemi kolegy informatiky, jeden z nich (říkejme mu Joe) rychle přepínal obrazovku na jiné okno. Hned se mi to zdálo podezřelé. Když už se to stávalo častěji než dvakrát denně, byl jsem si jistý, že se děje něco, o čem bych se měl dozvědět. Co to tam dělal, že to chtěl přede mnou tajit?

Joeův počítač fungoval jako terminál na přístup do firemního minipočítače, takže jsem na minipočítači VAX nainstaloval monitorující program, díky němuž jsem mohl sledovat, co Joe dělá. Program fungoval téměř tak, jako kdybych Joeovi postavil za rameno videokameru. Viděl jsem přesně to, co viděl on na svém monitoru.

Můj stůl stál hned vedle jeho stolu, obrátil jsem tedy monitor tak, abych mu trochu zakryl obraz. Přesto mohl Joe každou chvíli vzhlédnout a odhalit, že ho špehuji. To však nebyl žádný problém — byl příliš zaujatý tím, co dělal, než aby si čehokoli všiml.

Když jsem ho začal sledovat, spadla mi čelist a bez hlesu jsem koukal, jak si ten syčák Joe prohlíží údaje o mých výplatách!

Pracoval jsem tu teprve pár měsíců a Joe by asi nesnesl, kdyby se ukázalo, že si vydělám více než on.

O několik minut později jsem viděl, jak si ze sítě stahuje hackerské nástroje používané méně zkušenými hackery, kteří nesvedou natolik programovat, aby si takové nástroje vytvořili sami. Joe tedy žil v nevědomosti — neuvědomoval si, že vedle něho sedí jeden z nejzkušenejších hackerů na světě. V podstatě to bylo zábavnné.

Nemohl jsem ho zastavit, protože informace o mých výdělcích už stačil získat. Kromě toho každý pracovník s přístupem do databáze IRS nebo úředník pracující na Správě sociálního zabezpečení se může na mé příjmy podívat. Neměl jsem v úmyslu dávat mu najevo, že vím, co dělal. V té době bylo mým hlavním cílem zůstávat ve stínu. Dobrý sociotechnik se nechlubí svými dovednostmi a znalostmi. Chce být podceňován a nechce, aby v něm lidé viděli nebezpečí.

Proto jsem ho nechal být a v duchu jsem se smál tomu, že se Joeovi zdálo, že něco o mně ví, zatímco to bylo úplně naopak. Měl jsem nad ním převahu, když jsem věděl, co dělá.

Brzy jsem odhalil, že všichni moji spolupracovníci se bavili tím, že si prohlíželi výdělky té či oné krásné sekretářky nebo (jedním z těch informatiků byla žena) nějakého svalnatce. Byli schopni přečíst vydělky i odměny každé osoby v podniku včetně členů vedení.

Analýza podvodu

Tento příběh ilustruje zajímavý problém. Soubory s údaji o mzdách byly přístupné každému, kdo se zabýval správou počítačového systému firmy. Všechno nás tedy přivádí k personálním záležitostem, k výběru důvěryhodných osob. Občas informatici nemohou odolat čmuchání kolem. Mají k tomu odpovídající oprávnění umožňující jim obejít zabezpečení přístupu k souborům.

Jedním z možných zabezpečení by mohlo být sledování přístupu k obzvláště důvěrným souborům, jako je například seznam mezd. Samozřejmě každý s příslušnými oprávněními by mohl toto sledování deaktivovat nebo mazat protokoly, které by mohly umožnit odhalení pachatele. Každé dodatečné zabezpečení však zvyšuje úsilí, které musí zvědavec vynaložit, aby nebyl odhalen.

Prevence

Prohrabáváním popelnic počínaje a voděním strážných či recepčních za nos konče, dokáže sociotechnik proniknout na území naší firmy. Existují však prostředky, které nám pomohou se před tím ochránit.

Po pracovní době

Všichni zaměstnanci, kteří se objeví v práci bez identifikátoru, musejí být zadrženi v recepci nebo na vrátnici a musejí dostat dočasný identifikátor na daný den. Incident popsaný v prvním příběhu této kapitoly by mohl mít úplně jiný konec, kdyby ochranka měla povinnost postupovat podle pokynů přijatých pro případ zpozorování osoby bez identifikátoru.

Ve firmách nebo v těch částech firem, kde zabezpečení areálu nehraje tak velkou roli, nemusí mít identifikátor až tak velký význam. V případě, kdy jsou v areálu firmy zóny nepřístupné cizím lidem, by měly být identifikátory striktně vymáhány. Zaměstnanci musejí být proškolení a motivovaní, aby zastavovali osoby, které identifikátor nemají. A osoby vyšších pozicích musejí žádosti tohoto typu ze strany níže postavených zaměstnanců akceptovat, aniž by jim dělali potíže.

Bezpečnostní politika by měla připomínat postihy, které hrozí za notorické objevování se bez identifikátoru. Takovým postihem by mohlo být odeslání pracovníka na jeden den domů bez nároku na mzdu nebo záznam v osobních spisech. Některé podniky zavádějí progresivní systém postihů, mezi kterými může být informování nadřízeného dané osoby nebo písemná důtka.

Navíc pro místa, kde je přístup k chráněným informacím, by měla firma zavést pravidla pro osoby, které tam chtějí vejít po pracovních hodinách. Jedním z řešení je například požadavek předchozího oznámení této potřeby strážným nebo k tomuto účelu určené organizační jednotce. Tato jednotka by pak měla ověřit totožnost osoby žádající o vstup telefonátem jejímu vedoucímu nebo jiným bezpečným způsobem.

Úcta k odpadkům

Příběh o odpadcích ukázal, jak je možné s nekalými záměry využívat dokumenty, které končí v popelnici. Zde je devět klíčových pravidel, jak nakládat s odpadky:

- Zařaď všechny důvěrné informace do jednotlivých kategorií podle stupně jejich důvěrnosti.
- Zaveď v celé firmě pokyny, jak se zbavovat dokumentů obsahujících taková data.
- Vyžaduj, aby byl každý důvěrný dokument před vyhozením zničen.
- Nepoužívej levné skartovačky, které řežou dokumenty na proužky. Ty by mohl odhodlaný lovec informací při troše štěstí poskládat dohromady. Existují lepší skartovačky, které změní dokument na neužitečnou drť.
- Najdi způsob, jak ničit nebo *kompletně* mazat datové nosiče, čili diskety, zip disky, CD ROM i DVD obsahující soubory, výměnné pásky, staré disky, než budou vyhozeny. Je třeba mít na paměti, že mazání souborů ve skutečnosti nemaže obsah nosiče – je možné obnovení dat – o čemž se s hrůzou kdysi přesvědčilo vederu koncernu Enron, a nejen oni. Obvyklé vyhazování disket do koše je pozvánkou pro místního „smetištního potápěče". (Do 16. kapitoly byly zahrnuty podrobné pokyny týkající se zbavování se nosičů a zařízení.)
- Udržuj příslušnou úroveň kontroly nad výběrem uklízecího personálu, v případě potřeby kontroluj jejich činnost.
- Připomínej zaměstnancům, aby se zamýšleli nad tím, jaké materiály vyhazují do koše.
- Zamykej kontejnery s odpadky.
- Měj oddělené kontejnery na důvěrné materiály a najmi si firmu, která se zabývá účinným ničením odpadů tohoto typu.

Propouštění pracovníků

Již dříve jsem se v této kapitole zmínil o nutnosti existence pravidel pro propouštění zaměstnanců, kteří mají přístup k důvěrným informacím, heslům, přístupovým číslům a podobně. Bezpečnostní procedury by měly poskytovat možnost průběžné kontroly, kdo má přístup k různým systémům. Možná je zadržení odhodlaného sociotechnika před vniknutím do systému obtížné, ale alespoň to našim bývalým pracovníkům neulehčujme.

Nezapomínejme rovněž, že pokud byl propuštěný zaměstnanec oprávněný vyzvedávat záložní kopie od firmy, kterou máme na zálohování najatou, je třeba ho ze seznamu oprávněných lidí vyškrtnout.

V 16. kapitole lze najít podrobné informace k tomuto tématu. Zde si uvedeme pouze klíčové body, které bychom měli uplatňovat, abychom se vyhnuli situacím popsaným v této knize:

- Vyčerpávající a podrobný seznam kroků, které je třeba uskutečnit během propouštění zaměstnance, se speciálními klauzulemi týkající se osob, které měly přístup k citlivým informacím.
- Příkaz k okamžitému ukončení přístupu pracovníka k počítači – nejlépe ještě než opustí budovu.
- Procedura odevzdání všech identifikátorů a klíčů a elektronických přístupových zařízení.
- Bod, který přikazuje strážným požadovat od příchozích, kteří nemají identifikátor, doklad totožnosti s fotografií a ověřit jejich jméno na seznamu pracovníků, jestli jsou ve firmě opravdu zaměstnáni.

Některé další kroky mohou pro některé organizace být nepotrebné nebo příliš drahé, pro jiné však mohou být užitečné. Zde jsou některé z přísnějších bezpečnostních prostředků:

- Elektronické identifikátory a jejich čtečky při vchodech. Každý zaměstnanec přikládá svůj identifikátor ke čtečce, která ihned pozná, jestli je daná osoba ještě zaměstnána a jestli má právo vejít do budovy. (Je třeba proškolit strážné, aby si všímali osob, které se pokoušejí proniknout přes bránu těsně za pracovníkem oprávněným ke vstupu.)
- Požadavek, aby si všichni pracovníci oddělení, kde pracovala odcházející osoba (zvláště, jestli byla propuštěna) změnili heslo. (Přeháním? Mnoho let poté, co jsem krátce pracoval v General Telephone, jsem se dozvěděl, že když lidé zabývající se bezpečností v Pacific Bell, uslyšeli, že pracuji pro General Telephone, tak se váleli smíchy. Firmě General Telephone však budiž připsáno k dobru, že když se dozvěděla, Že zaměstnala známého hackera, dostal jsem ihned výpověď, přičemž byla *každému pracovníkovi firmy* nařízena změna hesla.)

Nechceme, aby naše firma připomínala vězení, ale na druhou stranu se musíme chránit před propouštěnými osobami, které se mohou vrátit s úmyslem způsobit škodu.

Na nikoho nezapomeň

Bezpečnostní pravidla mají často tendenci přehlížet takové osoby jako jsou recepční, které nemají přístup k citlivým informacím. Už jsme si jistě všimli během četby některé z předchozích kapitol, že recepční jsou pohodlným cílem útoku. V této kapitole popsaná příhoda nabourání se do sítě velkoobchodu s náhradními díly je další takový příklad. Milý, dobře oblečený člověk, který se představuje jako pracovník jiné pobočky, nemusí nutně být tím, za koho se vydává. Recepční se musí naučit jemně poprosit o identifikaci, když to situace vyžaduje. Školením tohoto typu musejí projít nejen recepční, ale také osoby, které za ně občas u pultu zaskakují.

Od hosta zvenku by se měl vyžadovat doklad totožnosti s fotografií a údaje z předloženého dokladu by se měly zapisovat. Získání falešnéh dokladu sice není příliš těžké, ale už to vyžaduje od útočníka další úsilí.

V některých firmách je smysluplné zavést povinnost doprovázet hosta z vrátnice a od setkání k setkání. Pravidla by měla vyžadovat aby eskorta doprovázející hosta na místo prvního setkání vysvětlila jestli osoba vešla do areálu firmy jako pracovník nebo jako osoba zvenku. Proč je to důležité? Jak jsme viděli v předchozích příbězích útočník se často představuje jako jedna osoba, aby se dostala na první schůzku, a potom hraje někoho úplně jiného. Pro útočníka je příliš snadné přijít jen tak do recepce a říct, že má schůzku, řekněme, s inženýrem. Jakmile ho doprovod dovede k inženýrovi, představí se jako obchodník, který by chtěl firmě něco prodat, a po schůzce s inženýrem má volný pohyb po areálu firmy.

Před vpuštěním pracovníka firmy z jiné lokality by se mělo ověřovat podle příslušné procedury, jestli je skutečně zaměstnancem firmy.

Osoby pracující v recepci nebo na vrátnici musejí být seznámeny s tím, jaké metody útočníci používají, když se vydávají za někoho jiného, aby se dostali se do areálu podniku.

Jak se bránit před vetřelci, kterým se podaří dostat do budovy a připojit svůj notebook k síti, vyhýbaje se tak firemnímu firewallu? V současnosti to vyžaduje hodně úsilí — konferenční, školící a podobné místnosti by neměly mít nezabezpečené porty vnitřní sítě, ale měly by byt chráněné firewallem či

routerem. Ale lepší ochranou by mohlo byt ověřování každého uživatele, který se chce nalogovat do sítě.

Bezpeční informatici

Je dobré mít na paměti, že v naší firmě každý informatik ví nebo se může kdykoli dozvědět, kolik vydělláváme my nebo nejvyšší management i kdo si vyjel na lyže služebním autem.

V některých firmách se může dokonce stát, že informatici nebo účetní si budou zvyšovat platy, vyplácet peníze na konta falešných dodavatelů, mazat nežádoucí zápisy ze svých osobních spisů. Někdy pouhý strach před dopadením způsobí, že zůstanou poctiví. Až konečně jednoho dne se mezi nimi objeví člověk tak chtivý a nepoctivý, že nebude dbát na riziko a udělá všechno, co mu podle jeho mínění projde.

Samozřejmě i na to existuje řešení. Důvěrné soubory mohou být chráněné instalací příslušných nástrojů kontroly přístupu, které povolí jejich čtení pouze oprávněným osobám. Některé systémy mají nástroje umožňující sledování operací.

Ty mohou být nakonfigurované tak, že se uchovávají logy s jistými událostmi, například každý pokus o otevření chráněného souboru kýmkoli, ať už pokus skončil úspěšně či ne.

Jestli si vaše firma uvědomila tento problém a zavedla příslušné prostředky kontroly přístupu a sledování operací s citlivými soubory, lze říci, že jste tím učinili obrovský krok správným směrem.

11

Sociotechnika a technologie

Sociotechnik využívá svou schopnost manipulace s lidmi takovým způsobem, aby mu pomáhali v dosahování jeho vlastních cílů. Úspěch však ve velké míře záleží také na jeho znalostech v oblasti počítačových a telefonních systémů.

Zde jsou příklady typických sociotechnických podvodů, kde technologie hrály důležitou roli.

Jak se dostat do vězení?

Co myslíte, které objekty jsou nejlépe zabezpečené, ať už před vloupáním fyzickým, telekomunikačním či elektronickým? Fort Knox? Samozřejmě. Bílý dům? Jistě. NORAD, severoamerická instalace vzdušné obrany ukrytá hluboko v nitru hory? Určitě.

A co vězení? Ta musejí být také dobře zabezpečena, ne? Jen zřídkakdy z nich někdo utíká a i když třeba uteče, brzy ho chytí. Člověk by usuzoval, že tyto objekty budou vůči sociotechnickým útokům imunní... Ale to by byl omyl — neexistuje žádné zabezpečení odolné vůči lidské tuposti.

Před několika roky se dvojice profesionálních podfukářů dostala do nesnází. Ukázalo se, že vytáhli docela slušnou částku peněz z místního soudce. Potíže se spravedlností mívali čas od času už léta, ale ted se záležitostí začali zabývat federální agenti, kterým se podařilo jednoho z podvodníků, Charlese Gondorffa, polapit a umístit ho v resocializacním středisku poblíž San Diega. Federální smírčí soudce nařídil jeho vazbu s odůvodněním, že jde o společensky nebezpečnou osobu.

Jeho kumpán, Johny Hooker, věděl, že Charlie bude potřebovat dobrého advokáta, ale kde na něj vzít peníze? Jako většina podvodníků peníze, které od lidí vymámili, rychle utráceli: za značkové oblečení, sportovní auta a ženy. Johny ted měl sotva na živobytí.

Peníze na advokáta musel tedy získat pomocí dalšího podvodu a Johny neměl v úmyslu jít do toho sám. Právě Charlie Gondorff byl vždycky mozkem jejich akcí. Nemohl, bohužel, navštívit kamaráda v nápravném zařízení a zeptat se ho, co má dělat. Zvláště když FBI věděla, že se podvodů účastnily dvě osoby a ráda by chytila i tu druhou. Tím spíš, že právo na návštěvy má pouze rodina, což znamenalo, že by se musel vydávat za příbuzného a musel by mít také falešný doklad totožnosti. Ohánět se falešným dokumentem ve federálním vězení asi není to pravé ořechové.

Ne, musel najít jiný způsob, jak se svým společníkem zkontaktovat.

Nebylo to jednoduché. Žádný vězeň nemá právo přijímat telefonáty. U každého telefonu určeného vězňům je cedulka s nápisem: „Pozor! Všechny hovory na tomto přístroji jsou monitorovány. Používáním tohoto přístroje vyjadřujete souhlas s monitorováním vedeného hovoru." Kdyby federální agenti slyšeli, jak si telefonicky domlouvají podrobnosti další akce, jistě by zajistili potřebné fondy na nucenou dovolenou za státní peníze.

Johny však věděl, že některé rozhovory odposlouchávané nejsou. Například hovory s advokátem, kde je soukromí zaručeno ústavou. Středisko, ve kterém Gondorff pobýval, mělo telefony propojené přímo do kanceláří Úřadu veřejných obhájců; zvednutí sluchátka jednoho z takových přístrojů způsobilo přímé spojení s některou z linek v úřadu Telekomunikační firmy nazývají něco takového *pevné směrování hovorů*. Nic netušící vězeňská stráž předpokládá, že tato služba je bezpečná, protože odchozí hovory mohou být směrované výlučně do kanceláří advokátů a příchozí jsou zablokované. I kdyby se někomu zvenku

podařilo nějak získat číslo toho telefonu, k ničemu mu to není, protože na tomto čísle je na ústředně nastavené *blokování spojení*.

Žargon
****
pevné směrování hovorů — takové telefonické spojení, kdy zvednutí sluchátka způsobí spojení s jedním, pevně určeným číslem.
Blokování spojení — servisní volba telefonní ústředny, která znemožňuje na daném čísle přijímání hovorů.
****

Každý poměrně dobrý podvodník dokáže manipulovat, takže Johny přišel k závěru, že se problém dá obejít. Gondorff už jednou zkoušel zvednout sluchátko telefonu do kanceláře advokátů a říct:

Tady je Tom, ze servisního střediska telekomunikací. Provádíme na této lince test a chtěl jsem vás požádat, abyste vytočili devítku a potom dvakrát nulu."

Devítka znamenala spojení ven a dvě nuly pak dovolovaly spojit se s meziměstským operátorem. Nepodařilo se. Osoba, která telefonát přijala, už tu fintu znala.

Johny mu se dařilo o něco lépe. Podařilo se mu zjistit, že ve vězení je deset budov a z každé z nich vedla jedna linka do úřadu veřejných obhájců. Po cestě viděl několik překážek, ale jako sociotechnik si s nimi dokáže poradit. Ve které budově je Gondorff? Jaké je číslo telefonu s přímým spojením v této budově? Jak dát Gondorffovi první echo, aby se to nedoneslo bachařům?

To, co by se obyčejným lidem mohlo zdát nemožné, například zjištění tajných telefonních čísel ve federálních institucích, častokrát nevyžaduje víc, než několik telefonátů, uskutečněných sociotechnikem na slovo vzatým. Po několika bezesných nocích strávených vymýšlením postupu jednoho rána vstal John z postele s určitým plánem. Skládal se ze čtyř etap.

Nejprve musel získat „normální" telefonní čísla na veřejné advokáty. Musel se dozvědět, ve které budově se Gondorff nachází. Pak bylo nutné najít číslo do toho baráku.

A konečně musel tajně předat Gondorffovi zprávu, kdy má očekávat telefon.

Brnkačka, pomyslel si.

Volám ze servisu

Johny začal telefonátem do telekomunikační firmy. Předstíral, že volá z Hlavní administrace služeb, agentury odpovědné za nákup zboží a služeb pro federální organizace. Řekl, že dostal objednávku na dodatečné služby a potřebuje informace z fakturací za všechna aktuálně používaná přímá spojení zároveň s jejich telefonními čísly a měsíční náklady pro resocializační centrum v San Diegu. Slečna na druhém konci ráda pomohla.

Pro jistotu zkusil zavolat na jednu z takto získaných linek a uslyšel zprávu: „Stanice s tímto číslem byla zrušena" — což samozřejmě nebyla pravda, ale věděl, že takováto zpráva se objevuje po zablokování příchozích hovorů. Přesně toto očekával.

Díky svým rozsáhlým znalostem postupů a činnosti telekomunikačních firem věděl, že se musí dovolat do oddělení nazvaného Centrum autorizací nových změn, tedy CANZ (vždycky mě zajímalo, kdo takové názvy vymýšlí!). Nejprve zavolal na telekomunikace, řekl, že telefonuje ze servisu a potřebuje číslo na CANZ, které má na starosti území s prefixem a směrovým číslem, které uvedl. Počáteční číslice vystupovaly ve všech přímých linkách resocializačního centra. Byla to vnitřní žádost. Tato informace byla montérům v terénu poskytována často, takže mu úřednice číslo bez zaváhání sdělila.

Zavolal CANZ, uvedl vymyšlené jméno a znovu řekl, že je ze servisu. Poprosil ženu, která zvedla telefon, aby zkontrolovala jedno z telefonních čísel, které předtím vymámil.

„Nemá to číslo nastavené blokování příchozích hovorů?" zeptal se Johny.

„Má," odpověděla.

„Aha, no tak to vysvětluje, proč se k zákazníkovi nikdo nemůže dovolat," řekl. „Mohla byste pro mne něco udělat? Musím změnit kód třídy linky a odstranit blokování příchozích hovorů."

Nastala pauza, kdy telefonistka ověřovala, jestli byla vystavena servisní objednávka, která by tuto změnu autorizovala.

„Tato linka *by měla* mít pouze odchozí spojení," řekla po chvíli. „Nemám tady servisní objednávku na takovou změnu."

„Nemáte, to je chyba. Měli jsme vystavit tu objednávku včera, ale člověk, který to má na starosti, je na neschopence a zapomněl to předat někomu jinému. A klient je už poněkud nervózní."

Žena na druhém konci chvíli přemýšlela o prosbě, která šla nad rámec běžných postupů a nakonec řekla:

„Dobrá."

Slyšel, jak ťuká do klávesnice a nastavuje změnu. Po několika sekundách bylo všechno hotovo.

Ledy byly prolomeny a spoutal je jistý druh spiklenectví. Cítil postoj a ochotu pomoci a tak Johny rychle přešel k síti.

„Mohla byste mi věnovat ještě pár minut?" zeptal se.

„Ano," odpověděla. „O co jde?"

Mám tu ještě několik jiných linek téhož klienta s tím samým problémem" já bych vám přečetl čísla a vy byste ověřila, jestli nejsou zablokované, ano?"

Souhlasila.

0 několik minut později byly už všechny linky „opravené" a bylo možné přijímat příchozí hovory.

Hledání Gondorffa

Ted bylo třeba najít budovu, ve které pobývá Gondorff. To je informace, kterou pracovníci věznice určitě nebudou chtít prozradit. Johny se musel opět spolehnout na své sociotechnické schopnosti. Zatelefonoval do federální věznice v jiném městě — vybral si Miami, ale stejně tak dobře si mohl vybrat kterékoliv jiné — a řekl, že volá z jiné věznice v New Yorku. Poprosil o spojení s někým, kdo pracuje s rejstříkem vězněných — databází obsahující informace o každém vězni umístěném v kterémkoli vězení na území USA.

Když dostal spojení, Johny začal mluvit s brooklynským přízvukem.

„Dobrý den," řekl. „Tady Thomas z FDC v New Yorku. Naše spojení s rejstříkem každou chvíli padá, mohl byste mi lokalizovat jednoho vězně? Myslím, že je ve vašem vězení."

Uvedl jméno Gondorffa a jeho registrační číslo.

„Ne, u nás není," odpověděl po chvíli muž na druhém konci. „Je v San Diegu."

Johny hrál překvapení.

„V San Diegu? Přece měl být minulý týden přemístěn do Miami vojenským letadlem! Je to opravdu ten vězeň? Jaké je jeho datum narození?"

„12.3.1960," přečetl protějšek z obrazovky.

„Ano, je to on. Ve kterém je baráku?"

„V desátém, severní křídlo," slyšel ihned odpověd, přestože nebyl žádny rozumný důvod, proč by to mělo pracovníka vězení z New y°rku zajímat.

Johny už odblokoval linku a dozvěděl se, kde je Gondorff. Teď bylo na radě zjistit, která telefonní linka vede do budovy číslo 10.

To bylo trochu obtížnější. Johny zavolal na jedno z čísel. Věděl, že zvonek je vypnutý a přístroj na druhé straně bude mlčet. Pohodlně se usadil, zabral se do čtení průvodce *Evropská města* a poslouchal při tom vyzváněcí

tón. Po nějaké době někdo na druhé straně zvedl sluchátko. Zjevné se nějaký vězeň chtěl spojit se svým obhájcem. Johny byl na to připraven.

„Kancelář veřejných obhájců," ohlásil se. Když se muž zeptal na svého obhájce, Johny odpověděl: „Podívám se, jestli tu je. A ze kterého baráku voláte?" Zaznamenal si odpověď, potom zaparkoval hovor a než uplynulo půl minuty, k hovoru se vrátil:

„Je u soudu, musíte zavolat později," oznámil a zavěsil.

Čekal několik hodin, ale nebylo to zas tak hrozné. Ukázalo se, že čtvrtý volající byl z budovy číslo 10. Takto Johny zjistil číslo telefonu do budovy, ve které přebýval Gondorff.

Seřiďme si hodinky

Teď bylo nutné předat Gondorffovi zprávu, kdy má zvednout sluchátko které vede přímo do kanceláře advokátů. Bylo to lehčí, než by se mohlo zdát.

Johny zavolal do nápravného zařízení a oficiálním tónem se představil jako pracovník vězení a požádal o budovu číslo 10. Byl přepojen. Když důstojník zvedl sluchátko, Johny ho oklamal žargonovou zkratkou oddělení příjmů a propouštění, které zařizuje záležitosti spojené s příjmem a propouštěním vězňů:

„Tady je Tyson z PaPu," řekl. „Prosil bych k telefonu vězně Gondorffa. Máme tu jeho věci, které musíme poslat a chceme se zeptat, na jakou adresu. Mohl bych ho dostat k telefonu?"

Johny slyšel, jak služba volá vězné. Po několika netrpělivých minutách uslyšel ze sluchátka známý hlas. Johny se ozval:

„Nic neříkej, dokud ti nevysvětlím, o co jde." Pak mu objasnil záminku rozhovoru, aby Gondorff mohl předstírat, že hovoří o tom, kam se mají poslat jeho věci. Potom řekl:

„Jestli se můžeš dnes okolo třinácté dostat k telefonu obhájců, nic neodpovídej. Jestli nemůžeš, řekni hodinu, kdy bys tam mohl byt." Gondorff nic neříkal. Johny pokračoval:

„Dobrá. Bud tam tedy v jednu, já budu volat. Zvedni sluchátko a jestli se začne spojovat s advokáty, zavěs a zkus to znovu za dvacet sekund. Zkoušej to tak dlouho, dokud mě neuslyšíš."

V jednu hodinu Gondorff zvedl sluchátko. Johny už na něj čekal. Mluvili dlouho, beze spěchu, domlouvali se ha následující hovory, aby naplánovali akci, která by přinesla peníze na zaplacení Gondorffova advokáta — a to všechno bez vládního odposlechu.

Analýza podvodu

Epizoda představuje prvotřídní ukázku toho, jak sociotechnik dělá nepředstavitelné věci. Jak oklame několik osob a každá z nich pak udělá něco, co samo o sebe nevzbuzuje žádné podezření. Ve skutečnosti každá z těchto činností představuje jeden prvek skládanky, až vytvoří celou intriku.

Pracovnice telekomunikací si myslela, že poskytuje informace někomu z Hlavní administrace služeb federální vlády.

Další pracovnice telekomunikací věděla, že by linkám neměla měnit třídy služeb bez objednávky, ale rozhodla se pomoci přátelskému člověku. Díky tomu se umožnilo volání na všech deset linek určených jen rozhovorům mezi vězni a jejich obhájci.

Člověku z miamské věznice se zdála žádost o pomoc ze strany pracovníka jiného federálního vězení, který měl problémy s počítačem, úplně odůvodněná. Dokonce i kdyby neviděl žádný rozumný důvod ptát se na číslo budovy, proč by na ten dotaz neodpověděl?

A co s pracovníkem v budově číslo 10, který uvěřil, že mu volá kolega z téhož vězení ve služební záležitosti? Žádost byla úplně normální, takže Gondorffa zavolal k telefonu. Nic významného. Série naplánovaných akcí se složila do plného obrazu intriky.

Rychlá kopie

Deset let po ukončení svých právnických studií potkával Ned Racine své spolužáky z ročníku, kteří bydleli v krásných domech se zahradami, patřili do různých klubů, jednou nebo dvakrát týdně hráli golf, zatímco on sám se zabýval záležitostmi lidí, kteří neměli peníze ani na to, aby naplatili jeho faktury. Občas nás zevnitř sžírá závist. Až konečně jednoho dne měl Ned toho všeho dost.

Jediným dobrým klientem, kterého kdy měl, byla malá, ale velmi

pružná účetní firma, která se specializovala na fúze a akvizice. Využívali Nedových služeb teprve krátce, ale už se stihl zorientovat, že se angažují v transakcích, které – jakmile se informace o nich dostanou do sdělovacích prostředků – ovlivní ceny jedné nebo dvou společností na burze. Nebývali to velké společnosti, ale to je možná lepší – malý cenový skok tu mohl znamenat velký procentní přírůstek zisků z investic. Jenom by se musel nějak dostat k jejich souborům a kouknout se, na čem právě pracují...

Znal člověka, který zase znal jiného člověka, který se vyznal v různých podivných věcech. Jakmile si ten plán poslechl, ihned se pro věc zapálil a přislíbil pomoc. Za nižší cenu než obvykle, ale za příslib procentního podílu na zisku z operací, poradil tento člověk Nedovi, co je třeba učinit. Dal mu též malé šikovné udělátko – novinku na trhu.

Několik dní po sobě pozoroval Ned parkoviště menší obchodní zóny, kde si účetní společnost pronajímala neokázalé místnosti. Většina lidí vycházela mezi půl šestou a šestou. V sedm večer bylo již parkoviště prázdné. Parta úklidové firmy se objevovala okolo půl osmé. Dokonalé.

Následujícího večera zaparkoval Ned pár minut před osmou na ulici naproti parkovišti. Jak očekával, bylo parkoviště prázdné, kromě auta ochranky. Ned přiložil ucho ke vstupním dveřím a uslyšel zapnutý vysavač. Hlasitě zaklepal a čekal oblečený v obleku a kravatě, s obnošeným kufříkem v ruce. Nikdo neotevíral, tak zaklepal znovu. Po chvíli se ve dveřích objevil jeden z uklízečů.

„Dobrý den," křičel Ned přes skleněné dveře a ukazoval přitom vizitku jednoho ze spoluvlastníků firmy, kterou kdysi dostal. „Zabouchl jsem si klíčky v autě a musím se dostat do svého stolu."

Muž otevřel dveře, opět je za Nedem zamkl a šel po chodbě a rozsvěcoval světla, aby Ned viděl na cestu. Proč by ne – měl příležitost pomoci člověku, díky kterému má práci. Nebo alespoň měl všechny důvody. aby si myslel, že tomu tak je.

Ned se usadil k počítači jednoho ze spoluvlastníků a spustil ho. Když se počítač rozběhl, připojil k USB portu to udělátko, které dostal – byl to předmět, který by mohl sloužit jako přívěsek ke klíčům, ale zároveň se na něj vešlo více než 120 MB dat. Přilogoval se do sítě pomocí uživatelského jména a hesla sekretářky spoluvlastníka. Tyto informace byly z pohodlnosti přilepené na monitor na kousku papíru. Než uplynulo pět minut, stihl Ned nahrát všechny dokumenty a excelovské sešity umístěné na počítači i v sítovém adresáři spolupracovníka a už se vracel autem domů.

Poznámka Mitnicka
****
Průmysloví špióni nebo hackeři se občas snaží dostat se fyzicky na půdu firmy, místo páčidla používá sociotechnik svou schopnost manipulace a přesvědčuje osobu na druhé straně dveří, aby mu otevřela.
****

Vyhraná sázka

Během mých prvních kontaktů s počítačem na gymnáziu jsme se museli připojovat přes modem na jeden z hlavních minipočítačů DEC PDP 11 v Los Angeles, který sloužil všem školám ve městě. Operační systém tohoto počítače se jmenoval RSTS/E a byl to první systém, ve kterém jsem se naučil pracovat.

Tehdy, v roce 1981, sponzoroval DEC každý rok konferenci pro uživatele svých produktů. Přečetl jsem si, že tentokrát se má konference konat v Los Angeles. Populární magazín pro uživatele tohoto systému zveřejnil oznámení o novém zabezpečovacím produktu *LOCK-11*. Byl inzerovaný pomocí nápadité reklamní kampaně, která byla založena na slovech: „Je půl čtvrté ráno. Johny na po tři sta třicáté šesté uhodl tvé přístupové číslo do sítě 555-0336. On je uvnitř a ty jsi venku. Právě si prohlíží tvé soubory. Objednej si *LOCK-11*." Produkt, jak sugerovala kampaň, měl chránit před hackery. Na konferenci se měla konat jeho prezentace.

Moc jsem to chtěl vidět. Můj tehdejší kamarád, Vinny, se kterým jsme si po několik let hráli na hackery a který se později rozhodl donášet na mě federálním úřadům, se mnou tento zájem sdílel a přesvědčoval mně, abych s ním šel na konferenci.

Hotovost na stole

Když jsme dorazili na místo, šířily se v davu účastníků novinky o *LOCK-11*. Prý tvůrci vsadili peníze na to, že se nikomu nepodaří nabourat se do systému zabezpečeného novým produktem. Takové výzvě jsem nedodal odolat.

Vydali jsme se přímo ke stánku LOCK-11 a narazili jsme tam na tři programátory, kteří byli autory toho vynálezu; poznal jsem je a oni mě také - ačkoli jsem byl ještě teenager, už jsem měl pověst phreakera a hackera díky obsáhlému článku v LA Times, který psal o mém prvním setkání se státní mocí. Článek popisoval, jak se mi podařilo přemluvit cizího hlídače, aby mne uprostřed noci vpustil do budovy Pacific Telephone. Odešel jsem odtamtud s dokumentací počítačových programů přímo před nosem hlídače. (Zdá se, že Timesy z toho chtěly udělat senzaci a proto se rozhodly uvést moje jméno; protože jsem byl ještě mladistvý, článek porušoval zvyk — pokud ne přímo zákon — který zakazoval zveřejňovat jména nezletilých osob, obviněných ze spáchání přestupku.)

Když jsme tam tedy spolu s Vinniem přišli, zájem byl oboustranný. Z jejich strany proto, že ve mně poznali hackera, o kterém četli, a byli překvapeni mým příchodem. Náš zájem pak směřoval ke třem stodolarovým bankovkám, zastrčených za visačkou každého z nich. Odměna osobě, která překoná jejich systém, činila 300 dolarů — pro dva teenagery to byla slušná částka. Nemohli jsme se dočkat, až dostaneme šanci.

LOCK-11 fungoval na principu dvou úrovní zabezpečení. Uživatel musel jako obvykle znát správné uživatelské jméno a heslo, a kromě toho musely být obě tyto věci zadané z autorizovaného terminálu Tato metoda se označuje jako *terminálová identifikace (terminal-based security)*. Hackerovi, který by chtěl prolomit toto zabezpečení, nestačí jenom login a heslo, musí je navíc napsat ze správného terminálu. Tato metoda byla obecně uznávaná a tvůrci *LOCK-11* byli přesvědčeni, že si tak počítač udrží hackery od těla. Rozhodli jsme se dát jim lekci a při té příležitosti si vydělat tři sta dolarů.

Žargon
****

Terminálová identifikace — zabezpečení založené částečně na identifikaci počítačového terminálu, ze kterého vychází pokus o připojení, tato

metoda byla oblíbená u počítačů IBM typu *mainframe* (velké sálové počítače).
****

Člověk, kterého jsem znal a který byl považován za guru ve věcech týkajících se systému RSTS/E, nás přemlouval, abychom to zkusili. Před lety byl jedním z těch, kteří mne přesvědčili, abych se naboural do vnitřního vývojářského systému DEC. Jeho společníci mne později udali. Dnes byl uznávaným programátorem. Ukázalo se, že se pokoušel zabezpečení překonat, ale nepodařilo se mu to. To jen utvrdilo tvůrce v přesvědčení, že je jejich produkt opravdu bezpečný.

Pravidla hry byla jednoduchá: když se ti podaří dostat se dovnitř, peníze jsou tvoje. Dobrý reklamní tah — ale jen do chvíle, kdy někdo tvůrce pokoří a získá odměnu. Byli si tak jistí a drzí, že vytiskli několik uživatelských jmen a hesel a pověsili je u vchodu do stánku. Nebyla to obyčejná uživatelská konta, ale privilegovaná — s vysokými přístupovými právy v systému.

Nebylo to až tak odvážné, jak to možná zní.

Věděl jsem, že každý terminál je zapojen do portu samotného počítače. V konferenčním sále bylo rozestavěno pět terminálů pro hosty, kteří se mohli logovat pouze jako neprivilegovaní uživatelé — znamenalo to, že bylo možné přihlásit se pouze na konta, která nemají práva jako správci systému. Zdálo se, že existují pouze dvě cesty: bud nějak obejít zabezpečovací software — před tím právě chránil *LOCK-11* — nebo obejít celý systém tak, jak by to nikdy jeho tvůrce nenapadlo.

Výzva

Vyšli jsme s Vincem ze stánku poradit se. Napadl nás jistý plán. Procházeli jsme nenápadně kolem a pozorovali jsme z dálky stánek. V době oběda, kdy dav trochu zřídl, využili tři programátoři sníženého ruchu a šli si něco sníst a ve stánku nechali ženu, která mohla být manželkou nebo přítelkyní jednoho z nich. Vrátili jsme se a zabavili ji dotazy na to i ono („Jak dlouho už tu pracujete?", „Co ještě prodáváte?" a podobně). Mezitím se Vince vzdálil z jejího zorného pole a zabral se do práce pomocí dovednosti, kterou jsme si oba osvojili. Kromě fascinace počítači a nabourávání se do nich nebo kromě mého zájmu o kouzelnictví jsme se totiž oba zajímali také o způsoby otevírání zámků. Jako kluk jsem sháněl v knihkupectví na San Fernando Valley knížky o otevírání zámků, uvolňování rukou z pout, vytváření falešných totožností a podobných věcech, o které se zajímají všechny děti.

Vinny se v tomto umění cvičil jako já a brzy jsme dokázali otevřít každý z obvyklých a v obchodech dostupných zámků. Kdysi jsem míval taková období, že jsem měl chuť si zašpásovat a vyhlédl jsem si někoho, kdo zamykal dveře na dva zámky a pak jsem zámky otevřel a vzájemně je zaměnil. Majitele to přivádělo k zoufalství, když se je pokoušel otevřít. Pokračoval jsem v odvádění pozornosti mladé ženy ve výstavní hale, zatímco Vinny v podřepu za stánkem, aby si ho nikdo nevšiml, se zabýval zámkem skříňky, ve které byl minipočítač PDP-11 zároveň s koncovkami kabelů. Označování skříňky jako „zamknuté" by bylo příliš nadnesené. Byla vybavena takovým zámkem, jako mívá domácí nábytek, který může neobyčejně snadno otevřít i takový nešikovný amatér, jakými jsme byli my.

Vinniem u trvalo otevření zámku asi minutu. Uvnitř našel přesně to, co očekával: řadu portů určených k připojování uživatelských terminálů a jeden port pro takzvanou konzoli. Konzole je speciální terminál, který slouží operátorovi nebo administrátorovi systému k řízení všech počítačů. Vinny na něj připojil jeden z terminálů ve výstavní hale.

V tom okamžiku se tento terminál stal konzoli. Usedl jsem k němu, přihlásil jsem se pomocí jednoho z hesel, programátory tak opovážlivě zpřístupněných. Program *LOCK-11* poznal, že se loguji z autorizovaného

terminálu a dovolil mi jít dál – dostal jsem se do systému a měl jsem práva správce. Poopravil jsem operační systém tak, aby se z každého terminálu v hale bylo možné dostat se do systému jako privilegovaný uživatel. Když jsem do systému nainstaloval svoji tajnou opravu, šel Vinny přepojit kabel na původní místo. A nakonec ještě dokázal zamknout skříňku.

Vypsal jsem si adresáře, abych se podíval, jaké soubory se na počítači nacházejí. Když jsem hledal program *LOCK-11* a s ním související soubory, narazil jsem na něco šokujícího. Adresář, který na tom počítači rozhodně neměl co dělat. Programátoři si byli natolik jistí tím, že se jejich program nedá prorazit, že se dokonce ani neobtěžovali odstranit zdrojový kód nového produktu. Přesedl jsem si k sousednímu terminálu, ke kterému byla připojena tiskárna a začal jsem tisknout části zdrojového kódu na nekonečný, zeleně proužkovaný papír (takzvaný traktor), který se v tiskárnách tehdy používal.

Sotva Vinny zamkl skříňku a připojil se ke mně, trojice programátorů se vrátila z oběda. Viděli, že sedím u jednoho z terminálů a ťukám do klávesnice, zatímco tiskárna pravidelně tiskla.

„Copak děláš, Kevine?" zeptal se jeden z nich.

„Ale nic, jenom si tisknu váš zdroják," odpověděl jsem.

Pochopitelně to pokládali za vtip. Potom se podívali na tiskárnu a uviděli svůj žárlivě střežený zdrojový kód *LOCK-11*.

Nevěřili, že sa mi podařilo přilogovat se jako privilegovaný uživatel.

„Zmáčkni *control-t,*" řekl jeden z nich.

Zmáčkl jsem. Zobrazená informace potvrdila to, co jsem udělal. Chytil se za hlavu a Vinny řekl pouze:

„Tři sta dolarů, prosím."

Zaplatili. Po zbytek dne jsme se s Vinniem procházeli po výstavní ploše se stodolarovými bankovkami zastrčenými za naše visačky. Každý, kdo je viděl, věděl, odkud pocházejí.

Samozřejmě jsme neprorazili jejich program a kdyby si víc rozmysleli pravidla soutěže, použili lepší zámek ve skříňce nebo si lépe hlídali své zařízení, nezažili by největší ponížení konference - ponížení od dvojice teenagerů.

Později jsem zahlédl, jak programátoři zastavili u banky: ty stodolarové bankovky byly asi jediné peníze, které si na konferenci vzali.

Poznámka Mitnicka

****

Tady je další příklad inteligentních lidí, kteří podceňují své protivníky. Odvážili bychom se vsadit 300 dolarů na to, že náš bezpečnostní systém je neprorazitelný? Občas je způsob obejití systému úplně jiný, než jsme očekávali.

****

Slovník jako zbraň

Když někdo získá naše heslo, je schopný se dostat do našeho systému. Ve většině případů si toho ani nevšimneme.

Mladý hacker, kterému budu říkat Ivan Peters, si dal za cíl získat zdrojový kód nové hry. Bez potíží se dostal do firemní sítě WAN, protože jeho hackerský kolega se už dříve dokázal nabourat na jeden i jejich webových serverů. Po odhalení jisté slabiny v softwaru div že nespadl ze židle. Ukázalo se, že systém používal tzv. *dual homing,* což znamená, že měl odtud přístup i do vnitřní sítě.

Avšak po připojení stál Ivan před podobným problémem, před jakým stojí turista v Louvre, který chce najít portrét Mony Lisy. Bez průvodce by tam mohl motat celé týdny. Byla to globální korporace se stovkami kanceláří a tisíci serverů, která ve své síti nezveřejňovala indexy vývojářských systémů nebo jiné průvodcovské služby po svých datech.

Místo toho, aby k nalezení serveru, na který se potřeboval dostat, použil technologické metody, využil metodu sociotechnickou. Uskutečnil několik telefonátů na základě postupů v této knize už popsaných. Nejprve zatelefonoval na technickou pomoc oddělení informatiky, před-tavil se jako zaměstnanec firmy a řekl, že by rád probral jistý problém spojený s rozhraním produktu, na kterém pracovala jeho skupina. Požádal o telefonní číslo na šéfa projektů ve skupině programátorů, kteří se zabývali hrami.

Potom zavolal na toto číslo a předstíral, že je pracovníkem oddělení Informatiky.

„Ještě dnes večer," řekl, „budeme měnit router a chceme se ujistit, že lidé z vaší skupiny neztratí spojení se serverem. Který server používáte?"

Síť byla neustále vylepšována a sdělení jména serveru nemůže ničemu vadit, že? Vždyť je přece chráněn heslem a samotná znalost jména nikomu nic nepřinese. A tak šéf projektů uvedl jméno serveru. Ani se nepokusil o zpětné zavolání a ověření této historky nebo alespoň o zapsání jména a telefonního čísla volajícího. Prostě sdělil jména serverů: ATM5 a ATM6.

Hledání hesla

Nyní se Ivan vrátil k technologickým metodám, aby získal autentikační informace. Ve většině případů je prvním krokem identifikace účtu se snadným heslem, které dovolí získat v systému první opěrný bod.

Pokud se útočník pokouší za pomoci hackerských nástrojů vzdáleně identifikovat hesla, vyžaduje to být po dlouhé hodiny připojen k firemní síti. Objevuje se tu nebezpečí: čím déle bude připojen k síti, tím větší je riziko jeho odhalení a dopadení.

Nejprve použil Ivan enumeraci, která umožňuje odhalit podrobnost o systému. Jako obvykle je možné vhodné nástroje nalézt na Internetu, (*http://mtslenth.0catch.com* — znak před „catch" je „nula"). Ivan našel na webu několik volně dostupných hackerckých nástrojů, které mu dovolili proces zautomatizovat a vyhnout se tak ruční práci, která by prodlužovala čas operace a tím by zvětšovala i riziko dopadení. Věděl, že firma většinou používá servery na platformě Windows a stáhl si program NTBEnum — enumerační nástroj NetBIOS (basic input/output system). Zadal IP adresu serveru ATM5 a spustil program. Nástroj dokázal identifikovat několik existujících kont na serveru.

> *Žargon*
> **********
> **Enumerace** — proces odhalující služby dostupné na daném serveru, jeho operační systém a názvy uživatelských kont, které mají přístup do systému.
> **********

Po identifikaci existujících kont stejný program umožnil spuštěni slovníkového útoku. Slovníkový útok je dobře známý lidem zabývajícím se bezpečností počítačových systémů a samozřejmě i hackerům. Ostatní lidi fakt, že je něco takového vůbec možné, šokuje. Tento útok má za cíl zjištění hesel uživatelů pomocí obecně užívaných slov.

Všichni jsme v některých věcech líní, ale nikdy mne nepřestane udivovat, že při výběru hesla má lidská kreativita a představivost prázdniny. Většina z nás chce mít heslo, které nás ochrání, ale zároveň je lehké si ho pamatovat. Obvykle to znamená použití nějakého nám blízkého slova. Mohou to být například naše iniciály, druhé jméno, přezdívka, jméno manžela, název oblíbené písničky, filmu či značky piva. Dále pak jméno ulice či města, kde bydlíme, značka auta, kterým jezdíme, oblíbené prázdninové místo nebo jméno potoku, kde nejlépe berou pstruzi. Vidíme to pravidlo? Většinou jsou to jména

nebo výrazy, které lze najít ve slovníku. Slovníkový útok zkouší postupně výrazy ze slovníku jako heslo jednoho či více uživatelů.

Ivan provedl slovníkový útok ve třech fázích. V první fázi seznam 800 nejčastěji používaných hesel. Seznam obsahuje taková jako *secret, work* nebo *password* (tedy *tajné, práce, heslo*). Kromě toho program tvořil permutace těchto výrazů s doplněnými číslicemi nebo s číslem aktuálního měsíce. Program zkoušel každé heslo na všeď nalezených účtech v systému. Bez výsledku.

Ve druhé fázi si otevřel stránku vyhledávače Google a zadal vyraz „*wordlists dictionaries*" a našel tisíce stran obsahující seznamy slov a anglické i jiné slovníky. Stáhl si celý elektronický anglický slovník. Doplnil ho o několik seznamů výrazů, které našel vyhledávač. Ivan si vybral adresu *www.outpost9.com/files/Wordlists.html* .

Z této stránky se mu podařilo stáhnout (úplně zadarmo) sadů souborů obsahující příjmení, neobvyklá jména, jména a výrazy spojené s politikou, jména herců a slova a jména pocházející z Bible.

Jiná stránka se seznamy výrazů je dostupná na univerzitě v Oxfordu na adrese *ftp://ftp.ox.ac.uk/pub/wordlists* .

Na jiných adresách můžeme najít seznamy se jmény postav z animovaných filmů, citáty ze Shakespeara, z Odyssey, z Tolkiena i Hvězdných válek a také slova spojená s vědou, náboženstvím atd. (Jedna internetová firma prodává seznam obsahující 4,4 milionu slov a jmen za pouhých 20 dolarů.) Atakující program může být zkonfigurován i tak, aby tvořil na základě výrazů ze slovníku anagramy — to je další oblíbená metoda uživatelů, která má zvětšit jejich bezpečnost.

Rychleji než si myslíš

Když si Ivan vybral seznam, který použije a spustil program, přepnul ho do automatického režimu a mohl se tak věnovat něčemu jinému. Člověk by si myslel, že takový útok dá útočníkovi čas na delší šlofíček a dokonce, že až se vzbudí, bude pokrok nevelký. Ve skutečnosti může byt — v závislosti na druhu napadeného systému, konfiguraci bezpečnostních systémů a rychlosti připojení — plná slovní zásoba z anglického slovníku otestována za 30 minut!

Během útoku zapnul Ivan druhý počítač a rozběhl podobný útok na druhý server, který používala skupina programátorů, ATM6. O dvacet minut později se podařilo něco, co se většině lidí zdá nemožné: prolomit heslo a odhalit, že jeden z uživatelů si zvolil heslo „Frodo", jméno jednoho z hobitů, hrdiny Pána prstenů.

S heslem v ruce se Ivan mohl připojit k serveru ATM6.

Čekala tam na něho dobrá a špatná zpráva. Dobrá, že konto, na které se naboural, mělo administrátorská práva. A špatná, že tam nikde nemohl najít zdrojový kód hry. Zřejmě byl na druhém serveru, ATM5, který se slovníkovému útoku ubránil. Ivan však neházel flintu do žita - stále ještě měl v zásobě pár triků.

V některých operačních systémech Windows a UNIX jsou zašifrovaná hesla přístupná každému, kdo má přístup na počítač, kde jsou umístěná. Důvodem je fakt, že zakódovaná hesla nelze dekódovat zpět a tedy není důvod je chránit. Tato teorie je mylná. Pomocí dalšího nástroje dostupného na síti, *pwdump3*, si stáhl zakódovaná hesla ze serveru ATM6. Typický soubor se zakódovanými hesly vypadá takto:

Administrator: 500:95E4321A38AD8D6AB75E0C8D76954A50:
2E48927AQB04F3BFB341E266D6L
akasper:1110:5A8D7E9E3C3954F642C5C736306CBFEF:393CE7F90A8357F157873D72D
digger:1111:5D15COD58D0216C525AD3B83FA6627C7:17AD564144308B42B8403D01AE256
555
ellgan:1112:2017DA45D8O1383EFF17365FAF1FFE89:07AEC950C22CBB9C2C734EB89j1

tafeeck:1115:9F5890B3FECCAB7EAAD3B435B51404EE:1F0115A728447212FC05E1D20820335
vkantar;1116:81A6A5D035596E7DAAD3B435B51404EE:B933D36DD12258946FCC7BD153F1CD6
vwallwick:1119:25904EC665BA30F44494F42E1054F192:15B2B7953FB632907455D2706A432
mmcdonald: 1121:
A4AED098D29A3217AAD3B435B51404EE:40670F936B79C2ED522F5ECA939c
kworkman:1141:C5C598AF45768635AAD3B435B51404EE:DEC8E827A121273EF084CDBF5FD192

Když měl soubor u sebe na počítači, použil Ivan další nástroj, který prováděl tzv. *útok hrubou silou*. Ten zkouší všechny kombinace alfanumerických a většiny speciálních znaků.

Žargon
****
Útok hrubou silou — strategie odhalování hesel, která spočívá v testování všech možných kombinací alfanumerických i speciálních znaků.
****

Ivan použil nástroj *L0phtcrack3* (čti loft-crack; je dostupný na adrese *www.atstake.com*; jiný zdroj vynikajících nástrojů na hádání hesel je *www.elcomsoft.com*). Správci používají L0phtcrack3 na vyhledávání „slabých" hesel a hackeři na jejich proražení.

L0phtcrack3 umožňuje zkoušet hesla s kombinacemi písmen, číslic a většiny symbolů včetně !@#$%^&. Systematicky testuje všechny možné kombinace většiny znaků. (Pokud jsou však v hesle použity neviditelné znaky, L0phtcrack3 nebude schopný heslo odhalit.)

Tento program pracuje s neuvěřitelnou rychlostí, která může na počítači s frekvencí procesoru 1 GHz dosáhnout hodnoty 2,8 milionu pokusu za sekundu. Dokonce i při této rychlosti může, pokud správce dobře zkonfiguroval systém Windows (tj. vypnul používání hašování LANMAN), prolomení hesla zabrat hodně času.

Z tohoto důvodu si útočník často stahuje soubory s hesly na svůj počítač a spouští útok u sebe, aby neriskoval odhalení během dlouho udržovaného spojení.

Ivan nemusel čekat dlouho. O několik hodin později našel program hesla všech členů skupiny programátorů. Byla to však hesla uživatelů na ATM6, kde nebyl zdrojový kód.

Co teď? Stále nebyl schopen získat hesla umožňující přístup k serveru ATM5. Jako hacker si uvědomoval zlozvyky většiny uživateiů a dosel k závěru, že si někdo z členů týmu mohl vybrat stejné heslo na obou serverech.

A bylo to tak. Jeden z programátorů měl heslo *gamers* jak na ATM5, tak i na ATM6.

Před Ivanem se otevřely dveře k hledám zdrojového kódu. Když ho našel a stáhl si celý strom, učinil ještě jednu pro hackera typickou věc. Změnil heslo na spícím kontě s administrátorskýrni právy, čistě pro případ, že by se sem chtěl později vrátit a stáhnout si novou verzi programu.

Analýza podvodu

V tomto útoku, který využíval zároveň lidská i technologická slabá místa útoku, začal útočník telefonátem, aby zjistil umístění a jména vývojářských serverů, na kterých se nacházely chráněné informace.

Potom využil softwarového nástroje ke zjištění existujících jmen všech uživatelů na serveru. Nato provedl dva úspěšné útoky na heslo, z toho jeden byl útok hrubou silou, který hledá hesla na základě všech výrazů ze slovníku,

občas rozšířený o dodatečné seznamy slov obsahující jména, názvy míst a předmětů, které jsou objektem všeobecného zájmu.

Protože jsou komerční i volně dostupné hackerské nástroje přístupné každému nezávisle na účelu použití, je důležité zabezpečit firemní počítače i síťovou infrastrukturu.

Stupeň tohoto ohrožení je velký. Podle časopisu *Computer World* vedla analýza provedená Oppenheimerovou nadací z New Yorku k překvapivému odhalení. Jeden z viceprezidentů odpovědný za bezpečnost sítě provedl útok na hesla zaměstnanců firmy pomocí jednoho ze standardních softwarových balíčků. Časopis udává, že během tří minut dokázal prorazit hesla 800 zaměstnanců.

> *Poznámka Mitnicka*
> **********
> Řečeno terminologií vypůjčenou ze hry Monopoly, pokud použiješ jako heslo výraz ze slovníku, pak: „Jdeš přímo do vězení, neprocházíš přes start, nebereš 200 dolaru." Zaměstnance je třeba naučit, jak si volit hesla, která firemní data opravdu ochrání.
> **********

Prevence

Sociotechnické útoky mohou být ještě destruktivnější, pokud sociotechnik použije navíc technické prostředky. Prevence před útoky tohoto typu obvykle vyžaduje, aby byla přijata opatření týkající se lidí i technických prostředků zároveň.

Stačí říci ne

V prvním příběhu této kapitoly pracovnice kanceláře CANZ telekomunikační firmy neměla rušit blokování příchozích hovorů, aniž by měla servisní objednávku autorizující tuto změnu. Samotná znalost pokynů nestačí. Pracovníci musejí pochopit, jaký význam mají pro firmu pokvny v oblasti ochrany před ohrožením zvenku.

Bezpečnostní politika by měla odrazovat od neplnění těchto pokynů systémem odměn a trestů. Samozřejmě politika musí být realistická a nesmí vyžadovat od pracovníků uskutečňování mnoha pracovních kroků které by pak raději ignorovali. Program školení by měl přesvědčovat zaměstnance, že jakkoli je důležité dokončit práci v předpokládaném termínu, mohou některé zkratky spojené s opomenutím bezpečnostních postupů způsobit firmě nebo spolupracovníkům újmu.

Při sdělování informací cizím osobám po telefonu je vždy nutné uplatňovat stejný stupeň obezřetnosti. Bez ohledu na nátlak, služební věk nebo postavení dané osoby ve firmě, by neměly být sdělovány žádné informace, které nejsou označené jako obecně dostupné, dokud nedojde k pozitivnímu ověření totožnosti volajícího. Pokud by bylo toto pravidlo striktně uplatňováno, sociotechnické taktiky použité v tomto příběhu by nebyly účinné a vězeň Gondorff by nikdy nebyl schopen spolu s Johnym naplánovat nový podvod.

Nejdůležitější bod, ke kterému se celou dobu na stránkách této knihy vracím, je verifikace, verifikace a ještě jednou verifikace. Bez ověření totožnosti tazatele by neměla být žádná žádost vyřízena.

Úklid

Každá společnost, která nemá čtyřiadvacetihodinovou ostrahu, se vystavuje nebezpečí, že se útočník dostane do kanceláří po pracovní době. Uklízeči budou obvykle mít respekt ke každému, kdo se objeví u dveří firmy a bude vypadat jako její zaměstnanec. Koneckonců taková osoba jim může způsobit potíže nebo je dokonce přivést ke ztrátě zaměstnání. Z tohoto důvodu musejí být uklízeči, ať už naši nebo z externí firmy, proškoleni v bezpečnostních otázkách.

Uklízení nevyžaduje vysokoškolské vzdělání, dokonce ani schopnost hovořit místním jazykem. V podstatě ani gramotnost. A pokud vůbec existuje nějaké školení, tak se týká spíše výběru správného čistícího prostředku než záležitostí spojených s bezpečností.

Organizace musí situaci, která je popsána v této kapitole, předvídat a příslušným způsobem vyškolit lidi. Z mých zkušeností vyplývá, že většina, ne-li všechny organizace soukromého sektoru, postupují v otázkách spojených s fyzickým zabezpečením prostor poměrně nenuceně. Lze na to jít také jinak a přehodit břemeno na zaměstnance. Ve firmě, která není pod ostrahou 24 hodin denně, by se měla zavést zásada, že pokud se chtějí lidé dostat do prostor podniku po pracovní době, musejí mít vlastní klíče nebo elektronické karty a v žádném případě nemohou žádat uklízeče o vpuštění dovnitř. Pak stačí instruovat uklízecí firmu, že její pracovníci nemohou sami pod žádnou záminkou vpouštět nikoho na půdu firmy. Pokud taková možnost existuje, lze toto pravidlo dát jako jednu podmínku do smlouvy uzavírané s uklízeči firmou.

Uklízeči musejí být také vycvičení na situace, kdy se neoprávněná osoba snaží projít vchodem těsně za oprávněnou osobou. Je třeba je vyškolit, aby nevpouštěli nikoho, kdo se pokouší vejít do budovy jen proto, že vypadá jako zaměstnanec firmy.

Připomínejme věci probrané na školení řekněme třikrát, čtyřikrát za rok zorganizováním pokusu nebo ohodnocením bezpečnostního stavu firmy. Pošleme někoho, aby se objevil u dveří během úklidu a pokusil se je přesvědčit, aby ho pustili do budovy. Je lepší si najmout firmu, která se na testy tohoto druhu specializuje, než k tomu využívat vlastní pracovníky.

Důležitá zpráva: chraňte svá hesla

Čím dál větší váhu přikládají organizace upevňování bezpečnosti pomocí technologických prostředků. Například konfigurují operační systémy, aby od uživatele vyžadovaly dodržování zásad týkajících se hesel a omezily počet neúspěšných pokusů o přihlášení, po kterém je konto zablokováno. Ve skutečnosti systémy Microsoft Windows mají tyto funkce zabudovány, ale protože mohou uživatele rozčilovat, jsou funkce spojené s bezpečností implicitně vypnuty. Je nejvyšší čas, aby výrobci softwaru s těmito praktikami přestali a začali tyto volby standardně zapínat (mám podezření, že na to sami brzy přijdou).

Bezpečnostní politika firmy by měla podporovat veškerou činnost správců sítě, která má pomocí technických prostředků zlepšit bezpečnost, všude tam, kde je to jen trochu možné. Účelem těchto akcí má být omezení nespolehlivého lidského faktoru na nejmenší možnou míru. To není nic těžkého. Je známo, že pokud například omezíme počet možných neúspěšných pokusů o přihlášení, značně ztížíme život potenciálním útočníkům.

Každá organizace se potýká s problémem rovnováhy mezi zachováním odpovídajícího stupně bezpečnosti a produktivitou. Někteří pracovníci mají kvůli tomu sklon část pokynů ignorovat a nepřiznávat jim význam, jaký pro ochranu důvěrných dat firmy mají.

Pokud tyto pokyny některá témata neobsahují, mohou mít zaměstnanci tendenci jít cestou nejmenšího odporu a pracovat pohodlným způsobem. Někteří se mohou bránit změnám návyku a zásady bezpečnosti otevřeně zlehčovat. Určitě jsme někdy potkali člověka, který postupuje podle směrnic, týkajících se

délky a komplikovanosti hesla ale vymyšlené heslo si zapisuje na papírek, který si přilepí na monitor.

Důležitým prvkem ochrany firmy je používání těžko odhadnutelných hesel spolu s takovou konfigurací zařízení, která posiluje bezpečnost systému.

Podrobnosti tykající se hesel si probereme v 16. kapitole.

12

První na ráně

Hodně zde uvedených příběhů ukazuje, že dobrý sociotechnik si často vybírá za oběť osobu s nízkým postavením ve firmě. Těmito lidmi je snadné manipulovat a vytahovat z nich zdánlivě nedůležité údaje, které krok za krokem přibližují útočníka k důvěrným informacím.

Útočník se zaměřuje na osoby na nízkých pozicích, protože ty si plně neuvědomují význam některých informací a důsledky některých činností. Kromě toho jsou proti sociotechnickým metodám méně odolné – volající má autoritu, zdá se milý a přátelský, dělá dojem, že zná různé lidi ve firmě, věc, o kterou žádá, velmi spěchá a oběť předpokládá, že si získá něčí uznání či vděčnost.

Zde je několik příkladů útoků na osoby s nízkým postavením ve firmě.

Ochranka pomůže

Když sociotechnici atakují takové osoby jako uklízečky nebo strážné, doufají, že narazí na někoho, kdo je přátelsky naladěn a důvěřuje lidem. Takoví lidé jsou nejochotnější pomoci. A o to právě šlo útočníkovi z následujícího příběhu.

Očima Elliota

Čas: úterý 3.26 ráno, únor 1998
Místo: výrobní závod Marchand Microsystems, Nashua, New Hampshire

Elliot věděl, že s výjimkou pochůzek nesmí opustit vrátnici. Bylo to však uprostřed noci a od začátku směny neviděl ani jednu podezřelou osobu. A kromě toho se stejně blížil čas obchůzky. Tón toho nešťastného chlápka, který telefonoval, ukazoval, že skutečně potřebuje pomoc. Občas je dobré udělat nějaký dobrý skutek.

Billův příběh

Bili Goodrock měl jasně vytčený životní cíl. Nezměnil ho od svých dvanácti let: jít do důchodu ve věku 24 let, aniž by se dotkl jediného penny z fondu, který byl pro něj určen. Chtěl ukázat svému otci, všemocnému a přísnému bankéři, že získá úspěch i bez jeho pomoci.

Zbývaly mu už jen dva roky a bylo jasné, že během následujících 24 měsíců nedosáhne úspěchu jako dokonalý obchodník nebo obratný investor. Jednou dokonce pomyslel na vyloupení banky, ale to byly jedině fantazie – bilance zisků a ztrát tu nevypadala příliš růžově. Místo toho se rozhodl udělat to, co se kdysi povedlo Rifkinovi – vyloupit banku elektronicky.

Když byl posledně Bili s rodinou v Evropě, otevřel si v Monaku bankovní účet a uložil tam 100 franků. Měl plán, díky kterému se tato částka mohla rychle zvětšit na sedmimístnou. A při troše štěstí dokonce osmimístnou.

Billovo děvče, Anně Marie, pracovala v M&A, velké bostonské bance. Jednoho dne, když čekal, až se Anně Marie vrátí z jednání, které se protáhlo, podlehl zvědavosti a napojil svůj notebook k ethernetovému portu v konferenční

místnosti, kam ho zatím posadili. Tak! Byl v jejich vnitřní síti, připojený k systému... za firemním firewallem. Něco ho napadlo.

O svůj objev se poděl se spolužákem, který se znal s jistou holkou, Julií – výbornou informatičkou, doktorandkou, která byla na stáži ve firmě Marchand Microsystems. Julia se zdála být vynikajícím zdrojem důležitých informací, které by jim dovolily změnit totožnost. Řekli jí, že píší scénář k filmu. Uvěřila.

Byla to pro ni dobrá zábava – pomáhat s vytvářením zápletky a radit se všemi detaily, jak provést intriku, kterou si vymysleli. Samotný námět se jí velmi zalíbil. Prosila, aby ji uvedli v poděkování v závěrečných titulkách.

Upozornili ji, že scénáristické nápady se velmi často kradou a nechali si slíbit, že o tom nikomu nic neřekne.

Bill vyškolený Julií se mohl sám věnovat riskantní části úkolu a nepochyboval, že se mu bude dařit.

* * *

Zatelefonoval jsem tam odpoledne a podařilo se mi zjistit, že vedoucí ochranky na noční směně se jmenuje Isaiah Adams. V půl desáté téhož večera jsem tam opět zavolal a mluvil se strážným, která hlídal vstupní halu. Měl jsem naléhavou záležitost a byl jsem trochu zmatený.

„Mám nějaké potíže s autem a nemůžu se dostat do firmy," řekl jsem. „Pokazil se mi počítač a opravdu potřebuji vaši pomoc. Zkoušel jsem se dovolat šéfovi ochranky, Isaiahovi, ale není doma. Mohl byste pro mne něco udělat? Byl bych vám opravdu zavázán."

Místnosti v budově byly označené kódy. Řekl jsem mu kód počítačové laboratoře a zeptal jsem se, jestli ví, kde to je. Řekl, že ví, a souhlasil, že tam půjde. Dodal, že mu ale potrvá několik minut, než tam dorazí. Řekl jsem, že mu tedy zavolám, až tam bude, že mám k dispozici pouze jednu telefonní linku a ještě se pokusím přes ni připojit k síti a vyřešit ten problém.

Když jsem vytočil číslo, už tam čekal. Řek jsem mu, jak má vyhledat konzolu, o kterou mi šlo. Byla na ní samolepka s nápisem „elmer". Na tomto počítači – alespoň podle toho, co říkala Julia – byly vytvářeny komerční verze operačního systému, který firma nabízela. Když se strážnému podařilo ho najít, byl jsem si už jistý, že si Julia nevymýšlela, a trochu se mi ulevilo. Řekl jsem mu, aby několikrát zmáčkl klávesu Enter. Odpověděl, že to zobrazilo několik symbolů libry. To znamenalo, že počítač je přilogovaný k síti s plnými právy. Psaní na klávesnici mu šlo ztěžka a pořádně se zapotil, když jsem se mu pokoušel nadiktovat příkaz, který vypadal víceméně takto:

```
echo 'fix:x:0:0::/:/bin/sh' >> /etc/passwd
```

Na konec se mu to podařilo. Tímto způsobem jsme založili nové konto s uživatelským jménem fix. Následně jsem ho nechal napsat:

```
echo "fix::10300:0:0" >> /etc/shadow
```

Tím se nastavuje šifrované heslo, které se nachází mezi dvěma dvojtečkami. Pokud tam není nic, znamená to, že konto není chráněné heslem. Jak vidno, pomocí dvou příkazů lze v systému založit konto *fix* s prázdným heslem. Nejlepší na tom ale je, že to konto bude mít stejná práva jako konto administrátora.

Další věc, o kterou jsem poprosil strážného, bylo zadání příkazu který vytiskl dlouhý seznam souboru. Řekl jsem mu, aby ten vytištěný kus odtrhl a vzal sebou do služebny, protože budu možná ještě něco z toho papíru později potřebovat.

Vtip této operace byl v tom, že strážný neměl ponětí, že vytvořil nové konto. Seznam souborů jsem ho nechal vytisknout proto, že jsem se musel pojistit, aby příkazy, které zadal, opustily místnost zároveň s ním. Díky tomu si správce nebo operátor ničeho nevšimnou a nevyvolají poplach.

Teď jsem měl konto, heslo a plná práva. Těsně před půlnocí jsem se dovolal do systému a postupoval podle instrukcí, které nám Julia dala „pro potřeby filmu". Po chvíli jsem měl přístup k jednomu ze serverů, který obsahoval hlavní kopii zdrojového kódu nové verze operačního systému firmy.

Nahrál jsem tam „opravu", kterou napsala Julia. Podle toho, co nám řekla, modifikovala proceduru v jedné z knihoven operačního systému. Díky tomu tam byla vytvořená tajná „zadní vrátka" umožňující přístup k systému pomocí tajného hesla.

Poznámka Mitnicka
****
Tento typ „zadních vrátek" nemodifikuje přihlašovací program. Skrytý vchod je vytvořený změnou funkce obsažené v dynamických knihovnách, které přihlašovací program používá. Vetřelec v typickém útoku mění samotný přihlašovací program, ale pozorný administrátor muže změnu odhalit, když si porovná program s originálem, který má například na instalačním CD.
****

Pečlivě jsem postupoval podle Juliina návodu. Nejprve jsem nainstaloval *patch*[21], následně jsem odstranil existující konto *fix* a vymazal jsem informace ze všech logů[22], abych zahladil stopy po své činnosti.

Firma bude brzy distribuovat novou aktualizaci systému svým klientům: finančním institucím rozesetým po celém světě. Každá kopie bude vybavena „zadními vrátky", které jsem před rozesláním umístil v hlavní distribuční kopii. Umožní mi to přístup do počítačového systému každé banky nebo makléřské agentury, která si aktualizaci nainstaluje.

Žargon
****
Aktualizace (ang. patch) — tradičně je to kus kódu, který po umístění ve spustitelném (binárním) souboru programu řeší nějaký problém.
****

To samozřejmě zatím nebyl konec — zůstalo mi na práci ještě pár věcí. Musel jsem získat přístup do vnitřní sítě každé instituce, kterou jsem hodlal „navštívit". Pak jsem se musel dozvědět, který z počítačů je používaný při peněžních převodech, a nainstalovat sledovací programy, abych se dozvěděl, jak se tyto operace uskutečňují.

To všechno jsem mohl dělat vzdáleně z počítače, který by se nalézal na libovolném místě, třeba někde s výhledem na písčitou pláž. Tahiti, přicházím!

Zavolal jsem znovu strážnému, poděkoval jsem mu za pomoc a řekl jsem, že ten výtisk už může vyhodit.

Analýza podvodu

Příslušník ochranky měl instrukce týkající se služby, ale ani ty nejlépe propracované pokyny nejsou schopny předvídat všechny situace. Nikdo mu neřekl, jaké škody může způsobit, když napíše na počítači několik znaků, které mu nadiktovala osoba vydávající se za firemního zaměstnance.

Ve spolupráci se strážnými bylo získání přístupu k serveru a k hlavní kopii systému poměrně jednoduché, bez ohledu na skutečnost, že se počítač

[21] Pozn. překl.: Anglické slovo patch znamená česky záplata. V podstatě to věrně odráží skutečnost, že programy jsou často děravé.

[22] Pozn. překl.: Slovo log se používá pro soubor obsahující záznamy o prováděné činnosti, protokol, žurnál.

nacházel za zamčenými dveřmi laboratoře — strážný měl pochopitelně klíče od všech dveří.

Dokonce i nejpoctivějšího zaměstnance (v našem případě doktorandku a stážistku Julii) lze občas podplatit nebo obelstít, aby nám prozradil informace pro sociotechnika klíčového významu, například kde se nachází zajímavý počítačový systém nebo — klíč k celému útoku — kdy bude dokončená nová verze aktualizace. Bylo to velmi důležité proto, že příliš brzy uskutečněná změna tohoto druhu je zatížena velkým rizikem odhalení nebo odstranění v důsledku obnovy systému z jiné kopie.

Možná jsme si všimli jednoho detailu: strážný s sebou odnesl výtisk a později ho vyhodil. Byl to podstatný prvek. Útočník by jistě nechtěl, aby operátoři, až přijdou ráno do práce, našli důkaz o jeho činu (na tiskárně se tisknou všechny zadané příkazy) nebo si ho všimli v odpadkovém koši. Když strážnému uvedl věrohodné vysvětlení, aby vzal výtisk s sebou, mohl se tomuto riziku vyhnout.

Poznámka Mitnicka
****
Pokud vetřelec nemá možnost získat fyzicky přístup k počítačovému systému nebo síti, pokusí se zmanipulovat jiné lidi, aby něco udělali místo něj. V případech, kdy je bezprostřední přístup k počítači nutný, je využití oběti jako prostředníka dokonce lepší, protože se útočník nevystavuje nebezpečí dopadení.
****

Havarijní záplata

Člověk by si myslel, že počítačový technik by si měl uvědomovat rizika, která s sebou přináší poskytnutí přístupu k počítači osobě zvenku. Jestliže je však touto osobou mazaný sociotechnik prohlašující se za představitele softwarového producenta ochotného pomoci, výsledky mohou být nečekané.

Záchranný telefon

Volající člověk chtěl vědět, kdo má na starosti počítače. Telefonistka ho přepojila na technickou podporu, Paula Ahearna.

Hlas ve sluchátku se představil:

„Tady je Edward ze SeerWare, dodavatel vaší databáze. Část našich klientů zjevně nedostala e-mail o havarijní aktualizaci, proto v rámci kontroly kvality obvoláváme vybrané firmy a chtěli bychom vědět, jestli nebyly s instalací patche nějaké potíže. Už jste ho instalovali?"

Paul odpověděl, že o žádné aktualizaci neslyšel.

„Hrozí nebezpečí nevratné úplné ztráty dat, proto doporučujeme, abyste ji nainstalovali co možná nejdříve," řekl Edward.

Paul odvětil, že by to samozřejmě rád co nejdříve udělal.

„Dobrá," řekl volající. „Pošleme vám pásku nebo CD ROM s patchem. Chtěl jsem jen dodat, že věc je opravdu vážná — dvě firmy už přišly o data za několik dní práce. Proto byste to *opravdu* měl nainstalovat tak rychle, jak je to jen možné, než se vám něco takového stane taky."

„Bylo by možné si to stáhnout z vašeho webu?" zeptal se Paul.

„Brzy by to tam mělo být, ted se ale všichni naši lidé věnují nápravám škod. Jestli si přejete, naše zákaznické centrum vám to nainstaluje na dálku. Můžeme se připojit přes váš modem nebo se dostat do systému přes Telnet."

Telnet máme zakázaný, zejména z Internetu – je to nebezpečné," odpověděl Paul. „Pokud máte SSH, pak to bude v pořádku," dodal. SSH je jméno produktu umožňující bezpečný přenos souborů.

„Máme SSH. Jaká je vaše IP adresa?"

Paul uvedl adresu a když se Edward zeptal na login a heslo, dostal oboje.

Analýza podvodu

Telefonát mohl samozřejmě pocházet od dodavatele databáze. Pak by se ovšem tento příběh neocitl v této knize.

Sociotechnik zde ovlivnil oběť tím, že vzbudil strach před ztrátou kritických dat, načež nabídl okamžité řešení problému.

Když si sociotechnik volí za cíl osobu, která zná hodnotu informací, jeho argumentace musejí být silné a přesvědčivé, aby vzdálený přístup do systému získal. Občas je nutné dodat prvek neodkladnosti, aby se oběť nesoustředěná kvůli spěchu podřídila dřív, než vůbec bude mít příležitost si žádost promyslet.

Nová pracovnice

Jaké vnitřní informace firmy mohou být objektem zájmu útočníka? Občas to může být něco, o čem se zdá, že nemá vůbec smysl chránit.

Telefonát Sarah

„Personální oddělení, u telefonu Sarah."

„Ahoj Sarah, tady je George z parkoviště u budovy. Volám kvůli těm kartám, které používáme, aby se lidé mohli dostat na parkoviště a k výtahům. Máme tu jeden problém a musíme přeprogramovat karty všem lidem, kteří byli přijati za posledních patnáct dní."

„Takže potřebuješ jejich jména?"

„A telefony."

„Podívám se na seznam nově přijatých osob a zavolám ti zpátky. Jaké máš číslo?"

„73..., ale právě odcházím, mám přestávku. Mohl bych ti zavolat za půl hodiny, může být?"

„Aha, dobře."

Když znovu zavolal, řekla mu:

„Takže máme jen dva nové. Anna Myrtle z finančního, sekretářka. A ten novy náměstek, pan Underwood."

„A telefonní čísla?"

„Už to bude...na pana Undenvooda – 6973 a na Annu Myrtle - 2127."

„Moc jsi mi pomohla, díky."

Telefonát Anně

„Finance, u telefonu Anna."

„Jsem rád, že jsem tam tak pozdě ještě někoho zastihl. Tady je Ron Vittaro. Jsem z edičního. Asi jsme ještě neměli příležitost se poznat. Vítám novou kolegyni."

„Děkuji."

„Anno, volám z Los Angeles a mám tu velký problém. Potřeboval bych od tebe deset minut."

„Samozřejmě, o co jde?"

„Jdi nahoru do mé kanceláře. Víš, kde je má kancelář?"

„Ne."

„Je to místnost na rohu v 15. patře – číslo 1502. Zavolám ti tam za několik minut. Až tam budeš, musíš zmáčknout na mém telefonu tlačítko *forward*, aby se nespustil záznamník, když budu volat."

„Dobře, už jdu."

O deset minut později byla ve zmíněné kanceláři, vypnula záznamník a čekala na zazvonění telefonu. Ron po ní chtěl, aby si sedla k počítači a spustila Internet Explorer. Když to udělala, řekl jí, aby tam napsala adresu: *www.geocities.com/ron_insen/manuscript.doc.exe* .

Když se objevilo dialogové okno, požádal ji, aby klikla na *otevřít*. Počítač začal stahovat dokument, ale za chvíli obrazovka zčernala. Když mu to oznámila, odpověděl:

„Ale ne! Už zase! Už posledně jsem měl potíže se stahováním souborů z téhle stránky, ale myslel jsem, že to už opravili. No nic, co se dá dělat, nedělej si s tím starosti. Zkusím to později nějak jinak."

Potom ji požádal, aby restartovala počítač, aby se ujistil, že po tom, co se stalo, správně funguje. Provedl ji procedurou opětovného spuštění počítače.

Když se počítač znovu podařilo rozběhnout, srdečně jí poděkoval a zavěsil. Anna se vrátila k sobě a dokončila práci.

Příběh Kurta Dillona

Nakladatelství Millard-Fenton Publishing bylo nadšené novým autorem, se kterým mělo právě podepsat smlouvu. Jednalo se o penzionovaného ředitele jedné z největších amerických firem a strhující příběh, který předkládal. Někdo mu doporučil manažera, který mu v jednáních s nakladatelstvím pomůže. Manažer se nechtěl přiznat, že je v záležitostech nakladatelských kontraktu úplným zelenáčem, takže si najal starého známého, aby mu pomohl získat potřebné informace. Nebyl to však dobrý výběr. Uvedený známý, Kurt Dillon, používal při svých pátráních dost netypické metody, které nebyly vždy v souladu s etickými zásadami.

Kurt si založil bezplatnou stránku na Geocities na jméno Ron Vittaro a umístil tam monitorující program. Změnil název souboru na *manuscript.doc.exe*, aby simuloval wordovský dokument a nevzbuzoval podezření. Ve skutečnosti všechno proběhlo mnohem lépe, než Kurt očekával; opravdový Vittaro totiž nikdy nezměnil jednu z implicitních voleb systému Windows, která způsobuje ukrývání přípon známých typů souborů. Díky tomu se soubor zobrazil jako *manuscript.doc.*

Později jeho přítelkyně zatelefonovala Vittarově sekretářce a podle Dillonových pokynů řekla:

„Jsem asistentka Paula Spandeho, prezidenta Ultimate Bookstores z Toronta. Pan Vittaro se před nějakým časem setkal na knižním veletrhu s mým šéfem a požádal ho o telefon, aby probrali jistý projekt, který by spolu mohli uskutečnit. Pan Spadone je často na cestách, takže mne pověřil, abych zjistila, kdy bude možné pana Vittara zastihnout v kanceláři."

Než se jim podařilo společně dohodnout nějaký termín, dokázala Kurtova známá získat dostatečné množství informací, aby útočník věděl, kdy bude pan Vittaro u sebe, což znamenalo také informaci o tom, kdy tam nebude. Přílišné úsilí nevyžadovalo ani zjištění, že sekretářka využije jeho nepřítomnosti a vyrazí na lyže. Krátkou dobu budou tedy pryč oba. Výborně.

První den jejich očekávané nepřítomnosti uskutečnil Kurt telefonát a předstíral, že má pro pana Vittara neodkladnou záležitost. Recepční odpověděla:

„Pan Vittaro není ve své kanceláři. A jeho sekretářka také ne. Nebudou ani zítra ani pozítří."

Už první pokus přesvědčit nového zaměstnance, aby se jeho plánu účastnil, se povedl. Anna ani nemrkla okem, když jí požádal o stažení "rukopisu", který byl ve skutečnosti populárním obecně přístupným *monitorujícím programem* upraveným tak, aby proběhla *tichá instalace*, Při této metodě nebude program odhalen žádným antivirovým softwarem. Z nepochopitelných důvodů výrobci antivirových programů nevytvářejí programy, které by odhalovaly obecně dostupné monitorující prograny.

Žargon
****
Monitorující program (ang. *spyware*) — speciální software, který skrytě monitoruje události na sledovaném počítači. Takovéto programy jsou používané kromě jiného ke sledování stránek, které navštěvují lidé nakupující prostřednictvím Internetu, aby byly publikované reklamy šité na míru podle jejich zájmu. Kromě toho může software plnit funkci „štěnice" (v tomto případě je tím „odposlouchávaným" počítač). Program zachycuje každou aktivitu uživatele včetně zadávání hesel, stisku kláves, elektronické pošty, chatování, komunikačních programů typu ICQ a všech navštívených webových stránek, dokonce i kopií obrazovek uživatele.
Tichá instalace (ang. *silent install*) — taková metoda instalace aplikace, kdy si uživatel ani neuvědomí, že k něčemu takovému vůbec došlo.
****

Ihned potom, co mladá žena stáhla program na počítač Rona Vittara, přihlásil se Kurt ke své webové stránce a zaměnil soubor *manuscript.doc.exe* za rukopis knížky, který našel na Internetu. To pro případ, kdyby podvod někdo odhalil a vrátil se na jeho stránku, aby zjistil, co se vlastně stalo — našel by pak pouze nevinný amatérský a k vydání zcela nevhodný rukopis.

Po nainstalování programu a opětovném spuštění počítače se monitoring ihned aktivoval. Ron Vittaro se za pár dní vrátí a začne pracovat s počítačem a počítač bude předávat všechny stisknuté klávesy, odeslanou poštu i kopie obrazovek ukazující obsah dokumentů zobrazovaných na monitoru. Všechny tyto informace budou v pravidelných intervalech posílány na bezplatný e-mailový server na Ukrajině.

Během několika dní po příjezdu Rona Vittara se Kurt probíral logy hromadícími se v ukrajinské poštovní schránce a brzy našel důvěrné maily, ze kterých se dalo usoudit, jak daleko může nakladatelství Millard-Feton Publishing při vyjednávání s autorem zajít. Vybavený touto znalostí bude autorův agent schopný vyjednat mnohem lepší podmínky/ než které byly nabídnuty na počátku, aniž by hrozila ztráta kontraktu. Bylo to pochopitelně spojené s vyšší provizí pro agenta.

Analýza podvodu

V této akci podvodník uspěl hlavně díky využití nového pracovníka v roli prostředníka, jelikož počítal s jeho větší ochotou ke spolupráci — chce se uvést jako dobrý spolupracovník — a v menší míře také protože bude mít menší znalosti o firmě, její struktuře a zavedených postupech, které by mohly útok zmařit.

Kurt v rozhovoru s Annou z finančního oddělení předstíral, že je viceprezident, a v této souvislosti je málo pravděpodobné, že se Anna bude zabývat otázkou jeho totožnosti. Spíš ji mohlo těšit pomyslem, že si získá uznání, když pomůže viceprezidentovi.

Celý proces instalace monitorujícího programu, kterým Annu provedl, vypadal zdánlivě nevinně. Neměla ponětí, že to, co dělá, pomůže útočníkovi získat cenné informace, které mohou být využity proti zájmům podniku.

A proč se Kurt rozhodl předávat informace z viceprezidentova počítače do emailové schránky na Ukrajině? Vzdálená tajná schránka z několika důvodů ztěžuje akce namířené proti útočníkovi. Zločiny tohoto druhu nemají v takových zemích jako je Ukrajina, kde milice často nebere zločiny přes Internet příliš vážně, obyčejně nijak vysokou prioritu. Z tohoto hlediska je umístění tajné schránky v zemi, která s americkými úřady spíše nebude spolupracovat, dobrá strategie.

Prevence

Sociotechnik bude vždy dávat přednost útoku na pracovníka, u kterého jeho žádosti nebudou vzbuzovat velké podezření. Nejenže mu to usnadní práci, ale také ho to vystavuje menšímu riziku — což příběhy v této kapitole potvrzují.

> *Poznámka Mitnicka*
> **********
> Žádost o službičku směrovaná ke spolupracovníkovi nebo k podřízenému je normální věc. Sociotechnik ví, jak využít naši přirozenou ochotu ke spolupráci a pomoci. Útočník touto pozitivní lidskou vlastností manipuluje a přemlouvá nás k činnostem, které ho přibližují k cíli. Pochopení této prosté zásady je důležité — dovoluje to obrnit se proti manipulacím tohoto typu.
> **********

Využívání neopatrnosti

Již dříve jsem zdůrazňoval nutnost vyškolení pracovníků tak, aby se nikdy nedali přesvědčit cizím člověkem, který je žádá o službu. Všichni zaměstnanci si také musejí uvědomovat nebezpečí, které je spojené s vykonáváním nějaké činnosti na počítači jiné osoby na žádost cizího člověka.

Mělo by to být zakázané, ledaže by s tím výjimečně nadřízený souhlasil Tyto výjimky se mohou týkat následujících situací:

- Žádost o pomoc pochází od člověka, kterého známe a který nás o to požádá osobně nebo jehož hlas v telefonu nepochybně poznáme.
- Po pozitivním ověření totožnosti žadatele podle schválených pokynů.
- Když byla žádost potvrzena nadřízeným nebo jinou osobou na odpovídající pozici, která osobně zná člověka, který o službu žádá.

Na školení se zaměstnanci musejí naučit odmítat pomoc lidem, které neznají osobně, dokonce i v tom případě, kdy se žadatel prohlašuje za někoho z vedení. V okamžiku zavedení ověřovacích postupu musí vedení začít podporovat zaměstnance, aby tyto postupy používali, dokonce i tehdy, když to znamená odmítnutí pomoci členu vedení, který se snaží bezpečnostní procedury obejít.

Každá firma by také měla mít instrukce, podle kterých by pracovníci měli při vyřizování žádostí o vykonání nějaké činnosti na počítači nebo na podobném zařízení postupovat. V příběhu o nakladatelství si sociotechnik vybral za cíl zaměstnance, který neprošel školením z procedur a praktik svázaných s bezpečností informací. Aby se útokům tohoto typu předcházelo, každý zaměstnanec, ať už dlouholetý nebo nový, se musí držet prosté zásady: nedělej nic na počítači na žádost neznámé osoby. Tečka.

Je nutné si pamatovat, že každý pracovník, který má fyzický nebo elektronický přístup k počítači či zařízení podobného typu, je vystavený

nebezpečí manipulace ze strany útočníka, který se ho může snažit přesvědčit, aby vykonal jisté úkony.

Zaměstnanci, a zejména personál informatiky, si musejí uvědomovat to, že umožnění přístupu do vnitřní sítě osobě zvenku je stejné, jako kdyby sdělili číslo konta telemarketingové firmě nebo číslo kreditní karty cizímu člověku, který zrovna sedí ve vězení. Pracovníci si musejí dávat pozor, jestli vyslyšení prosby nemůže vést ke zpřístupnění důvěrných informací nebo usnadnit nabourání do firemního počítačového systému.

Informatici si musejí dávat pozor na neznámé volající, kteří se představují jako zástupci dodavatele softwaru. Firma by se měla zamyslet nad určením kontaktních osob pro každého dodavatele s tím, že jiní pracovníci nemohou odpovídat na požadavky zástupců dodavatele na zpřístupnění informací na téma používaných technologií nebo na zadání změn v jakémkoli počítačovém nebo telekomunikačním zařízení. Při tomto přístupu se určení lidé seznámí s personálem dodavatele, který telefonuje nebo navštěvuje firmu a jsou tak méně vystaveni útokům podvodníků. Pokud volá představitel výrobce, se kterým firma nemá podepsanou žádnou servisní dohodu, mělo by to také vzbudit podezření.

Každý člen organizace by si měl být vědom rizika ohrožení bezpečnosti dat. Je nezbytné, aby pracovníci ochrany kromě normálního školení v oblasti bezpečnosti museli projít školením také z oblasti bezpečnosti informací. Poněvadž tito lidé mají často fyzický přístup do všech místností ve firmě, musejí být schopní rozeznat typy sociotechnických útoků, které mohou být proti nim podniknuty.

Pozor na spyware

Komerční monitorující programy byly zpočátku používané rodiči, kteří chtěli kontrolovat děti surfující po Internetu, nebo zaměstnavateli, kteří kontrolovali, jestli se zaměstnanci nepoflakují na Internetu místo toho, aby pracovali. Vážnější bylo jejich využití při odhalování potenciálních zlodějů informací nebo průmyslových špiónů. Výrobci nabízejí své monitorovací programy jako nástroje pomáhající chránit děti, ačkoli ve skutečnosti jsou kupujícími ti, kteří touží někoho špehovat. Dnes je prodej monitorujících programů hnaný především touhou přesvědčit se, jestli nás manžel či partner nepodvádí.

Než jsem začal psát pro tuto knížku příběh o monitorujícím programu, člověk, který pro mě přijímá maily (já sám mám zákaz používání Internetu), narazil na dopis obsahující reklamu na monitorující programy. Jeden z nich byl popsán takto:

Náš favorit. Musíš ho mít! Tento monitorující program tajně zaznamenává všechny stisknuté klávesy, čas otevření a název každého aktivního okcna přímo do textového souboru a pracuje skrytě na pozadí. Textové soubory mohou být šifrované a automaticky zasílané na uvedenou e-mailovou adresu nebo jen zapisované na harddisk. Přístup k programu je chráněn heslem a lze ho skrýt tak. že nebude vidět ani v menu CTRL+ALT+DEL. Díky němu je možné monitorovat zadané adresy URL. session chatu, e-maily a mnoho dalších věcí (dokonce i hesla :-)) Nainstaluj ho na LIBOVOLNÉM počítači a nech si posílat logy!!! !!!

Jiný program nabízený ve stejném mailu sliboval zaznamenávat obrazovkv uživatele tak, jako by za jeho zády byla umístěna kamera. Některé tyto programy dokonce ani nevyžadují fyzický přístup k počítači oběti. Stačí nainstalovat a zkonfigurovat aplikaci na dálku a máte ihned počítačový odposlech. FBI musí tuto technologii zbožňovat.

Když jsou monitorovací programy obecně dostupné, musejí firmy zavést dvě úrovně ochrany. Měly by na všech počítačích nainstalovat software, který odhaluje monitorovací programy, například SpyCop (dostupný na adrese www.spycop.com) a po zaměstnancích vyžadovat pravidelné skenování systému.

Kromě toho by mělo proběhnout školení zaměstnanců, aby si dávali pozor na manipulátory, kteří se je pokoušejí přesvědčit, ke stažení programu nebo otevření přílohy v poště, což by mohlo vést k instalaci monitorujícího programu.

Navíc, abychom se vyhnuli instalaci programu v době chvilkové nepřítomnosti zaměstnance v kanceláři, lze zavést povinnost zabezpečit počítač šetřičem obrazovky s heslem nebo nějakou podobnou metodou – značně to zmenší riziko, že neoprávněná osoba získá přístup k počítači některého ze zaměstnanců. Tímto způsobem by vetřelec, kterému by se podařilo nepozorovaně proklouznout do kanceláře nepřítomného pracovníka, neměl přístup k jeho souborům, a ani možnost instalovat monitorovací programy. Nastavení hesla na šetřiči obrazovky nevyžaduje žádné náklady a zisk z ochrany počítačů může být značný. Bilance zisků a ztrát by měla být v této situaci očividná.

Díra v antivirových programech?

****

Antivirový software neodhaluje po světě rozšířené monitorovací programy. Nepovažuje je za nebezpečné ani tehdy, když jsou používány ke špehování jiných lidí. Počítačová obdoba odposlechu tak prochází nepovšimnuta a proto je na každodenním pořádku. Takto je každý z nás vystaven riziku sledování. Samozřejmě výrobci antivirových programů budou tvrdit, že monitorující programy mohou být používány legálně, takže není vhodné s nimi zacházet jako s viry. Na druhou stranu však podobné nástroje vytvořené a používané komunitou hackerů, které byly později zdarma nebo za poplatek zpřístupněné, jsou nadále pokládány za nebezpečné. Je tu jistá nedůslednost a stále přemýšlím, proč...

****

13

Rafinované triky

Víme už, že když neznámá osoba telefonuje s prosbou o poskytnutí důvěrné informace nebo žádá o něco, co může být pro pracovníka cenné, musí byt ten, kdo hovor přijímá, vyškolen tak, aby se zeptal na telefonní číslo volajícího a zavolal mu zpátky. Tak se přesvědčí, jestli je volající skutečně ten, za koho se vydává, například pracovník firmy, zaměstnanec spolupracující firmy nebo technik některého z jejích dodavatelů.

Ale i když firma zavede postupy pro pečlivé ověřování volajících, budou mít útočníci v zásobě mnoho triků, jak své oběti obalamutit a ujistit je o své totožnosti. Dokonce i ostražitý pracovník se může stát obětí níže uvedených metod.

Klamavá identifikace

Každý, kdo měl co do činění s mobilním telefonem, se setkal s funkcí nazývanou identifikace volajícího nebo identifikace příchozích hovorů - na displeji telefonu se zobrazuje telefonní číslo člověka, který nám volá. Pro firmu je to dost užitečná funkce — umožňuje pracovníkům rychle se zorientovat, jestli je daný telefonát od spolupracovníka z firmy nebo od osoby zvenku.

Před mnoha lety se několik ctižádostivých phreakerú začalo možnostmi takové identifikace zabývat, ještě než dostaly telekomunikační firmy svolení nabízet tuto službu široké veřejnosti. Byla to legrace oslovit volajícího jménem, než stačil pronést jediné slovo.

Předpokládejme, Že považujeme tuto službu za bezpečny způsob identifikace a zavedeme postupy založené na důvěře v informaci, která se na displeji objeví. Právě na to muže útočník sázet.

Telefon Lindě

Čas: úterý 23. července, 15.12

Místo: kanceláře finančního oddělení firmy Starbeat Aviation

Telefon Lindy Hill zazvonil v okamžiku, kdy psala poznámku pro šéfa. Podívala se na displej, který ukazoval, že volá nějaký Victor Martin z hlavního sídla firmy v New Yorku — to jméno jí ale nic neříkalo.

Chvíli to nechtěla zvedat, ať to vezme záznamník, protože nechtěla přetrhnout tok myšlenek spojený s psaním. Nakonec však zvědavost zvítězila a Linda sluchátko zvedla. Volající se představil a řekl, že volá z oddělení public relations a že pracuje na nějakém materiálu pro prezidenta společnosti.

„Prezident právě letí do Bostonu na jednání s našimi bankéři a potřebuje finanční přehled za poslední kvartál," řekl. „A ještě jedna věc. Potřebuje také finanční program projektu Apache," dodal Victor. Apache byl pracovní název produktu, který se měl objevit na jaře.

Požádala ho tedy o jeho e-mailovou adresu, ale řekl, že má problém s přijímáním pošty, na kterém právě pracuje technik, a jestli by mu tedy mohla poslat materiály faxem. Souhlasila a on jí sdělil vnitřní číslo faxu.

O pár minut později nafaxovala materiály.

Victor však nepracoval v oddělení public relations. Nebyl dokonce ani zaměstnancem firmy.

Příběh Jacka

Jack Dawkins začal svou profesionální kariéru již v útlém věku. Jako kapsář působil během zápasů na stadionu Yankee Stadium, v přeplněných chodbách metra i ve večerním davu turistů na Time Square. Byl tak obratný a mazaný, že dokázal sundat z cizí ruky hodinky, aniž ty si toho někdo všiml. Když povyrostl a stal se teenagerem, jeho zručnost se zhoršila a nakonec byl dopaden. Ve vězení však poznal nový obor, při kterém bylo riziko odhalení mnohem menší.

Poslední zakázka představovala zjistit bilanci zisku a ztrát za čtvrtletí a informace o příjmech jisté společnosti dříve, než je předá Komisi cenných papírů. Jeho zákazník byl zubař, který nechtěl prozradit, na co tyto informace potřebuje. Jacka bavila ta přehnaná opatrnost. Znal to už nazpaměť — chlápek měl zjevné problém v s hazardem nebo finančně náročnou milenku, se kterou se jeho žena ještě neměla to štěstí seznámit. A třeba jenom prostě chtěl dokázat své ženě, že má talent investovat na burze a ztratil značnou částku peněz. Teď chtěl vsadit sice hodně, ale zato na jistého koně, když bude vědět, co se stane s cenou akcií po oznámení čtvrtletních výsledků.

Lidé bývají překvapení, když vidí, jak rychle dokáže bystrý sociotechnik nalézt řešení situace, se kterou se dříve nesetkal. Než se Jack ze schůzky s dentistou vrátil, začal se mu v hlavě rýsovat plán. Jeho přítel, Charles Bates, pracoval ve společnosti Panda Importing, která měla vlastní telefonní ústřednu.

Ústředna byla zapojena na digitální službu, nazývaná T1, která byla zkonfigurována jako hlavní interface (PRI) sítě ISDN. Znamenalo to, že každý telefonát uskutečněný ze sídla firmy Panda byl do firemní ústředny doprovázen nastavením a dalšími informacemi spojenými s hovorem zaslanými přes datový kanál. Informace obsahovaly číslo volajícího, které (pokud nebylo zablokováno) bylo předáváno na telefon, který hovor přijal.

Jackův přítel věděl, jak centrálu naprogramovat, aby osoba na druhé straně neviděla číslo telefonu z firmy Panda, ale jakékoliv jiné číslo, které tam naprogramuje. Tento trik funguje, protože místní telekomunikační firmy nekontrolují, jestli se zobrazovaná čísla shodují s čísly, za která dostávají zaplaceno.

Jack Dawkins potřeboval tedy pouze přístup ke službě tohoto typu. Naštěstí jeho přítel a občasný spolupachatel Charles Bates byl za pevnou částku vždy ochotný pomoci. Pro tuto příležitost Jack a Charles dočasně přeprogramovali ústřednu tak, aby se rozhovory z jedné linky zobrazovaly jako vnitřní číslo Victora Martina z firmy Starbeat Aviation.

Telefonní číslo objevující se na displeji je jen zřídka ověřováno, protože si jen málo lidí uvědomuje, že je možné ho změnit. V tomto případě poslala Linda bez rozmyslu fax člověkovi, o kterém si myslela, že je z oddělení public relations.

Když Jack zavěsil, Charles přeprogramoval ústřednu do původního stavu.

Analýza podvodu

Některé firmy nechtějí, aby klienti nebo dodavatelé znali telefonní čísla zaměstnanců. Například Ford se může rozhodnout, že telefony ze zákaznického centra se budou zobrazovat jako číslo zelené linky do centra a název typu „Ford — podpora" místo zobrazení skutečného čísla konzultanta, který volá. Microsoft zase může zaměstnancům ponechat možnost sdělování telefonních čísel

na sebe, zároveň však vypnout zobrarazení jejich čísel, aby nikdo nemohl ihned poznat vnitřní linku. Takto firma zachovává důvěrnost svých vnitřních čísel.

Stejná možnost přeprogramování zobrazovaných čísel je nástrojem v rukou vtipálků, telefonických obchodníků a samozřejmě sociotechniků.

Volá prezident

Jako spolumoderátor pořadu „Temná strana Internetu" v KFI Talk Radio v Los Angeles jsem pracoval pro programového ředitele. David je ze všech lidí, které znám, snad nejvíc pohlcen svojí prací. Je tak zaneprázdněný, že je telefonicky prakticky nedosažitelný. Patří k těm lidem, kteří nezvedají telefony, ledaže by se tam zobrazilo číslo člověka, se kterým zrovna chtějí mluvit.

Když jsem mu volal z různých telefonů (na svém mobilu mám výchozí hovory blokované), nezvedal to a ozývala se jen hlasová schránka. Bylo to pro mne velmi frustrující.

Hovořil jsem o tom se starým známým, který je spoluzakladatelem firmy v oboru realit — pronajímá firmám kancelářské plochy. Společně jsme vymysleli jistý plán. On měl přístup k ústředně své firmy, Meridan, a mohl na ní naprogramovat číslo volající osoby tak, jak bylo popsáno dříve. Když jsem se musel nutně spojit s programovým ředitelem a nemohl jsem se mu dovolat, poprosil jsem přítele o naprogramování mnou zvoleného čísla, aby se objevilo na identifikátoru volajícího. Občas jsem dělal, jako že volá asistent z Davidovy kanceláře, jindy se zase objevilo číslo holdingu, které je vlastníkem rádia.

Mým oblíbeným kouskem však bylo naprogramování Davidova domácího čísla, což vždy zvedal. Přes všechno si ho velmi cením. Vždycky to bral sportovně, když po přijetí hovoru uslyšel, že se dal opět napálit. Nejlepší však bylo, že jsem si s ním mohl delší chvíli pohovořit a on se snažil řešit moje problémy.

Když jsem ten trik demonstroval v programu Art Bell Show, změnil jsem svou identifikaci tak, aby se zobrazovalo jméno a číslo sídla FBI v Los Angeles. Art byl dost šokovaný a pokáral mne, že to, co dělám je nezákonné. Odvětil jsem, zeje to úplně legální, pokud nemáme v úmys spáchat nějaký podvod. Po odvysílání pořadu jsem dostal několik mailú s dotazem, jak jsem to udělal. Tak ted už to víte.

Pro sociotechnika je to vynikající nástroj na budování důvěry. Pokud například v přípravné fázi před sociotechnickým útokem zjistí, že oběť využívá identifikaci hovorů, může útočník změnit svoje číslo na číslo důvěryhodné firmy nebo pracovníka. *Zloděj pohledávek* (ang. *bill collector*) může zařídit, že váš identifikátor bude ukazovat vaše pracoviště.

> *Žargon*
> **********
> **Zloděj pohledávek** — podvodník snažící se dostat k osobám, které mají prošlé závazky vůči různým institucím či firmám, představit se jako zástupce věřitele a pokusit se převzít dlužné peníze.
> **********

Zamysleme se však nad důsledky. Vetřelec nám může zavolat domů a hrát informatika z naší firmy. Musí nutně znát heslo, aby mohl obnovit naše soubory po havárií serveru. Nebo se nám objeví číslo naší banky či makléřské kanceláře — dívka s příjemným hlasem žádá pouze ověření našeho čísla konta a dívčího jména matky. Pro jistotu ještě prosí o kontrolu PIN z důvodů nějakých problémů se systémem. Někdo může uskutečnit hovor z burzy cenných papírů tak, aby se zdálo, že telefon přichází ze Citibank nebo Merril Lynch. Někdo, kdo chce získat naše osobní údaje, může například zatelefonovat z naší banky a

přemluvit nás, abychom sdělili číslo kreditní karty. Osoba, která se nám chce pomstít, se může představovat jako inspektor finančního úřadu nebo agent FBI.

Máme-li přístup k telefonnímu systému připojenému k PRI a trochu znalostí jeho programování — což lze jistě najít na internetové stránce dodavatele systému — můžeme provádět známým různé kousky. Známe třeba někoho s přehnanými politickými ambicemi? Stačí naprogramovat číslo 202 456-1414 a identifikace volajícího způsobí zobrazení nápisu „BÍLÝ DŮM".

Náš známý si pomyslí, že mu volá sám prezident!

Poučení z příběhu je jednoduché: není vhodné věřit tomu, co se nám objevuje na telefonu, ledaže by se to týkalo vnitřních linek. Doma i v práci si musíme uvědomovat tuto možnost a vědět, že identifikace volajícího nemůže být používána k verifikaci totožnosti volajícího.[23]

Poznámka Mitnicka
****
Až ti příště zazvoní telefon a jeho displej ti ukáže, že volá tvá drahá babička, vůbec si tím nemůžeš být jistý — možná ti volá nějaký drahý sociotechnik.
****

Neviditelný pracovník

Shirley Cutlass objevila nový fascinující způsob, jak si vydělat peníze. Je konec s trávením dlouhých hodin v kanceláři. Připojila se ke stovkám podvodníků odpovědných za největší vlnu zločinů desetiletí. Stala se zlodějem totožností.

Dnes měla v úmyslu získat důvěrné informace z oddělení zákaznických služeb jisté banky. Po shromáždění vstupních informací zvedla telefon a řekla telefonistce, že by chtěla spojit s telekomunikačním oddělením. Po spojení poprosila k telefonu správce hlasové pošty.

Na základě získaných informací vysvětluje, že se jmenuje Norma Todd a pracuje v kanceláři v Clevelandu. S použitím nám už známé finty řekla, že se vydává na týden do sídla firmy a bude potřebovat hlasovou schránku, aby nemusela k té své přistupovat přes meziměsto. Řekla, že nechce fyzické přípojení, pouze hlasovou schránku. Administrátor odpověděl, že se na to podívá a zavolá jí, až bude všechno hotovo, aby ji sdělil potřebné informace.

„Jsem ted na cestě na jednání, mohla bych zavolat tak za hodinu?" zeptala se milým hlasem.

Když se znovu ozvala, bylo už všechno zařízeno a dostala příslušné informace: vnitřní číslo a dočasné heslo. Administrátor se zeptal, jestli ví, jak si změnit heslo v hlasové poště. Dovolila mu, aby ji provedl přes příslušné kroky, ačkoli je znala přinejmenším stejně dobře jako on.

„A jen tak mimochodem," zeptala se. „Na jaké číslo mám volat z hotelu, abych si poslechla záznamy?"

Správce jí sdělil číslo.

Shirley tam zavolala, změnila si heslo a nahrála novou úvodní zprávu.

Shirley útočí

Snazší část úkolu měla už za sebou. Teď nastal čas na umění manipulace.

Zatelefonovala na firemní oddělení klientských služeb.

---

[23] Pozn. překl.: Možná jste si všimli, že hovory zvenčí a vnitřní mají různé vyzváněcí signály. Například tv zvenku jsou táhlé, kdežto z firmy jsou takové ukvapenejší.

„Volám z inkasního oddělení pobočky v Clevelandu," řekla a použila jednu z variant známého triku. „Můj počítač je v opravě a potřebovala bych pomoct s nalezením jisté informace."

Nadiktovala jméno a datum narození osoby, jejíž totožnost chtěla ukrást. Potom vyjmenovala informace, které potřebuje: adresu, dívcí jméno matky, číslo kreditní karty, limit kreditu, dostupný kredit a historii plateb.

„Zavolejte mi, prosím, na toto číslo," řekla a uvedla linku, kterou pro ni vytvořil správce hlasové pošty. „Pokud budu mimo dosah, nechte mi ty informace v hlasové schránce."

Zbytek dopoledne strávila zařizováním různých záležitostí, aby se odpoledne konečně podívala na svoji schránku. Než zavěsila, vymazala úvodní zprávu. Ponechání nahrávky s vlastním hlasem by nebylo zrovna vrcholem opatrnosti.

Krádež totožnosti se v Americe stává čím dál tím rozšířenějším zločinem, zločinem 21. století. Shirley může s těmito informacemi v ruce dělat nákupy na náklady své oběti.

Analýza podvodu

V tomto příběhu útočnice nejprve obelstila správce hlasové pošty, když se představila jako pracovnice firmy a žádala ho o založení dočasné hlasové schránky. Pokud by se pokusil o ověření její věrohodnosti, ukázalo by se, že jméno i telefonní číslo, které uvedla, opravdu figuruje na seznamu pracovníků.

Zbytek už závisel pouze na tom, jestli uvede věrohodnou příčinu potíží s počítačem, prosby o potřebné informace a jejich nahrání na hlasovou schránku. Proč by pracovník nemel poskytnout tyto informace jinému zaměstnanci? Telefonní číslo, které uvedla, bylo vnitřní, takže nebyl žádný důvod k pochybnostem.

Poznámka Mitnicka
****
zkoušejte občas svou vlastní hlasovou schránku. Pokud uslyšíme uvítání nahrané cizí osobou, možná se jedná o naše první setkání se sociotechnikem.
****

Nápomocná sekretářka

Robert Jordan byl cracker a pravidelně se nabourával do počítačové sítě globální korporace Rudolpho Shipping, Inc. Ve firmě si nakonec všimli, že někdo hackuje jejich server a získává odtamtud přístup ke všem počítačovým systémům. Aby firma svoji sít zabezpečila, rozhodla se zavést heslo na telefonické spojení s každým serverem.

Robert zavolal na síťové operační středisko a předstíral, že je advokát z právního oddělení a že má problém s připojením se k síti. Administrátor, na kterého narazil, mu objasnil, že z důvodu bezpečností musejí všichni uživatelé, kteří se připojují zvenku, získat hesla na daný měsíc od svého šéfa. Robert se zajímal, jak jsou hesla předávána vědoucím nebo jak je oni mohou získat. Ukázalo se, že heslo na následující měsíc bylo rozesílané vnitřní poštou každému vedoucímu.

To celou záležitost usnadnilo. Robert provedl malý průzkum, zavolal do do firmy hned po prvním dnu nového měsíce a spojil se se sekretářkou jednoho oddělení, která se představila jako Janet.

„Ahoj, Janet, tady Randy Goldstein z rozvojového oddělení. Vím, že jsem dostal papír s heslem na telefonické připojování k síti, ale nemohu ho nikde najít. Ty už jsi to lejstro dostala?"

Odpověděla, že dostala.

Zeptal se jí, jestli by mu ho nemohla nafaxovat. Souhlasila. Sdělil ji číslo faxu na recepční ve foyer jiné budovy firmy, kde už dříve poprosil, aby fax pro něj rovnou předali dál. Tentokrát Robert použil jinou metodu přesměrování faxu. Uvedl recepční číslo na internetovou službu přijímající fax. Když tato služba přijme fax, je automaticky předávaný na e-mailovou adresu abonenta.

Nové heslo dorazilo do zřízené tajné schránky — na bezplatné e-mailové konto v Číně. Byl si jist, že pokud snad bude někdy fax vystopován, vyšetřovatel si bude rvát vlasy při pokusech o navázání spolupráce s čínskými orgány, které v záležitostech tohoto druhu pomáhají jen neochotně. Nejlepší však bylo to, že se nemusel nikde osobně ukazovat, aby fax převzal.

Poznámka Mitnicka
****
Dobrý sociotechnik prokazuje při ovlivňování lidí velkou mazanost, aby od nich získal nějakou službičku. Přijetí faxu a jeho předání dál se zdá být tak neškodné, že přemluvit recepční je neobyčejně snadné. Když nás někdo nezámý prosí o službu spojenou s předáním nějaké informace a nemáme možnost ověřit si jeho totožnost, stačí prostě odmítnout.
****

Pokuta

Snad každý, kdo někdy dostal pokutu za překročeni rychlosti se zamýšlel, jestli by se s tím nedalo něco udělat, aby ten problém jaksi zmizel. Ale tak, aby nebylo nutné platit příslušnou částku nebo se pokoušet přesvědčit soud, že policejní radar nebyl kalibrován. Nejlepší by bylo, kdyby se nám podařilo nějak oblafnout systém.

Podvod

Ačkoliv takové způsoby řešení pokut nedoporučuji (všechno, co děláš, děláš na své vlastní triko), je to dobrý příklad na ukázku, jak může umění klamu sociotechnikovi pomoci.

Našmu silničnímu pirátovi můžeme říkat Paul Durea.

První kroky

„Policie, služebna Hollenbeck."

„Dobrý den, chtěl bych mluvit s někým, kdo se zabývá záležitostmi svědčení u soudních jednání."

„Tím se zabývám já."

„Výborně. Tady John Leland. Jsem právníkem z firmy Meecham and Talbott. Chtěl bych pozvat za svědka jednoho z vašich lidí."

„Kterého?"

„Pracuje u vás nějaký Kendall?"

„Jaké má číslo?"

„21349."

„Ano. Kdy ho potřebujete?"

„Někdy příští měsíc, ale ještě musím pozvat několik jiných svědků a teprve potom určit termín. Nemá příští měsíc pan Kendall naplánovanou nějakou nepřítomnost?"

„Koukneme se... Má dovolenou od dvacátého do třiadvacátého a školení od osmého do šestnáctého."

„Děkuji. Zatím je to všechno. Zavolám, až bude určen termín soudního jednání.“

Kancelář oblastního soudu

Paul: „Chtěl bych naplánovat termín jednání ohledně té pokuty."

Úředník: „Dobrá. Mohu vám nabídnout šestadvacátého příští měsíc."

"Chtěl bych se také domluvit na úvodní výslech."

„Vy chcete úvodní výslech v záležitosti pokuty?"

„Ano.“

„No Dobrá. Termín by mohl být zítra ráno nebo odpoledne. Který se vám hodí?“

„Odpoledne.“

„Výslech bude zítra v půl druhé, jednací síň číslo 6."

„Děkuji, budu tam.“

Oblastní soud, jednací síň číslo 6

Čas: úterý 13.45

Zapisovatelka: „Pane Durea, prosím, předstupte na stanoviště svědků."

Soudce: „Pane Durea, byl jste už poučen o svých právech?"

Paul: „Ano, vaše ctihodnosti."

Soudce: „Chcete využít možnosti zúčastnit se školení v autoškole? Vaše záležitost bude po absolvování osmihodinového kursu odložena. Prostudoval jsem váš spis a tato možnost by tu byla."

Paul: „Ne, vaše ctihodnosti. S veškerou úctou prosím, aby proběhlo jednání. Ještě jedna prosba, vaše ctihodnosti, cestuji do zahraničí, ale budu zde osmého a devátého. Byla by možnost určit termín projednávání mého případu na jeden z těch dní? Zítra odlétám na služební cestu do Evropy a vrátím se za čtyři týdny."

Soudce: „Dobře. V tom případě určujeme datum jednání na 8. června 8.30, jednací síň číslo 4."

Paul: „Děkuji, vaše ctihodnosti."

Oblastní soud, jednací síň číslo 4

Paul dorazil k soudu dříve, v osm hodin. Když se objevil soudce, zapisovatelka mu dala seznam případů, na které nedorazili svědkové z policie. Soudce si zavolal obhájce, mezi nimi i Paulova advokáta a oznámil jim, že jejich případy jsou odložené.

Analýza podvodu

Když policista vystavuje pokutu, podepisuje ji svým jménem a číslem odznaku. Nalézt stanici, kde pracuje, je hračka. Stačí zavolat na telefonní informace s dotazem na telefonní číslo služebny uvedené na předvolání. Po

spojení se službukonajícím policistou se lze zeptat na číslo úředníka, který zařizuje svědčení policistů z oblasti, kde jsme byli pokutováni.

Policisté jsou předváláváni k soudu s pravidelností, která záleží na konkrétním teritoriu. Když oblastní prokurátor nebo obhájce chtějí předvolat za svědka policistu, vědí, jak systém funguje a nejprve se snaží ujistit se, že daný policista bude dosažitelný. K tomu stačí zavolat s dotazem příslušnému úředníkovi, který dostavování se policistů jako svědků organizuje.

Obvykle se během takového rozhovoru právník ptá úředníka, jestli daný policista bude moci přijít toho a toho dne. Zde potřeboval Paul trochu citu: musel uvést hodnověrný důvod, proč ho zajímají data, kdy tu daný policista nebude.

Proč Paul během první návštěvy u soudu prostě neřekl, které datum ho zajímá? To je jednoduché — podle toho, co je známo, většinou soudní úředníci neumožňují stranám výběr data jednání. Pokud datum, které navrhne úředník, straně nevyhovuje, nabídne jí jeden nebo dva alternativní termíny, ale s více ať raději nepočítá. Na druhou stranu každý, kdo vyjádří ochotu dostavit se k výslechu, má v této oblasti obvykle více štěstí.

Paul věděl, že má nárok na žádost o výslech. Věděl také, že se soudci často prosbám o určení termínu jednání na konkrétní den přizpůsobí, poprosil tedy jemně o datum, které kolidovalo se školením policisty. Věděl, že v tomto státě má školení přednost před dostavením se k soudu.

Když se policista nedostaví, je záležitost odložena. Nebude žádný trest, povinné školení ani trestné body. A, což je nejdůležitější, naše akta zůstávají čistá!

Myslím, že až si policisté, soudní úředníci, oblastní prokurátoři a podobně přečtou tento příběh, souhlasně přitakají, že je takový úskok možný. Ale kromě toho přikývnutí určitě nic jiného neudělají. Jsem připraven se vsadit. Dokud je policie ochotná podávat informace o rozvrhu práce policistů prakticky každé osobě, která zavolá, do té doby bude možné vyhnout se pokutám. Nejsou v naší organizaci podobné díry, které by dovolily chytrému sociotechnikovi získat informace, které mu rozhodně nenáleží?

> *Poznámka Mitnicka*
> **********
> Lidská mysl je ohromující. Je zajímavé, jak se stáváme vynalézaví, když jde o hledání oklik, abychom něco získali nebo abychom se dostali z nějaké patálie. Stejnou vynalézavost bychom měli projevit při zabezpečování informací a počítačových systémů, jak ve veřejném sektoru, tak i v soukromém. Mějme na paměti, abychom se, až budeme vytvářet bezpečnostní politiku naší firmy, snažili o to, aby naše myšlenky šly mimo zažité šablony.
> **********

Samanthina pomsta

Samantha Gregson byla vzteky bez sebe.

Těžce pracovala, aby získala titul inženýra ekonomie, o úvěrech na studia nemluvě. Vždy se jí zdálo, že tento titul znamená kariéru místo obvyklé práce a při té příležitosti také velké peníze. Bohužel však nemohla po ukončení školy nikde najít dobré místo.

Zaradovala se, když konečně dostala nabídku z Lambert Man facturing. Pravda, pozice sekretářky byla trochu ponižující, ale pan Cartright říkal, že jim na ní hodně záleží a práce sekretářky jí otevře cestu k postupu.

O dva měsíce později slyšela, že jeden z vedoucích výroby od Cartrighta odchází. Tu noc skoro nemohla usnout, představovala si sebe samu v samostatné kanceláři na pátém patře, jak se účastní jednání a činí rozhodnutí.

Hned ráno zamířila do kanceláře pana Cartrighta. Řekl jí, že si myslí že by se měla o oboru dozvědět ještě trochu více, než bude na takovou funkci připravena. A zaměstnal amatéra zvenku, který o oboru věděl rozhodně méně než ona.

A tehdy jí začalo svítat. Firma zaměstnává hodně žen, ale skoro všechny jsou sekretářkami. Vypadalo to, že zde místo vedoucího nikdy nedostane.

Odveta

Promýšlení pomsty ji zabralo skoro celý týden. Před zhruba měsícem se jí snažil vyzpovídat novinář z oborového časopisu, když tu byl na premiéře nového produktu. O pár týdnů později jí zatelefonoval do práce a řekl, že pokud mu pošle nějaké informace o postupech práce na projektu Cobra 273, tak ji pošle květiny. A pokud ty informace budou opravdu senzační, tak se bude obtěžovat přijet až z Chicaga jen proto, aby ji pozval na oběd.

Jednoho dne byla v místnosti u pana Johannsona, když se právě logoval do sítě. Bezmyšlenkovitě pozorovala jeho prsty na klávesnici. Zadával heslo „marty63".

Její plán se začal rýsovat. Zapamatovala si obsah jedné z poznámek, kterou přepisovala brzy po nástupu do práce. Našla soubor s její kopií a napsala novou verzi v příslušném stylu. Její verze zněla takto:

> Komu: C. Pelton. odd. informatiky
> Od: L. Cartright. odd. rozvoje
> Martin Johannson bude pracovat v mém oddělení ve skupině speciálních projektů. Timto ho zplnomocňuji k přístupu na servery používané inženýry.
> Profil pana Johannsona musí být upraven tak. aby měl stejná práva, jaká mají osoby vyvíjející produkt.
> Louis Cartright

Když většina, lidí odešla na oběd, vystřihla z předchozího dopisu Cartrightův podpis a nalepila ho na nový, potom zaretušovala okraje bělobou. Na kopírce udělala kopii vzniklého dokumentu a posléze kopii kopie. Na ní už byly okraje okolo podpisu prakticky neviditelné.

Nafaxovala to přístrojem vedle kanceláře pana Cartrighta.

O tři dny později zůstala po pracovní době a čekala, až všichni odejdou z práce. Přešla do kanceláře Johannsona a pokusila se přihlásit do sítě pomocí jeho uživatelského jména a hesla „marty63". Podařilo se.

Bylo jen otázkou minut, než našla soubory se specifikacemi produktu Cobra 273 a nahrála je na zip disk.[24]

Disk byl bezpečně uložen v kabelce, když šla v mrazivém večerním větru k parkovišti. Ještě dnes to pošle reportérovi.

Analýza podvodu

Nespokojený pracovník, prohledání souborů, rychlé padělání podpisu, něco kopírování a jeden fax. Voilá! — Přístup k důvěrným specifikacím produktu a marketingovým datům je otevřen.

O několik dní později zveřejnil časopis z branže senzační informace obsahující specifikace a marketingové plány nového, převratného produktu, které se tak ocitly v rukou předplatitelů časopisu měsíce před jeho premiérou. Konkurenční firmy budou mít několik měsíců na zahájení vlastních

[24] Pozn. překl.: Nabízím výsledek nereprezentativní ankety, jak v češtině označují uživatelé výměnný zip disk o kapacitě 100 nebo 250 MB firmy iomega: zipka, zipketa, zip disketa, zipina.

prací na novém produktu a na spuštění odpovídající kampaně, která Cobru 273 podkope.

Časopis pochopitelně svůj zdroj nikdy neprozradil.

Prevence

Když jsou pracovníci žádáni o poskytování důležitých, důvěrných nebo kritických informací, které by mohly přinést užitek konkurenci nebo komukoliv jinému, musejí si být vědomi, že identifikace volajícího na displeji nemůže být nástrojem ověření totožnosti. V takových případech je nutné používat jiné prostředky ověřování, například dotaz u šéfa dané osoby, jestli žádost autorizoval a jestli je žadatel oprávněn takové informace obdržet.

Proces verifikace vyžaduje vyváženost, kterou si musí každá firma určit sama: bezpečnost versus produktivita. Jakou prioritu dáme zvyšování bezpečnosti firmy? Nebudou pracovníci vykazovat nechuť přizpůsobit se bezpečnostním procedurám a nebudou je dokonce obcházet, aby své povinnosti plnili rychleji? Chápou zaměstnanci, proč je bezpečnost pro firmu důležitá? Abychom uzpůsobili bezpečnostní politiku potřebám a kultuře naší organizace, je nutné si na výše uvedené otázky odpovědět.

Většina lidí nevyhnutelně začíná považovat za obtěžující všechno, co jim překáží při práci, a může začít obcházet všechny bezpečnostní prostředky, které se zdají být jen ztrátou času. Klíčová je tedy motivace zaměstnanců jejich vzděláváním a poučováním tak, aby se myslet na bezpečnost stalo součástí jejich každodenních povinností.

Ačkoli jako prostředek verifikace nemůže být používána identifikace volajícího, může k tomuto účelu posloužit jiná služba, nazvaná automatická identifikace čísla (ANI). Tato služba je k dispozici, když si firma zaplatí bezplatnou telefonní linku a platí za příchozí hovory. Tu jako ověřovací prostředek používat lze. Na rozdíl od identifikace volajícího se ke zobrazení čísla v ústředně telekomunikační firmy nevyužívá žádné informace pocházející od klienta. Číslo vysílané přes ANI je číslo, za které volající osoba platí účty.

Několik firem vyrábějících modemy doplnilo svá zařízení o funkci identifikace spojení, aby bylo možné lépe chránit firemní sítě a umožnit vzdálený přístup pouze telefonním číslům z dříve autorizovaného seznamu. Modemy s identifikací spojení jsou přijatelným prostředkem autorizace v případě nepříliš velkého potenciálního ohrožení bezpečnosti. Mělo by ale být jasné, že záměna čísla je pro počítačové vetřelce relativně jednoduchá záležitost, a proto není dobré se na tuto identinkaci spoléhat v případech většího ohrožení bezpečnosti.

Chceme-li předejít krádežím totožnosti, jako tomu bylo v příběhu s administrátorem vytvářejícím hlasovou schránku v telefonním systému firmy, je dobré zavést požadavek, že všechny telefonní služby, hlasové schránky i změny v telefonním seznamu jak v papírové, tak i v elektronické verzi by měly být prováděny pouze na písemnou žádost podanou na zvláštním, k tomuto účelu vytvořeném formuláři. Žádost by měla být podepsána nadřízeným osoby žádající o změnu a administrátor by si tento podpis měl ověřit.

Bezpečnostní politika firmy by měla vyžadovat, aby se zakládání počítačových kont nebo zvyšování přístupových práv provádělo pouze po pozitivním ověření osoby, která o to žádá, například po telefonátu administrátora systému nebo jeho zástupce na číslo, které je uvedené ve firemním telefonním seznamu. Pokud firma používá bezpečnou elektronickou poštu, kde mohou pracovníci využívat elektronické podpisy, lze ji využít jako alternativní metodu verifikace.

Je dobré mít na paměti, že každý zaměstnanec, nezávisle na tom, zda má přístup k firemním počítačům nebo ne, se může stát obětí socioiotechnika. Proto musí každá osoba projít bezpečnostním školením. Asistenti vedení, recepční, telefonistky i pracovníci ochrany by měli vědět, jaké druhy

sociotechnických útoků mohou být namířené proti nim, aby byli lépe připraveni na jejich eventuální odražení.

14

Průmyslová špionáž

Ohrožení vlád, firem a vědeckých institucí útoky, jejichž cílem je krádež informací, je všeobecné. Snad každý den přinášejí média zprávy o nových počítačových virech nebo o krádeži údajů o kreditních kartách z nějakého internetového obchodu.

Občas čítáme také o případech průmyslové špionáže: firma Borland obviňuje Symantec z krádeže obchodního tajemství, Cadence Design Systems vyvolává proces proti konkurenci kvůli krádeži zdrojového kódu. Mnoho lidí z oboru si tyto příběhy čte a myslí si, že něco takového by se v jejich firmě nemohlo stát.

Ale stává se. Každý den.

Variace schématu

Lest popsaná v následujících řádcích byla použita už mnohokrát, i když se zdá, že patří spíše do filmů typu *The Insider* nebo do románů Johna Grishama.

Proces

Představme si proces vedený na základě hromadné žaloby proti velké farmaceutické firmě Pharmomedic. Ve firmě si prý byli vědomi toho, že jeden z jimi vyráběných léků měl škodlivé vedlejší účinky na organismus, které se objevovaly teprve po jeho několikaletém užívání. Podle žaloby měl výrobce výsledky několika výzkumů, které toto ohrožení odhalovaly, ale důkazy zatajil a nepředal je FDA (Food and Drugs Administration — Úřad pro potraviny a léky), což byla jeho povinnost.

William („Billy") Chaney, advokát z newyorské kanceláře, která proces vyvolala, měl písemné svědectví dvou lékařů, kteří se k žalobě připojili. Oba však už byli v důchodu a neměli žádnou dokumentaci ani záznamy o léku, a proto nebyli příliš přesvědčivými svědky.

Billy si uvědomoval, že mu hoří půda pod nohama. Pokud nezíská kopii jedné z těch výzkumných zpráv, nějaký vnitřní dokument nebo jinou formu korespondence mezi vedením, pak bude případ prohraný.

Najal si tedy detektivní kancelář, jejíž služby využíval už dříve Anderson and Sons. Billy nevěděl a nechtěl vědět, jak Pete a jeho lidé všechny ty informace získávají. Jediné, co věděl jistě, bylo, že Pete Anderson je dobrý detektiv.

Anderson nazývá zakázky tohoto typu „černá práce". První pravidlo zní, že právnické kanceláře a firmy, které si ho najímají, se nikdy nedovídají, jak informace získal, takže jsou čisté. Celé případné riziko akce bere na sebe. Peníze, které za velké zakázky dostával, toto riziko kompenzovaly. Kromě toho jistě cítil osobní uspokojení, když přelstil inteligentní protivníky.

Pokud dokumenty, které chtěl Chaney získat, skutečně existovaly a nebyly zničené, měly by se nacházet někde ve spisech firmy Pharmo-medic. Ale jejich hledání v ohromné sbírce dokumentů velké firmy by byla sisyfovská práce. A co když firma předala kopie dokumentů své právní kanceláři, Jenkins and Petry?

Jestli obhájci o existenci těch dokumentů věděli a v procesu je neukázali, pak porušili kánon a etiku svého povolání i samotný zákon. Pokud tomu tak bylo, Pete mohl jednat, aniž by se musel na cokoliv ohlížet.

Pete útočí

Několik Petových lidí zahájilo průzkum a po několika dnech už věděl, u které externí firmy si kancelář uchovává záložní kopie svých dokumentů. Věděl také, že tato firma si vede seznam osob, které jsou oprávněné pásky s kopiemi za kancelář vyzvedávat. Každá z těchto osob měla vlastní heslo. Pete poslal dva lidi na černou práci.

Ve tři hodiny ráno si otevřeli zámek u dveří pomocí jednoho z paklíčů, které si objednali na adrese *www.southord.com* . Za několik minut vklouzli do kanceláří firmy a spustili počítače. Když uviděli logo Windows 98, na jejich tvářích se objevil úsměv — práce bude snadná-Windows 98 nevyžadují žádnou identifikaci. Po chvilce hledání narazili na databázi v Microsoft Accesu, která obsahovala jména lidí, oprávněných vyzvedávat pásky za firmu Jenkins and Petry. Přidali do toho seznamu jméno z falešného řidičského průkazu, který jeden z nich už dříve získal. Nemohli se jednoduše vloupat tam, kde byly skladovány pásky, a najít tu, na které jim záleží? Samozřejmě, že mohli. Ale pak by byli všichni zákáznici firmy, včetně té právní kanceláře, na vloupání upozorněni, útočníci by tak ztratili převahu. Profesionálové si rádi nechávají do hudoucna otevřené dveře.

Podle zásady průmyslových Špiónů, která káže shromaždovat další informace, které by se mohly později hodit, si pro všechny případy soubor se seznamem oprávněných osob zkopírovali na disketu. Neudělali to kvůli nějakému konkrétním nápadu, pouze podle pravidla „když už tady jsme, tak...". Byla to právě jedna z těch věcí, které by se mohly někdy jindy hodit.

Následujícího dne jeden z dvojice mužů zatelefonoval do firmy přechovávající záložní kopie, použil dopsané jméno a uvedl odpovídající heslo. Požádal o pásky firmy Jenkins and Petry z posledního měsíce a řekl, že si je vyzvedne kurýrní služba. Odpoledne už byly pásky v Andersonových rukou. Jeho lidé ve vlastním počítačovém systému data obnovili a připravili je k prohledávání. Anderson byl potěšen, že se kancelář, jak ostatně většina firem, nestarala o zašifrování dat na zálohovacích páskách.

Pásky byly externí firmě vráceny další den. Nikdo si ničeho nevšiml.

Analýza podvodu

Kvůli slabému fyzickému zabezpečení dokázali vetřelci snadno otevřít zámek u dveří firmy a získali přístup k počítačům. Upravili databázi obsahující seznam lidí oprávněných zacházet s páskami. Přidání jména do seznamu umožnilo podvodníkům „půjčit si" záložní kopie, na kterých jim záleželo, aniž by se museli vloupat do místnosti, kde byly uskladněné. A poněvadž většina firem na záložních kopiích data nešifruje, byly informace podány jako na talíři.

Tento incident ukazuje, jak dodavatelská firma, která neuplatňuje základní bezpečnostní zásady, může vystavit data svých klientů nebezpečí krádeže.

> *Poznámka Mitnicka*
> **********
> Cenné informace musejí být chráněné nezávisle na jejich formě i na místě jejich uložení. Seznam klientů firmy má jako výpis, jako soubor i jako páska stále stejnou hodnotu. Sociotechnici vždy útočí na místo, které lze nejsnáze obejít, které je nejméně chráněné. Útok na externí firmu, která skladuje záložní kopie, se bude vždy zdát méně riskantní. Každá organizace, která uchovává u třetích osob data pro svoji činnost cenná,

důvěrná nebo kritická, by je měla šifrovat, čímž bude chránit jejich důvěrnost.
****

Nový společník

Sociotechnici mají oproti tradičním podvodníkům jednu velkou výhodu – odstup. Podvodník nás obelstí pouze při bezprostředním kontaktu, čímž riskuje, že si zapamatujeme jeho popis, nebo že dokonce zatelefonujeme na policii, když včas podvod zvětříme.

Sociotechnici se obvykle bezprostřednímu kontaktu vyhýbají. Občas je však riziko s tím spojené vyváženo potenciální odměnou.

Příběh Jessicy

Jessica Andover byla spokojená, že dostala místo v moderní firmě zabývající se robotikou. Zpočátku samozřejmě moc nevydělávala, ale firma měla komorní atmosféru, lidé byli přátelští a vždycky existovala šance, že náhle zbohatne díky zaměstnaneckému balíku akcií, který dostala. No, možná nebude milionářka jako zakladatelé firmy, ale vydělá opravdu hodně peněz.

V úterý vesel Rick Daggot do foyer firmy se zářivým úsměvem ve tváři. V drahém obleku od Armaniho, s bezvadným účesem, s blýskajícími se zlatými hodinkami Rolex President šířil okolo sebe atmosféru sebejistoty, po které šílely všechny dívky, když Jessica chodila na gymnázium.

„Dobrý den," řekl. „Jsem Rick Daggot a mám tu schůzku s Larrym."

Úsměv z tváře Jessicy zmizel.

„S Larrym?" podivila se. „Ten je přece celý týden na dovolené."

„Byl jsem s ním domluvený na jednu hodinu. Právě jsem přiletěl z Louisvillu, abych se s ním setkal," pověděl Rick, vytáhl svůj palmtop, zapnul ho a ukázal jí datum.

Podívala se a zlehka přikývla.

„Dvacátého," řekla. „To je za týden."

Rick zvedl svůj palmtop a začal na něj civět.

„Ach ne," zaúpěl. „To snad není možné, že jsem udělal takovou idiotskou chybu!"

„Mám alespoň zarezervovat zpáteční let?" zeptala se účastně.

Během telefonování jí Rick prozradil, že chtějí s Larrym uzavřít strategické spojenectví. Rickova firma vytvářela produkty pro výrobní a montážní linky, které by dokonale doplňovaly jejich nový produkt C2Alpha. C2Alpha spolu s Rickovým produktem tvořilo kompletní řešení, které mohlo oběma firmám otevřít cestu na důležité trhy.

Když Jessica dokončila rezervaci na večerní let, Rick řekl:

„Možná bych si mohl popovídat alespoň se Stevem, pokud je u sebe. Viceprezident a společník Steve také nebyl.

Rick byl na Jessicu velmi milý a dokonce s ní trochu flirtoval. Navrhl, že když už přijel a zpáteční let má až večer, chtěl by pozvat pár lidí na oběd. A dodal:

„Vás samozřejmě také – je tu někdo, kdo to tady za vás může vzít?"

Omámená skutečností, že s ní počítá, se zeptala:

„Kdo chcete, aby šel?"

Znovu se podíval do svého palmtopu a vyjmenoval několik osob – dva inženýry z oddělení výzkumu a vývoje, nového člověka z odbytu a marketingu a člověka z finančního, který byl do toho projektu zapojen. Rick navrhl, aby jim řekla, jaký má k firmě vztah a že by se jim chtěl osobně představit. Jmenoval nejlepší restauraci v okolí – kam Jessica vždycky toužila někdy

zajít – a řekl, že sám zarezervuje stůl na 12.30 a za nějakou chvíli zavolá, aby se ujistil, že je všechno připraveno.

Když se setkali v restauraci – oni čtyři a Jessica – jejich stůl ještě nebyl připravený, tak se posadili u baru a Rick oznámil, že všechno platí. Rick měl úroveň a styl, v jeho společnosti se všichni cítili skvěle. Jako by se znali léta. Vždy věděl, co říci, měl trefné poznámky nebo říkal něco zábavného, když rozhovor začal váznout; každý se s ním cítil dobře.

Podělil se s nimi o dostatečný počet podrobností na téma svých vlastních produktů, aby si mohli představit myšlenku společného řešení, kterým se zdál být tak nadšený. Jmenoval několik největších firem v zemi, kterým už ted své výrobky prodával, což způsobilo, že si všichni kolem začali představovat nevyhnutelný úspěch v okamžiku, kdy kompletní produkt vyjede z výrobních pásů.

Později se Rick přitočil k Brianovi, jednomu z inženýrů. Zatímco zbytek se bavil mezi sebou, Rick se s ním podělil o několik koncepcí a získal pár detailů o C2Alpha zároveň s popisem odlišností tohoto projektu od konkurenčních produktů. Brian se zmínil o několika detailech, které jsou podle něho „prima", ale firma je spíš bagatelizuje.

Rick postupně hovořil osobně se všemi přítomnými. Člověk z marketingu byl rád, že si konečně mohl popovídat o datu premiéry a o marketingových plánech. Člověk z finančního vytáhl z kapsy obálku a napsal na ni podrobnosti materiálových a výrobních nákladů, navrhovanou cenu, očekávanou marži a to, jaké podmínky chce vyjednat s každým z dodavatelů, které jmenoval.

Než byl stůl připraven, stačil si Rick vyměnit pár slov s každým z přítomných a získal si tím spojence. Po jídle všichni Rickovi poděkovali a podali si ruce. Rick si se všemi vyměnil vizitky a Brianovi se při té příležitosti zmínil, že by si s ním chtěl domluvit delší schůzku, až se Larry vrátí.

Druhý den měl Brian telefon. Volal Rick, že právě mluvil s Larrym.

„Přijedu opět v pondělí, abych s ním probral pár detailů," řekl Rick. „Larry chce, abych byl v obraze, co se týče vašeho produktu. Říkal, že mu máte poslat nejnovější specifikace a projekty. On z nich vybere věci které bych měl vědět a ty mi potom pošle."

Inženýr řekl, že se o to postará.

„Dobře," odpověděl Rick. „Larry prosil, abych vyřídil, že má problémy se stahováním své pošty," pokračoval. „Že mu to nemáte posílat na jeho normální adresu, ale na účet na Yahoo, který si založil v hotelu. Tady je adresa, na kterou se mají soubory poslat: *larryrobotics@yahoo.com*."

Když se následující pondělí opálený a odpočatý Larry objevil v práci, nemohla se Jessica udržet, aby se o Rickovi nezmínila.

„Takový skvělý člověk. Pozval několik z nás na oběd, dokonce i mě."

Larry vypadal překvapeně:

„Rick? Jaký zase Rick?!"

„Jak to jaký? Přece tvůj nový společník."

„Kdo??!!!"

„Všichni jsme s ním byli nadšení. Měl otázky k věci."

„Neznám žádného Ricka..."

„Co je to s tebou, Larry? To je nějaký vtip? Děláš si blázny, že?"

„Svolej celé vedení do zasedačky. Hned! Je úplně jedno, co právě dělají. A všechny, co byli na tom obědě, včetně tebe."

Usedli okolo stolu v pohřební náladě. Skoro nemluvili. Larry přišel, posadil se a řekl:

„Neznám nikoho, kdo by se jmenoval Rick. Nemám žádného nového společníka, kterého bych měl před vámi tajit. Myslel jsem, že je to jasné. Pokud je vtipálek, který to vymyslel, mezi námi, ať se přihlásí."

Ticho. Atmosféra se stávala čím dál tím víc ponurá.

Nakonec se ozval Brian.

„Proč jsi mi nic neřekl, když jsem ti poslal ten mail se specifikacemi produktu a zdrojáky?"

„Jaký mail?!"

„Do pytle!" ztuhl Brian.

Do hovoru se vmísil Cliff, druhý inženýr:

„Všem nám dal vizitky. Musíme mu zavolat a záležitost si vyjasnit.

Brian vytáhl svůj palmtop, vyhledal číslo a podal ho přes stůl Larrymu. S kapkou naděje všichni hleděli jak hypnotizovaní, jak Larry vytáčí číslo. Po chvíli zmáčkl tlačítko hlasitého telefonu a všichni slyšeli signál obsazeno. Po několika dalších pokusech během následujících dvaceti minut vytočil frustrovaný Larry telefonní ústřednu, aby poprosil o havarijní přerušení hovoru a o spojení s tímto číslem.

Když se operátorka po několika chvílích vrátila k hovoru, zeptala se poněkud podezíravě:

„Kde jste, prosím, vzal to číslo?"

Larry jí řekl, že bylo na vizitce člověka, se kterým se musím naléhavě spojit. Operátorka odvětila:

„Je mi líto, ale to je testovací číslo telekomunikací. Vždycky je obsazené."

Larry začal dávat dohromady seznam informací, které Rick získal, nevypadalo to moc dobře.

Přijeli dva vyšetřovatelé z policie, aby sepsali protokol. Když si celou věc vyslechli, prohlásili, že podle zákonů státu nebyl spáchán žádný zločin. Nemohli nic dělat. Poradili Larrymu, aby se spojil s FBI, protože ta se zabývá zločiny spojenými s mezistátní hospodářskou činností. Když Rick Daggot pod cizím jménem požádal inženýra, aby mu poslal data, možná spáchal federální zločin, ale aby se to potvrdilo, je třeba si promluvit s FBI.

O tři měsíce později seděl Larry v kuchyni a četl si u snídaně ranní noviny, když náhle málem vylil kávu. Věc, které se od okamžiku, kdy uslyšel o Rickovi, nejvíce obával, se stala skutečností. Na první straně ekonomické přílohy bylo černé na bílém napsáno, že firma, o které nikdy neslyšel, ohlašuje premiéru nového produktu, přesně takového jako C2Alpha, na kterém on pracoval dva roky.

Kvůli jednomu podvodu utrpěl porážku na trhu. Jeho sny byly v troskách. Miliony dolarů investované do výzkumu a vývoje byly ztracené. A navíc nemohl s největší pravděpodobností nikomu nic dokázat.

Příběh Sama Stanforda

Sam Stanford byl natolik chytrý, že by si mohl vydělávat dobré peníze poctivě, ale byl také natolik pokřivený, že dával přednost tomu, živit se podvody. A nedařilo se mu špatně. Časem si ho všiml jistý špion, který byl předčasně penzionovaný kvůli problémům s alkoholem. Zahořklý a pomstychtivý začal prodávat své schopnosti v oblastech, ve kterých se za ta léta práce pro vládu stal odborníkem. Pořád se poohlížel po lidech, které by mohl využít. Sama si všiml už při jejich prvním setkání- Ukázalo se, že přenesení zájmu z lidských peněženek na firemní tajemství pro něj nepředstavovalo žádný problém.

* * *

Většina lidí by neměla odvahu něco takového udělat. Něco jiného je pokusit se obelstít někoho přes telefon nebo přes Internet, kde nás nemá nikdo šanci uvidět. Každý dobrý podvodník ze staré školy (dodnes jich je kolem nás hodně, víc, než by se mohlo zdát) se ale dovede podívat přímo do očí, říct drzou lež a zařídit, abychom jí uvěřili. Znám asi dva prokurátory, kteří to považují za kriminální čin. Já si myslím, že je to prostě talent.

Není však možné začít naslepo. Nejprve je třeba posoudit situaci. Pouliční podvodník může odhadnout člověka po krátkém přátelském rozhovoru a několika dobře obalených slovech. Pokud člověk reaguje podle jeho předpokladů, znamená to, že skočil na špek.

Podvádění firem vyžaduje větší úsilí. Je potřeba se připravit, poznat oběti i jejich přání, naplánovat útok. Trpělivě dělat domácí úkoly. Určit svou roli a naučit se své věci. Bez takové přípravy nemá cenu nic začínat.

Přípravy na tuto akci mi zabraly více než tři týdny. Dva dny mne klient učil, čím se moje firma zabývá a jakým způsobem mám popisovat všechny klady strategického spojenectví.

Potom jsem měl štěstí. Zatelefonoval jsem do firmy a řekl jsem, že jsem z investiční společnosti a že bychom se s nimi rádi setkali. Žongloval jsem s daty, abych se dozvěděl, kdy budou všichni čtyři společníci během následujících dvou měsíců dosažitelní a jestli nebudou nějaké termíny, kterým bych se měl vyhnout, protože Larry nebude v práci. Budou. Ukázalo se, že Larry neměl dovolenou už dva roky, od té doby, co založil firmu, a jeho žena ho konečně vytáhla na „golfovou dovolenou" v prvním srpnovém týdnu.

To bylo za dva týdny. To jsem klidně mohl počkat.

Mezitím jsem získal z odborného Časopisu jméno reklamní agentury pracující pro firmu, o kterou mi šlo. Řekl jsem jim, že mě zajímá reklamní prostor, který poskytují té firmě, co se zabývá robotikou, a že bych chtěl s člověkem, který má tu firmu na starost, mluvit o práci pro moji vlastní společnost. Ukázalo se, že je to mladá energická dáma, které samozřejmě záleželo na tom, aby získala nového zákazníka. Během nákladného oběda s poněkud větším množstvím alkoholu, než byla zvyklá, dělala všechno, aby mně přesvědčila, že jsou opravdu vynikající, co se týče chápání potřeb klienta a vytváření účinných reklamních kampaní. Bylo těžké mne přesvědčit, dožadoval jsem se detailů. Než stačli číšníci odnést talíře z našeho stolu, prozradila mi pod mírným nátlakem o novém produktu a problémech firmy víc, než se dalo očekávat.

Všechno šlo jako po drátkách. Historku s rozpaky ohledně omylu v datu schůzky a že když už tam jsem, tak se alespoň seznámím s osazenstvem, spolkla recepční i s navijákem. Dokonce se mnou upřímně soucítila. Oběd mne stál 150 dolarů včetně spropitného. Získal jsem to, co jsem chtěl: telefonní čísla, pracovní pozice a jednoho klíčového člověka, který věřil, že jsem tím, za koho se vydávám. Přiznávám, že Brian mne potom trochu překvapil. Vypadal, že by mi bez řečí poslal všechno, oč bych ho požádal, ale když přišlo na věc, ucítil jsem, že se drží zpátky. Využil jsem e-mailové konto s Larryho jménem, které jsem si pro všechny případy připravil. Lidé z bezpečnostního oddělení firmy Yahoo pravděpodobně dodnes čekají, až konto znovu někdo použije, aby ho mohli vysledovat. Budou si asi muset ještě nějaký Čas počkat. Já už mám novou zakázku.

Analýza podvodu

Každý, kdo podvádí svoji oběť tváří v tvář, se musí prezentovat tak, aby byl v očích své oběti akceptovatelný. Jinak se bude chovat na dostizích, jinak v místní hospodě a ještě jinak v exkluzivní hotelové kavárně.

To samé se týká průmyslových špiónů. Útok může vyžadovat převléci se do obleku s kravatou či koupit drahý kufřík, pokud má špión v úmyslu vvdávat se za prezidenta velké společnosti, konzultanta nebo obchodního zástupce. Když se bude příště vydávat za informatika, technologa nebo někoho z podatelny, jeho oblečení a vzhled budou úplně jiné.

Věděl, že pokud chce do firmy infiltrovat, pak jeho Rick Daggot musí udělat dojem sebejistého a kompetentního člověka a opírat se o detailní znalosti branže a výrobku.

Informace potřebné před osobní návštěvou nebylo těžké získat. Použil jednoduchý trik, aby se dozvěděl, kdy bude šéf nepřítomný. Jistou výzvou, ale stále nepříliš velkou, bylo získání tolika informací o projektu, aby o něm mohl hovořit jako zasvěcená osoba. Informace tohoto druhu mají často někteří dodavatelé firmy, její investoři, bankéři nebo právní kanceláře. Útočník ale musí dávat pozor: najít někoho, kdo je schopen podělit se o potřebné

informace, může být obtížné. Na druhou stranu testování dvou, tří zdrojů, abychom našli ten pravý, zvyšuje riziko, že se někdo zorientuje. Tato cesta je nebezpečná. Rickové Daggotové tohoto světa musejí pečlivě vybírat a využívat každou informační cestu pouze jednou.

Oběd byl další riskantní záležitostí. První problém byl zařídit věci tak, aby byla možnost pohovořit si s každým osobně, dál od uší ostatních. Jessice řekl, že oběd v exkluzivní restauraci bude v půl jedné, ale stůl zarezervoval na jednu hodinu. Měl tak naději, že až se objeví na místě, Půjdou se na chvíli do baru něčeho napít. A tak se také stalo. Ideami Příležitost přistupovat postupně ke každému z nich a vyměnit si s ním Pár slov.

Stále však existovalo tolik možností prozrazení — špatná odpověd nebo nepromyšlená poznámka by mohly odhalit, že je podvodník. Pouze ohromně sebejistý a zkušený průmyslový špión by se odvážil riskovat tímto způsobem. Léta, která strávil jako pouliční šejdíř, vybudovála jeho sebejistotu a víru, že i když někde klopýtne, bude schopen věc natolik dobře zaretušovat, aby nevzbudil žádná podezření. Byla to nejnáročnější a nejnebezpečnější část celé operace. Vzrušení, které cítil, když se mu podařilo provést intriku hodnou filmu „Podraz", mu dovolilo uvědomit si, proč nemusí jezdit rychlými auty, skákat s padákem nebo podvádět svou ženu — dostatečnou hladinu adrenalinu mu nabízela jeho práce. Kolik tak lidí, přemýšlel, prožívá to, co on?

Poznámka Mitnicka
****
To, že se většina sociotechnických útoků odehrává po telefonu či e-mailem, neznamená, že se odvážný vetřelec nikdy neobjeví na půdě naší firmy osobně. Ve většině případů používají podvodníci sociotechniku, aby se dostali do budovy poté, co padělají identifikátor pracovníka pomocí obecně dostupných programů, jako je například Photoshop.
A vizitka s testovacím telefonním číslem telekomunikací? Televizní pořad The Rockford Files, což byl seriál o soukromých detektivech, jednou ukazoval chytrou a zároveň vtipnou techniku. Rockford (hrál ho James Garnet) má v autě přenosnou tiskárnu vizitek, kterou používá, aby si sám vytiskl vizitku vhodnou pro danou příležitost. Dnes si může sociotechnik opatřit vizitku v každém kopírovacím středisku během hodiny nebo si ji vytisknout doma na laserové tiskárně.
****

Poznámka
****
John Le Carré, autor knížek Špión, který přichází z chladu, Dokonalý špión a mnoha dalších, vyrostl jako syn prvotřídního podvodníka. Jako mládenec Le Carré s překvapením zjistil, že i když po otci zdědil schopnost podvádět jiné, sám býval naivní a často se stával obětí podvodníků. To dokazuje, že prakticky každý je vystaven riziku sociotechnického útoku — dokonce i jiný sociotechnik.
****

Přískoky vpřed

Hádanka: následující příběh se netýká průmyslové špionáže. Během čtení se, prosím, pokuste odpovědět na otázku, proč jsem se jej přesto rozhodl umístit v této kapitole!

Hany Tardy po návratu domů zahořkl. Služba u vojenského námořnictva vypadala jako velké dobrodružství, dokud ho nevyčerpal polygon. Vrátil se tedy do města, které tak nenáviděl, zapsal se na počítačový kurs na místní univerzitě a přemýšlel, jak by se celému světu pomstil.

Nakonec něco vymyslel. Se spolužákem z kursu seděli nad pivem, nadávali na svého instruktora — sarkastického a vševědoucího chlápka - až nakonec

společně vypracovali scénář, jak mu dát za vyučenou. Chtěli ukrást zdrojový kód populárního digitálního diáře (PDA), poslat no na instruktorův počítač a zanechat výraznou stopu, která by k němu vedla, takže by ho firma považovala za pachatele krádeže.

Nový kamarád, Karl Alexander, řekl, že „zná několik fíglů" a řekne Harrymu, jak na to a jak při tom nebýt dopaden.

Domácí úkoly

Počáteční průzkum ukázal, že produkt byl vytvářen ve Vývojovém centru umístěném v sídle výrobce PDA v zahraničí. Firma měla kromě toho oddělení výzkumu a rozvoje na půdě USA. Karl poznamenal, že to vypadá dobře, protože, aby se operace povedla, musí existovat v USA nějaké oddělení, které rovněž potřebuje přístup ke zdrojovému kódu.

Nyní byl Hany připravený zavolat do zahraničního vývojového centra. Měl v úmyslu prosit o soucit: „Proboha, mám strašný problém, potřebuji pomoci, prosím, pomozte!" Prosba měla být přirozeně poněkud subtilnější. Karl napsal Harrymu, co má říkat, ale ten to četl úplně uměle. Nakonec cvičil s Karlem tak dlouho, až to dokázal říct normálním tónem.

To, co nakonec do telefonu řekl, když Karl seděl vedle něho, znělo víceméně takto:

„Telefonuji z oddělení výzkumu a rozvoje v Minneapolis. Náš server chytil vira, který infikoval celý počítačový systém. Museli jsme znovu nainstalovat celý operační systém a potom, když jsme chtěli obnovit data ze záložních pásek, žádná nechtěla fungovat. Bohužel za udržování záložních kopií jsem odpovědný já. Šéf na mě ječí a celé vedení se hrozí, že jsme ztratili veškerá data. Potřeboval bych nejnovější verzi zdrojového kódu tak rychle, jak je to jen možné. Potřeboval bych, abyste zazipovali celý strom se zdrojáky a poslali mi ho."

V tomto okamžiku mu Karl napsal něco na kus papíru a Harry do telefonu řekl, že pouze chce, aby mu ten soubor přehráli vnitřní sítí do Minneapolis. To bylo neobyčejně důležité: když žádáme někoho o vydání souboru pouze do jiného oddělení téže firmy, uklidňujeme jeho případná podezření — co na tom může být špatného?

Člověk na druhé straně s tímto postupem souhlasil. Krok za krokem, se sekundujícím Karlem u boku, musel Harry vysvětlit, jak spustit pakování velkého množství zdrojového kódu do jednoho kompaktního suboru. Kromě toho mu navrhl název komprimovaného souboru „novadata". Díky tomu se prý vyhne pomíchání dobrého kódu se starými, Poškozenými soubory.

Následující krok musel Karl vysvětlit Harrymu dvakrát, než ho pochopil. Tento krok byl ústředním bodem celého plánu. Harry musel zavolat na oddělení výzkumu a rozvoje do Minneapolisu a říct někomu: „Chci vám poslat soubor, který vy za mně pošlete někomu jinému" — samozřejmě to bylo všechno obalené příslušnými zdůvodněními, která dají prosbě věrohodnost. Nejméně pochopitelné pro Harryho bylo to, že musel říci: „Chci vám poslat soubor", zatímco žádné posílání souboru nebylo v plánu. Musel zapůsobit, aby si člověk z oddělení výzkumu a rozvoje myslel, že soubor pochází od něho, zatímco ve skutečnosti obdrží centrum soubor s chráněným zdrojovým kódem z Evropy.

„Proč mu mám říkat, že je ten soubor ode mě, když přijde ze zámoří?" chtěl vědět Harry.

„Ten chlápek je pro nás právě nejdůležitější," vysvětloval Karl. „Má si myslet, že dělá pouze laskavost kolegovi z jiného oddělení na území USA, přijímá soubor a posílá ho dál."

Harry nakonec pochopil. Zavolal do oddělení výzkumu a rozvoje a požádal recepční o spojení s výpočetním centrem, kde zase poprosil o počítačového operátora. K telefonu přišel chlápek v Harryho věku. Harry ho pozdravil a řekl, že volá z výrobního závodu v Chicagu a že se pokouší poslat soubor do jedné firmy, která se podílí na práci na jejich projektu, ale: „Máme nějaký

problém s routerem a nemůžeme se odtud dostat na jejich síť. Mohl bych poslat soubor vám a až dorazí, že bych zavolal ještě jednou, abych vysvětlil, kam je potřeba ho poslat?"

Zatím šlo všechno podle plánu. Harry se zeptal, jestli má jejich výpočetní centrum *anonymní FTP*, které umožňuje přenos souborů bez nutnosti uvést heslo. Ano, *anonymní FTP* je dostupné a Harry obdržel jeho IP adresu.

> Žargon
> **********
> Anonymní FTP — služba umožňující přístup ke vzdálenému počítači, na kterém nemáme založené konto FTP (FTP je zkratka z Filé Transfer Protocol — protokol přenosu souborů). Přístup k anonymnímu FTP nevyžaduje heslo, ale přístupová práva jsou obvykle omezena jen na některé adresáře.
> **********

Když už měl Harry adresu, zavolal zpátky do zahraničního vývojového centra. Sbalený soubor byl mezitím připraven a Harry sdělil pokyny, jak přenést soubor na anonymní FTP. Než uplynulo pět minut, zapakovaný zdrojový kód byl přenesen k tomu klukovi z oddělení výzkumu a rozvoje.

Namočení oběti

Byli v polovině. Ted museli Harry a Karl chvíli počkat, než učiní další krok, aby měli jistotu, že soubor už dorazil. Mezitím přešli k instruktorově počítači a postarali se o dvě podstatné věci. Nejprve založili na instruktorově počítači anonymní FTP server, který bude konečnou stanicí pro cestující soubor.

Druhý krok řešil jistý podstatný problém. Nemohli přece říci člověku z oddělení výzkumu a rozvoje, aby poslal soubor na adresu typu, řekněme, warren@rms.ca.edu . Doména „edu" by celou boudu prozradila, protože i napůl bdělý informatik ji rozpozná jako adresu školy. Aby se tomu vyhnuli, zjistili si v systému Windows, jaká je číselná IP adresa počítače a v této podobě ji chtěli uvést.

Přišel čas, aby opět zatelefonovali operátorovi v oddělení výzkumu a rozvoje. Harry si ho vyžádal k telefonu a řekl: „Právě jsem odeslal ten soubor, můžeš se podívat, jestli už dorazil?"

Dorazil. Harry tedy poprosil, aby ho zkusil poslat dál a řekl mu IP adresu. Čekal na sluchátku, zatímco se operátor pokoušel připojit a zahájit přenos. S úsměvem na tváři hleděli na druhý konec místnosti, kde na instruktorově počítači poblikávala dioda pevného disku zaměstnaného přijímáním souboru.

Harry si s operátorem vyměnil pár poznámek o tom, že snad někdy v budoucnu budou počítače spolehlivější, poděkoval mu a rozloučil se.

Harry a Karl zkopírovali soubor z instruktorova počítače na dvě zip diskety, jednu pro každého, aby si ho mohli později prohlédnout. Připomínalo to krádež obrazu z muzea — lze se jím kochat pouze o samotě, nemůžete se s ním chlubit známým. I když v tomto případě byl ukraden pouze duplikát a originál zůstal v muzeu.

Karl provedl Harryho kroky, jak odstranit FTP server z instruktorova počítače a vymazat stopy jejich přítomnosti, aby nezůstaly nějaké důkazy toho, co udělali — pouze tam na viditelném místě nechali ukradený soubor. Posledním krokem bylo vyslání úryvku zdrojového kódu z instruktorova počítače na jednu z diskusních skupin. Byl to pouze malý fragment, který nemohl firmě způsobit žádnou škodu, ale zanechával výraznou stopu, která vedla směrem k instruktorovi. Bude mít co vysvětlovat.

Analýza podvodu

Celá akce zafungovala jako výsledek kombinace několika prvků, ale nikdy by se nepovedla bez šikovné hry na soucit a ochotu pomoci druhému člověku: šéf na mě ječí, celé vedení je v pozoru atp. To ve spojení s jasným vysvětlením, jak nám může člověk na druhé straně pomoci, znamenalo podstatu celého podvodu. Potvrdilo se to zde i v mnoha jiných situacích.

Druhý klíčový prvek: člověk, který si citlivou podstatu souboru uvědomoval, byl požádán pouze o vyslání souboru na vnitřní firemní adresu

A třetí prvek skládanky: operátor. Viděl, že soubor k němu přišel zevnitř firmy. Znamenalo to — nebo to tak alespoň vypadalo — že člověk, který mu soubor poslal, by ho mohl sám poslat kamkoliv, kdyby jeho externí síť fungovala správně. Co by tedy mělo být špatného na tom, když to pošle za něj?

Proč dali zkomprimovanému souboru právě takové jméno a ne jiné? Zdánlivě maličkost, ale velmi důležitá.

Útočník si nemohl dovolit, aby soubor dorazil se jménem, které by ho identifikovalo jako zdrojový kód nebo připomínalo jméno produktu. Prosba o vyslání souboru s takovým jménem mimo vnitřní síť firmy by mohla vzbudit podezření. Změna jména na docela nenápadné byla tedy klíčová. Jak se ukázalo, mladík z výpočetního centra neměl žádné zábrany před odesláním souboru ven. Soubor s názvem „novadata", který nijak nenaznačoval jeho skutečný obsah, neměl nárok, aby v něm vzbudil nějaké podezření.

Vraťme se k hádance. Už víte, proč byl tento příběh zařazen do kapitoly pojednávající o průmyslové špionáži? Pokud ne, zde je odpověď: to, co dva účastníci kursu učinili ze zlomyslnosti, mohl udělat profesionální průmyslový Špión placený konkurencí nebo vládou jiného státu. V každém z těchto případů by způsobená škoda mohla představovat pro společnost katastrofu a negativně ovlivnit příjmy z prodeje po tom, co by se objevil konkurenční produkt.

Je vaše firma zabezpečená před útokem tohoto druhu?

> Poznámka Mitnicka
> **********
> Zde je základní pravidlo, které by si měl každý pracovník navždy zapamatovat: bez souhlasu vedení nikdy neposílej soubory lidem, které osobně neznáš; dokonce ani tehdy, když se cíl zdá být uvnitř firemní počítačové sítě.
> **********

Prevence

Průmyslová špionáž, která je odedávna trápením mnoha podniků, se nyní stala všedním chlebem pro mnoho tradičních špiónů, kteří se po skončení studené války věnují placenému vykrádání firemních tajemství.

Zahraniční korporace a vlády využívají služeb průmyslových Špiónů na volné noze, aby vykrádaly informace. Firmy na území USA si rovněž najímají takzvané obchodníky s informacemi, kteří neváhají překročit zákon, aby získali přístup k důvěrným datům. V mnoha případech to jsou lidé, kteří dříve pracovali ve výzvědných službách a mají odpovídající znalosti a zkušenosti, což jim usnadňuje infiltraci do organizací. Týká se to zejména těch firem, které nedokázaly zavést odpovídající bezpečnostní prostředky pro ochranu svých informací ani vyškolit svoje lidi.

Bezpečnost směrem navenek

Co by mohlo pomoci firmě, která se dostala v souvislosti s přechováváním svých dat mimo firmu do potíží? Nebezpečí je možné se vyhnout šifrováním dat. Šifrování samozřejmě vyžaduje dodatečný čas i náklady, ale za tu námahu to stojí. Zašifrované soubory musejí být pravidelné namátkově kontrolovány, aby byla jistota, že šifrování funguje bez problémů.

Vždy existuje nebezpečí, že se Šifrovací klíče ztratí nebo že jedinou osobu, které je zná, srazí autobus. Ale toto nebezpečí se dá minimalizovat a každý, kdo přechovává své důvěrné informace mimo svou firmu, aniž by je šifroval, je s prominutím idiot. To je jako procházet se v nocí v nejhorší čtvrti s dvousetdolarovou bankovkou čouhající z kapsy — sami si říkáme o to, aby nás okradli.

Přechovávání záložních kopií na místě, kde není odpovídající dozor, je časté nedopatření. Před několika lety jsem byl zaměstnán ve firmě, která by mohla vynakládat při ochraně dat klientů trochu větší úsilí. Pracovníci zabývající se archivací nechávali záložní kopie mimo zamčený počítačový sál, aby si je kurýr mohl každý den vyzvednout. Prakticky každý mohl odtamtud vyjít se záložními kopiemi obsahujícími dokumenty v nezašifrované podobě. Pokud firma archivuje data zašifrovaná, jejich ztráta je nanejvýš otravná. Pokud firma data nešifruje — dobrá, pak určitě sama nejlépe dokáže odhadnout příslušný dopad.

Potřeba vnější archivace dat ve velkých firmách je odůvodněná. proto by se také bezpečnostní zásady měly vztahovat i na archivační firmu a mělo by se kontrolovat, nakolik svědomitě jsou tam dodržovány pokyny spojené s bezpečností. Pokud tato firma nepřikládá těmto záležitostem stejnou váhu jako naše společnost, znehodnocuje tím naše úsilí v této oblasti.

Menší firmy mají dobrou alternativu přechovávání záložních kopií. Mohou denně posílat nové i změněné soubory některé z firem nabízezících archivaci on-line. Zde je rovněž třeba mít na paměti, aby byla data zašifrovaná. Jinak se informace stanou přístupné nejen nějakému nepoctivému zaměstnanci archivační firmy, ale každému vetřelci, který by se mohl nabourat do jejího počítačového systému.

Pokud jsme zavedli systém šifrování zabezpečující naše záložní kopie je třeba také zavést vysoce bezpečnou proceduru přechovávání šifrovacího klíče nebo dešifrovacího hesla. Tajné šifrovací klíče by měly být umístěny v trezoru. Standardní postup by měl také předvídat situaci že pracovník odpovědný za tyto záležitosti může náhle firmu opustit nebo umřít. Vždy musejí být alespoň dvě osoby, které znají místo, kde jsou uložena data, šifrovací a dešifrovací procedury. Je třeba také určit kdy a jak se bude klíč měnit. Procedury musejí vyžadovat změnu klíče ihned poté, co z firmy odejde člověk, který k němu měl přístup.

Kdo je tam?

Příběh v této kapitole, popisující mazaného, rafinovaného podvodníka, který pomocí osobního kouzla vytahuje od zaměstnanců informace, znovu ukazuje důležitost ověřování totožnosti. Žádost o vyslání zdrojového kódu na FTP server rovněž dokazuje, jak je důležité znát osobu, která nás o něco Žádá.

V 16. kapitole se nacházejí konkrétní postupy ověřování totožnosti nám neznámé osoby, která žádá o informace nebo o vykonání nějaké činnosti. Otázky ověřování se nám v této knize vracejí jako bumerang — v 16. kapitole přejdeme k podrobnostem této procedury.

IV

Vozová hradba

Bezpečnost informací – informování a školení
Doporučená politika bezpečnosti informací

15

Bezpečnost informací — informování a školení

Sociotechnik právě dostal zakázku získat plány našeho nového objevného produktu, do jehož uvedení na trh zbývají dva měsíce. Co ho může zadržet?

Náš firevvall? — Ne.

Vyspělá ověřovací zařízení? — Ne.

Systém detekce vetřelců? — Ne.

Šifrování? — Ne.

Omezení přístupu k seznamu telefonních čísel, kterými se lze připojit k systému? — Ne.

Kódové názvy serverů ztěžující člověku zvenčí odhalit, na kterém serveru se nacházejí plány produktu? — Ne.

Opravdu neexistuje žádná technologie, která by mohla sociotechnickému útoku předcházet.

Technologická zabezpečení, školení a procedury

Firmy, které provádějí penetrační testy bezpečnostních systémů, uvádějí, že pokusy nabourat se do počítačového systému zákazníka pomocí sociotechnických metod jsou skoro stoprocentně účinné. Technologická zabezpečení mohou takové útoky ztížit tím, že minimalizují účast lidí v rozhodovacím procesu. Ale jedinou skutečně účinnou metodou oslabení tohoto ohrožení je použití technologických zabezpečení *v kombinaci* s bezpečnostními postupy, které určují základní principy chování pracovníků a také jejich odpovídající teoretické i praktické školení.

Existuje pouze jeden způsob ochrany plánů našeho produktu: mít vyškolené, informované a svědomité pracovníky. S tím se váže nutnost školení v oblasti bezpečnostní politiky a procedur a kromě toho — možná především — stálého připomínání. Někteří odborníci doporučují, aby 40 % rozpočtu určeného na bezpečnost bylo určeno na proces neustálého procvičování pracovníků v této oblasti.

Prvním krokem je uvědomění každého člena organizace, že existují lidé bez zábran, kteří se budou pokoušet manipulovat jimi pomocí podvodů a psychologických metod. Pracovníci musejí vědět, které informace je třeba chránit a jak. Jakmile pochopí, jak mohou být zmanipulováni, budou schopni dostatečně včas útok rozeznat.

Bezpečnostní informovanost znamená také vzdělávání všech zaměstnanců v oblasti firemní bezpečnostní politiky a postupů. Jak je uvedeno v 16. kapitole, taková politika je nezbytná pro vytváření pravidel chování, které mají za cíl chránit informační systémy a důvěrná data.

Tato a následující kapitola jsou věnované vytváření bezpečnostního systému, který nás ochrání před zhoubnými útoky. Pokud naši pracovníci nejsou vyškolení, pozorní a nepostupují podle propracovaných procedur, pak je jen otázkou času, kdy kvůli sociotechnickému útoku ztratíme nějaké informace. Nečekejme tedy, až se tak stane, protože ztráty firmy i zaměstnanců mohou být nenahraditelné.

Jak útočníci využívají lidskou přirozenost

Než začneme vytvářet úspěšný program školení, potřebujeme si nejprve uvědomit, proč jsou lidé vůči útokům zranitelní. Když tyto tendence během školení předvedeme — například pomocí hraných scének, které na ně upozorňují — usnadníme pracovníkům uvědomit si, že vŠichni můžeme podlehnout sociotechnikově manipulaci.

Manipulace je předmětem studia sociologů už nejméně padesát let. Článek Roberta B. Cialdiniho v *Scientific American* (únor 2001) shrnuje celý výzkum a ukazuje šest „základních vlastností lidské povahy", které se projevují při pokusu podřídit někoho vůli sociotechnika.

Právě na těchto šesti vlastnostech stavějí sociotechnici (vědomě či častěji podvědomě) během pokusů o manipulování s jinými.

Autorita

Lidé mají tendenci podřídit se vůli osoby, která má moc. Jak je ukázáno na jiném místě této knížky, člověk se může podřídit žádosti, když věří, že žadatel má moc nebo že je oprávněn žádat o danou službu.

Ve své knížce *Ovlivňování lidí. Teorie a praxe (Influence)* popisuje Dr. Cialdini případ tří nemocnic, ve kterých se jistá osoba vydávala za lékaře dané nemocnice. Nezávisle se zkontaktovala s 22 sestrami a dávala pokyny k dávkování léků pacientům na oddělení. Sestry, které přijímaly pokyny, volajícího neznaly. Nevěděly dokonce, jestli je ve skutečnosti lékařem (nebyl!). Přijímaly telefonické pokyny týkající se dávkování, což bylo porušením směrnic nemocnice. Lék, který měly podat, nebyl schválen k použití na odděleních a dávka, kterou měly dát, dvojnásobně překračovala maximální denní dávku tohoto léku a mohla ohrozit život pacientů. Cialdini píše, že v 95 % případů „se sestra vydávala směrem ke skříňce s léky, aby vzala navrženou dávku, načež zamířila k pacientovi". Posléze byla samozřejmě zastavena pozorovatelem, který ji informoval o experimentu.

Příklad útoku: sociotechnik se maskuje aureolou moci, říká, že pracuje v oddělení informatiky, je z vedení nebo pracuje pro někoho z vedení firmy.

Sympatie

Lidé mají sklon vyhovět, když je žadatel schopen ukázat se jako sympatická osoba, která má podobné zájmy, názory a přístup k životu jako oběť.

Příklad útoku: během rozhovoru se útočník dozvídá o nějakém koníčku nebo zájmu oběti a následně deklaruje svůj zájem a nadšení pro stejný koníček. Může též říci, že je ze stejného státu, kraje či školy nebo má stejné cíle. Sociotechnik se také bude snažit o podobné chování jako má oběť, aby vytvořil zdání podobnosti.

Vzájemnost

Můžeme se automaticky podřídit žádosti, jestliže nám bylo něco cenného slíbeno nebo dáno. Dárek může být hmotný nebo může představovat radu či pomoc. Když pro nás někdo něco udělal, cítíme potřebu odvděčit se. Tato silná potřeba se objevuje dokonce i tehdy, kdy jsme o to, co jsme dostali, nežádali. Jedním z nejúčinnějších způsobů ovlivňování lidí tak, aby nám

„udělali službičku", je dát jim nějaký dárek nebo pomoc, což vyvolá pocit vděčnosti.

Vyznavači Hare Krišny velmi účinně ovlivňovali lidi, aby od nich získali příspěvek, když jim na počátku dali jako dárek knížku nebo kytičku. Pokud se obdarovaný pokoušel dárek vrátit, oni ho odmítali přijmout se slovy: „To je náš dárek pro tebe". Využívání principu vzájemnosti značně zvyšovalo příspěvky.

Příklad útoku: pracovník přijímá hovor od osoby, která se představuje jako informatik. Vysvětluje, že některé počítače byly napadeny novým virem, který antivirový software neodhalí a který může zničit všechny soubory v počítači. Potom nabízí provést pracovníka přes několik kroků, které mu umožní předejít problému.

Hned potom volající prosí oběť o otestování nějaké aplikace, která byla právě vylepšená tak, že umožňuje uživatelům změnu hesla. Pracovník nejspíš neodmítne, protože volající mu právě pomohl při ochraně před virem. Revanšuje se tedy a vyhoví žádosti.

Důslednost

Lidé mají tendenci se podřídit, jestliže předtím veřejně vyhlásili svou podporu a angažovanost v dané záležitosti. Pokud jsme už jednou slíbili, že něco uděláme, nechceme vypadat nedůvěryhodně a postupujeme podle našich dřívějších prohlášení či slibů.

Příklad útoku: útočník se kontaktuje s poměrně novým pracovníkem a informuje ho o nutnosti přizpůsobit se bezpečnostní politice a procedurám, jakožto podmínce — získání přístupu k podnikovým počítačovým systémům. Po probrání několika bezpečnostních praktik žádá volající o sdělení hesla za účelem „kontroly jeho slučitelnosti" se směrnicemi přikazujícími výběr hesla, které by bylo těžké uhodnout. Když zaměstnanec heslo prozradí, útočník dává doporučení, jak vytvářet budoucí hesla tak, aby je sám dokázal snadno uhodnout. Oběť se podvoluje, protože se už dříve zavázala dodržovat firemní praktiky a ted může být přesvědčena, že volající je z firmy, který pouze kontroluje dodržoval těchto praktit.

Společenský souhlas

Lidé mají tendenci vyhovět prosbám, jestliže se to zdá shodné s chováním jiných. Příklad jiných je vnímán jako souhlas a potvrzení, že dané chování je správné a vhodné.

Příklad útoku: volající tvrdí, že provádí anketu a jmenuje několik osob z oddělení, které se už dříve rozhodly na otázky odpovědět. Oběť věří, že chování jiných potvrzuje věrohodnost žádosti, a souhlasí s účastí v anketě. Volající zadává řadu otázek, mezi nimiž se skrývá i dotaz na uživatelské jméno a heslo.

Vzácná příležitost

Lidé mají tendenci se podřídit, když věří, že vytoužený objekt je v malém množství a je žádaný mnoha jinými nebo je dostupný jen kratičký čas.

Příklad útoku: útočník rozesílá e-maily oznamující, že prvních 500 osob, které se zaregistrují na nové stránce firmy, vyhraje volné vstupenky na premiéru nejnovějšího filmu. Když se nic netušící osoba na webové stránce registruje, je žádána o uvedení své firemní e-mailové adresy a o zvolení hesla. Mnoho lidí má z pohodlnosti sklon používat to samé heslo v každém počítačovém systému, kam přistupuje. Útočník, který o tom ví, se může pokusit nabourat do našich firemních nebo soukromých počítačových systémů a využít k tomu uživatelské jméno a heslo, které jsme uvedli při registraci.

Vytváření programu školení a informovanosti

Vydání brožurky o bezpečnosti informací nebo odkázání pracovníků na internetovou stránku, která popisuje bezpečnostní politiku firmy, samo o sobě riziko nezmenšuje. Každá firma musí nejen zásady písemně definovat, ale musí vynaložit další úsilí s cílem přesvědčit *všechny* osoby, které mají co do činem s informacemi nebo počítačovými systémy, aby se zásady naučily a také podle nich postupovaly. Navíc je třeba se ujistit, že všichni rozumějí důvodům, proč byly jednotlivé principy zavedeny, aby se je nepokoušeli z pohodlnosti obejít. Jinak bude neznalost pro pracovníka vždy dobrou výmluvou a pro sociotechnika slabinou, kterou ochotně využije.

Hlavním cílem každého programu informovanosti je takové ovlivnění lidí, aby změnili svůj přístup a chování, a také jejich motivace, aby se sami *chtěli* účastnit v procesu ochrany informačního majetku firmy.

Vynikající motivací je v tomto případě popis prospěchu pro firmu i samotné pracovníky, který vyplývá z takovéhoto postoje. Protože firma má také část osobních informací každého zaměstnance, přispívání k ochraně firemních dat znamená rovněž příspěvek k ochraně osobních údajů.

Program školení z oblasti bezpečnosti vyžaduje značné úsilí. Školení musí zahrnout každého člověka ve firmě, který má přístup k důvěrným informacím nebo počítačovým systémům. Znalosti musejí být neustále osvěžovány a aktualizovány, aby se pracovníci mohli stavět proti stále novým hrozbám. Zaměstnanci musejí vidět, že management se v programu také plně účastní. Tato účast musí být opravdová a nesmí se omezovat na orazítkování spisu obsahujícího stručné instrukce. Program musí být podložený dostatečnými zdroji, aby bylo možné ho rozvíjet, diskutovat, testovat a analyzovat jeho úspěšnost.

Cíle

Základní směrnice, kterou je třeba mít při vytváření programu školení a informovanosti v záležitostech bezpečnosti na paměti, je soustředit se na vybudování povědomí u pracovníků, že útok může nastat kdykoli. Musejí se naučit, že každý zaměstnanec má při obraně proti pokusům získat přístup k počítačovému systému nebo krádeži důvěrných dat svou úlohu.

Protože je mnoho aspektů informační bezpečnosti spojených s technologiemi, začínají si pracovníci příliš snadno myslet, že tento problém řeší firewally a jiné zabezpečovací systémy. Základním cílem školení by mělo být vytvářet u lidí vědomí, že právě oni znamenají hlavní obrannou linii nezbytnou k zajištění úplné bezpečnosti v organizaci.

Školení musí mít vyšší cíl než pouhé oznámení zásad. Tvůrce programu školení musí rozeznávat silné pokušení části pracovníků pod nátlakem každodenních povinností obcházet či ignorovat bezpečnostní pokyny. Znalost taktik používaných sociotechniky i způsobu ochrany před nimi je důležitá, ale bude mít cenu pouze tehdy, když se školení soustředí na *motivaci* pracovníků využívat získané poznatky.

Firma může prohlásit, že program školení splnil základní požadavky-jestliže jsou všichni jednoznačně přesvědčení a motivováni jednou základní věcí: že zabezpečení informací tvoří součást jejich normálních povinností.

Pracovníci se musejí smířit se skutečností, že ohrožení sociotechnickým útokem je reálné a že vážná ztráta důvěrných informací muže ohrozit firmu, její pracovníky i jejich zaměstnání. V jistém smyslu je bezstarostný přístup k bezpečnosti informací stejný jako bezstarostný přístup k PIN kreditní karty. Tato analogie může pomoci při budování porozumění pro bezpečnostní praktiky.

Zavádění programu do života

Osoba odpovědná za vytvoření programu školení v oblasti bezpečnosti informací si musí být vědoma toho, že školení nemůže být stejné pro všechny. Školení musí být naplánované tak, aby odpovídalo specifickým nárokům různých skupin pracovníků podniku. Zatímco se hodně z doporučení obsažených v 16. kapitole vztahuje na všechny zaměstnance, část z nich má ohraničený okruh. Jako nezbytné minimum budě většina firem potřebovat programy uzpůsobené pro následující skupiny: vedení, informatický personál, počítačové uživatele, administrativní pracovníky, recepční a vrátné, pracovníky ostrahy. (V 16. kapitole se nacházejí podrobně vyjmenovaná doporučení v závislosti na postavení.)

Protože se od pracovníků bezpečnostní služby obvykle nevyžaduje obsluha počítače a prakticky nemají kontakt s podnikovou sítí, nejsou obvykle při vytváření programu bráni v úvahu. Sociotechnik však dokáže obelstít strážného tak, aby ho vpustil do budovy nebo vykonal nějaké činnosti, jejichž následkem dojde k nabourání do systému. To, že strážní nemusejí projít školením určeným pro uživatele firemních počítačů, ještě neznamená, že mají být při vytváření programu školení úplně opominuti. V organizaci je pravděpodobně jen málo záležitostí důležitých pro všechny pracovníky, které mají tak podstatný význam, a zároveň jsou tak nudné, jako jsou otázky bezpečnosti. Dobrý program školení musí současně informovat, poutat pozornost a vzbuzovat zájem posluchačů. Školení a udržování povědomí o bezpečnosti musí zaujímat pozornost a být interaktivní zkušeností. Používané techniky mohou demonstrovat sociotechnické metody pomocí scének s rozdělením rolí, přehledu zpráv ze sdělovacích prostředků o posledních případech útoků na smolařské firmy a probírání způsobů, jak by se tomu naše firma mohla vyhnout; stojí za to zamyslet se nad promítáním filmu na téma bezpečnostních zásad, který by byl zároveň zábavný i poučný. Existuje několik firem, které se zabývají distribucí filmů a materiálů týkajících se bezpečnostních otázek.

Příběhy popsané v této knize představují dobrý materiál, který objasňuje metody a taktiky používané sociotechniky, zvyšuje povědomí ohrožení a demonstruje slabiny lidského chování. Lze promyslet využití těchto scénářů jako základu při vytváření scének. Tyto příběhy rovněž provokují diskusi na téma, co by mohla oběť odpovědět, aby útok odrazila.

Dobrý tvůrce programu a dobrý školitel najdou vedle množství výzev také hodně postupů na oživení školení a v konečném výsledku i na motivaci lidí, aby se stali součástí mechanismu ochrany.

Poznámka
****
Instituce, které nemají možnost zorganizovat vnitřní školení z oblasti bezpečnosti, mohou využít nabídky některé ze školicích firem, které nabízejí kursy z této oblasti.
****

Struktura školení

Program základního bezpečnostního školení by měl být povinný pro všechny zaměstnance. U nových by se měla vyžadovat účast na takovém školení jako jeden z prvků jejich uvádění do práce. Doporučuji, aby jim byl přístup k počítači umožněn teprve po absolvování takového kursu.

Počáteční etapa školení by měla být natolik soustředěná, aby upoutala pozornost, a natolik krátká, aby byly důležité body zapamatovány. Samozřejmě množství otázek k probírání určitě ospravedlňuje delší školení, ale na druhou stranu nezbytnost zajistit povědomí a motivaci, jakož i sdělit jen zapamatovatelné množství základních bodů mě vede k tomu, že je lépe upustit od několikahodinových nebo celodenních školení. Po nich jsou lidé zdeptáni a zahlceni množstvím informací.

Důraz během těchto setkání musí být položen na pochopení škod, které mohou firmu i samotné pracovníky postihnout, pokud nebudou dodržovat odpovídající pokyny týkající se bezpečnosti. Důležitější než samotné nastudování zásad a praktik je motivace pracovníků, která vede k přijetí jejich vlastní odpovědnosti za bezpečnost.

V situacích, kdy někteří pracovníci nemají možnost ihned začít školení, by je měla firma proškolit jinou formou, například pomocí instruktážních filmů, počítačových prezentací, internetového kursu nebo písemných materiálů.

Po první, počáteční etapě Školení, by měla další a delší setkání probírat konkrétní slabiny a metody útoku — v závislosti na postavení školené osoby. Školení osvěžující znalosti by mělo být organizované alespoň jednou ročně. Podstata ohrožení a používané metody podléhají stálým změnám, proto musí být program školení aktualizován. Navíc se ostražitost s časem zmenšuje, a proto musí být školení pravidelně opakováno, aby se povědomí důležitosti dodržování bezpečnostních zásad upevnilo. Musí být také udržována motivace pracovníků k jejich dodržování, například odhalováním specifických hrozeb a metod používaných sociotechniky.

Vedení musí dát svým podřízeným dostatečný čas seznámit se s bezpečnostními praktikami a postupy a také čas na účast v programu bezpečnostních školení. Od zaměstnanců nelze očekávat studium bezpečnostních praktik a účast na kursech mimo pracovní dobu. Novým pracovníkům by se měl dát čas, aby se seznámili s bezpečnostní politikou a postupy dříve, než budou uvedeni do svých normálních pracovních povinností.

Od pracovníků, kteří mění místo v rámci jedné firmy a jejich nová práce je spojená s přístupem k důvěrným údajům nebo počítačovým systémům, by samozřejmě mělo být vyžadováno absolvování školení z bezpečnostních zásad, uzpůsobeného požadavkům nové pozice. Pokud například počítačový operátor povýší na správce systému nebo se recepční stane asistentkou, je vyžadováno nové školení.

> *Poznámka*
> **********
> Žádné školení týkající se bezpečnosti není dokonalé. Proto je potřeba používat zabezpečení technologické, kde je to jen možné, aby se vytvořil neproniknutelný obranný systém. Znamená to, že míra bezpečnosti záleží spíše na technologii než na lidech — například tehdy, když je operační systém zkonfigurovaný tak, aby neumožňoval pracovníkům stahování programů z Internetu nebo znemožňoval volení krátkých, snadno uhodnutelných hesel.
> **********

Obsah školení

Po redukci na jisté základní zásady mají všechny sociotechnické útoky jeden společný prvek: podvod. Oběť je přesvědčena, že útočník je kolega z

práce nebo jiná osoba oprávněná k přístupu k důvěrným informacím, případně někým pověřená vydávat příkazy, které se váží s vykonáváním činností na počítači či podobném zařízení.

Skoro každý takový útok by mohl být zmařen, kdyby pracovník, který je cílem útoku, postupoval podle následujících dvou kroků:

- Ověření totožnosti osoby, která o něco žádá — je osoba tím, za koho se vydává?
- Ověření, zda je osoba oprávněná — skutečně potřebuje tuto informaci nebo je nějak jinak oprávněná k tomu, aby ji získala?

Pokud by školení vedlo ke změně chování pracovníků tak, aby každý z nich důsledně kontroloval každou žádost s příslušnými kritérii, pak by se rizika spojená s útokem sociotechnika radikálně snížila.

Praktický program školení bezpečnosti a informovanosti, který zahraje lidské chování i aspekty sociotechniky, by měl obsahovat následující body:

- Popis, jak útočníci používají sociotechniku, aby obelhávali lidi.
- Metody, které sociotechnici používají, aby dosáhli zamýšleného cíle.
- Způsoby rozpoznávání sociotechnického útoku.
- Procedury postupu v případě podezřelé žádosti.
- Informace o tom, kde se mají hlásit pokusy nebo úspěšné sociotechnické útoky.
- Upozornění na nutnost ověření každé osoby, která na nás směřuje podezřelou žádost, nezávisle na jejím postavení v hierarchii firmy.
- Skutečnost, že by se nemělo implicitně věřit jiným bez odpovídajícího ověření, dokonce i když přirozeným impulsem je presumpce neviny.
- Úloha identifikace totožnosti každé osoby, která žádá o informace nebo vykonání nějaké činnosti (viz „Ověřovací a autorizační procedury" v 16. kapitole — jsou zde popsány způsoby ověření totožnosti).
- Procedury ochrany citlivých informací včetně znalosti existujícího systému klasifikace dat.
- Místo, kde lze nalézt firemní bezpečnostní postupy a jejich úloha v procesu ochrany informací a informačních systémů.
- Shrnutí bezpečnostní politiky a vysvětlení významu jejích jednotlivých aspektů. Například by každý zaměstnanec měl být seznámen s tím, jak si vytvořit heslo, které je těžké uhodnout.
- Povinnost přizpůsobit se pokynům bezpečnostní politiky a důsledky v případě jejich nedodržování.

Sociotechnika už z definice zahrnuje jistý druh interakce mezi lidmi. Útočník bude na cestě k cíli velmi často využívat mnoho komunikačních metod a technologií. Z tohoto důvodu by měl dobře propracovaný program informovanosti o hrozbách obsahovat některá nebo všechna následující témata:

- Bezpečnostní praktiky spojené s hesly umožňujícími přístup k počítači a hlasové poště.
- Postup poskytování důvěrných informací nebo materiálů.
- Způsob používání elektronické pošty, včetně prostředků chránících před nebezpečnými programy: viry, trojskými koňmi atp.
- Fyzické bezpečnostní požadavky jako povinnost nošení identifikátorů (visaček).
- Povinnost zadržování těch osob na půdě firmy, které nemají visačku.
- Zásady spojené s používáním hlasové pošty.
- Klasifikace informací a prostředky jejich ochrany.
- Vhodné způsoby odstraňování důvěrných dokumentů a datových nosičů, které obsahují důvěrné materiály nebo je obsahovaly kdykoli v minulosti.

Pokud firma plánuje penetrační testy, které mají určit účinnost opatření proti sociotechnickým útokům, je dobré na to pracovníky upozornit. Ať vědí, že v rámci takového testu mohou mít telefon nebo dostat e-mail zjišťující jejich reakce. Výsledky testu nemají vést k vyměřování trestů pracovníkům, mají pouze sloužit k určení jistých dodatečných oblastí vyžadujících školení.

Podrobnosti týkající se všech výše zmíněných aspektů lze najít v 16. kapitole.

Testování

Firma může chtít zkontrolovat, nakolik pracovníci ovládli informace prezentované na školení, než je pustí k počítači. Pokud vytváříme testy s úmyslem umístit je na síti, můžeme využít některý z programů, které pomáhají takové testy vytvářet a analyzují výsledky, které nám pomohou určit oblasti vyžadující dodatečnou pozornost.

Firma může přiznávat zvláštní certifikát potvrzující absolvování školení z oblasti bezpečnosti, který plní funkci odměny a motivace.

Jako rutinní prvek školení se doporučuje požádat účastníky o podpis prohlášení, že se budou řídit bezpečnostní politikou a budou dodržovat zásady sdělené jim na školení. Výzkumy dokazují, že osoba, která takový svazek podepisuje, vynakládá větší úsilí, aby se těmto zásadám přizpůsobila.

Udržování povědomí

Většina z nás si uvědomuje, že má sklon zapomínat i důležité věci, pokud znalosti čas od času neosvěžujeme. Je tedy nutný program udržování povědomí o problematice.

Jednou z metod nastavení vysoké priority bezpečnosti je, že učiníme každou osobu nějakým způsobem odpovědnou za bezpečnost informací. To vede k uvědomění si svého významu v udržování bezpečnosti firmy. Jinak existuje silná tendence si myslet, že bezpečnost „nepatří k mým povinnostem".

Zatímco je odpovědnost za zajištění bezpečnosti informací obvykle připsána osobě z oboru bezpečnosti nebo informatiky, program informovanosti o záležitostech spojených s bezpečností informací by měl být realizovaný s oddělením, které má na starosti školení.

Program stálého udržování znalostí musí využívat všechny možnosti komunikace o bezpečnostních záležitostech, aby byl sdělovaný obsah snadno zapamatovatelný a v pracovnících byly zformovány správné návyky. Podobně jako v reklamě zde mohou pomoci humor a důvtip. Formulujme ty samé body pokaždé jiným způsobem, abychom se se vyhnuli hrozbě, že budou časem přehlíženy.

Seznam možností v oblasti udržování povědomí může obsahovat tyto body:

- Opatřit všem zaměstnancům exemplář této knížky.
- Obsadit informační položky ve vnitřních zpravodajích: články, rámečky (raději kratší a poutající pozornost) nebo například i komiksy.
- Zveřejněnit fotografii Mistra bezpečnosti za daný měsíc.
- Vyvěšovat na pracovištích plakáty.
- Posílat poznámky do vnitřních diskusních skupin.
- Přikládat letáčky do obálek obsahujících například prémie.
- Zasílat připomínající e-maily.
- Používat šetřiče obrazovek s tématikou bezpečnosti.
- Zanechávat zprávy v hlasových schránkách zaměstnanců.
- Vytisknout samolepky na telefony s nápisy typu: „Je volající opravdu tím, za koho se vydává?"

- Zavést připomínající hlášky, které se při přihlašování objevují na počítači, například: „Pokud posíláš důvěrné informace e-mailem, šifruj je!"
- Zohlednit povědomí o bezpečnosti jako jeden z kroků při vytváření hodnocení pracovníka.
- Umístit prvky připomínající zásady bezpečnosti na internetu, například pomocí komiksů, vtipných obrázků nebo jinými poutavými způsoby.
- Používat světelné panely například v jídelně či závodní kantýně, které by často měnily body týkající se bezpečnosti.
- Distribuovat brožury.
- Jiné nápadité finty, například sušenky štěstí, které by místo věštby obsahovaly některou z bezpečnostních zásad.

Ohrožení je neustálé, proto je třeba ho stále připomínat.

A co z toho budu mít já?

Kromě školení silné doporučují i dobře propracovaný systém odměn. Je třeba vyjadřovat uznání pracovníkům, kteří odhalili sociotechnický útok a zabránili mu nebo se nějak jinak zasloužili o úspěch informačního bezpečnostního programu. Existence systému odměn by měla být oznamována pracovníkům na všech akcích týkajících se bezpečnosti a všechny případy porušení bezpečnostních zásad by měly být v organizaci široce publikovány.

Existuje ale také druhá strana mince. Lidé si musejí být vědomi důsledků, když se nebudou přizpůsobovat bezpečnostním postupům ať už z bezstarostnosti, nebo ze vzdoru. Všichni děláme chyby, ale opakující se případy porušování bezpečnostních pravidel nemohou být tolerovány.

16

Doporučená politika bezpečnosti informací

Devět z deseti velkých korporací a vládních úřadu bylo napadeno počítačovými vetřelci — to je závěr výzkumu provedeného FBI a zveřejněného agenturou Associated Press v dubnu 2002. Zajímavý je také fakt, že pouze jedna organizace ze tří nějaké útoky hlásila nebo je veřejně potvrdila. Zdrženlivost ve zveřejňování informací tohoto typu má své důvody. Aby se předešlo ztrátě důvěry ze strany klientů i dalším útokům ze strany útočníků, kteří by se dozvěděli o slabých místech firmy, většina organizací raději incidenty tohoto typu nezveřejňuje.

Zdá se tedy, že neexistují statistiky týkající se sociotechnických útoků, ale i kdyby existovaly, nebyly by směrodatné. Ve většině případů se totiž firma nikdy nedozví, že byla okradena o informace, proto většina útoků zůstává nepostřehnuta a není nikomu hlášena.

Proti většině typů sociotechnických útoků lze přijmout preventivní opatření. Podívejme se však pravdě do očí — dokud všichni lidé z organizace nepochopí důležitost zabezpečení a respektování pravidel se nestane jejich osobní záležitostí, tak budou firmu sociotechnické útoky stále ohrožovat.

Ve skutečnosti bude díky dostupnosti stále účinnějších technologických bezpečnostních prostředků sociotechnický přístup — využívání lidí k získávání střežených informací nebo k nabourávání se do firemních sítí — stále častěji používán a stane se pro zloděje informací lákavější pracovní metodou. Průmyslový špión bude samozřejmě chtít dosáhnout svého cíle tou nejsnazší a nejméně riskantní metodou. V zásadě může být proto firma, která své počítačové systémy a síť zabezpečila nejnovějšími a nejpropracovanějšími technologiemi, tím spíš vystavena nebezpečí útoků ze strany útočníků, kteří používají k dosažení svých cílů sociotechnických metod, strategií a taktik.

Tato kapitola představuje doporučované praktiky a postupy vytvořené proto, aby se minimalizovalo riziko spojené se sociotechnikou. Jsou namířené proti útokům, které se neopírají pouze o využívání technologických děr, ale týkají se pokusů o podvádění pracovníků a manipulování s nimi, aby od nich byly získány informace nebo aby byly jimi samými vykonány činnosti, které umožní vetřelci přístup k citlivým datům firmy nebo do firemní počítačové sítě.

Co je bezpečnostní politika?

Bezpečnostní politika se skládá z jasných instrukcí, které popisují směrnice týkající se chování pracovníků za účelem ochrany informací. Jsou základním stavebním materiálem, ze kterého se skládá systém ochrany před potenciálními ohroženími. Nejdůležitějším úkolem těchto instrukcí je však pomoc při odhalování sociotechnických útoků a zajištění ochrany před nimi.

Efektivní ochranná opatření jsou zaváděna pomocí školení pracovníků na základě dobře vypracovaných instrukcí a postupů. Nicméně je třeba mít na paměti, že všechna doporučení, dokonce i když jsou nejúzkostlivěji dodržována všemi pracovníky, nezaručují stoprocentní ochranu před všemi sociotechnickými útoky. Reálným cílem by mělo být snížení rizika útoku na přijatelnou úroveň.

Uvedené instrukce popisují rovněž opatření, která nesouvisejí těsně se sociotechnikou. Přesto sem byla zařazena, protože mají nějakou souvislost s technikami používanými během útoků. Příkladem mohou být instrukce týkající se otevírám příloh v poště, které mohou obsahovat trojské koně umožňující

útočníkovi převzetí kontroly nad počítačem oběti. Jak je vidět, jsou spojené s jednou z metod často používaných počítačovými vetřelci.

Etapy vytváření programu

Komplexní program ochrany informací obvykle začíná odhadem rizika, který má za cíl určit:

- Jaké firemní informace musejí podléhat ochraně?
- Jaká konkrétní ohrožení těchto agend existují?
- Jakou škodu by způsobilo uskutečnění potenciálních útoků?

Hlavním cílem odhadu rizika je zjištění, které z agend vyžadují okamžité zabezpečení, a jestli budou použitá bezpečnostní opatření po zohlednění analýzy zisků a ztrát rentabilní. Zkrátka: které agendy je třeba zabezpečit nejdříve a kolik to bude stát?

Velmi důležité je, aby vyšší vedení silně podporovalo nutnost vytvoření bezpečnostní politiky a programu ochrany informací. Podobně jako v případě každého celozávodníno programu, je předpokladem úspěchu takového programu nejen podpora vedení, ale také demonstrace jeho angažovanosti a příklad samotného vedení. Pracovníci si musejí být vědomi, že vědení vykazuje silnou víru, že bezpečnost informací je pro fungování firmy nezbytná, že ochrana obchodních informací je nutná pro udržení pozice na trhu a že úspěch programu závisí na individuálním postoji každého zaměstnance.

Člověk, který má za úkol sepsat bezpečnostní postupy a pokyny, si musí uvědomovat, že se v takových dokumentech musí vyhýbat technické hantýrce, aby byly pro pracovníky neseznámené s technikou srozumitelné. Je důležité, aby tam bylo vysvětleno, proč je každé doporučení významné, jinak mohou pracovníci některé pokyny odmítnout jako zbytečnou ztrátu času. Pisatel by měl vytvořit jeden dokument, který představuje firemní politiku s rozdělením na jednotlivé body, a druhý, který obsahuje podrobné postupy. První, obecný dokument se pravděpodobně nebude tak často měnit, jako dokument obsahující postupy.

Navíc by si měl tvůrce těchto dokumentů být vědom technologických možností, které lze při posilování bezpečnosti využít. Například většina operačních systémů může od uživatelů vyžadovat, aby jejich heslo splňovalo některé požadavky (například délku). V některých firmách může být zákaz stahování programů zajištěn odpovídajícím globálním i lokálním nastavením v systému. Politika firmy by měla vyžadovat využívání technologií, kdekoliv se to finančně vyplatí, aby se eliminoval lidský faktor.

Pracovníci musejí být informováni o důsledcích nedodržování pokynů a postupů. Měl by se vytvořit systém trestů za porušování instrukcí a rozdistribuovat jej. Kromě toho lze vytvořit systém odměn pro pracovníky, kteří dávají při dodržování bezpečnostních zásad dobrý příklad, a pro zaměstnance, kteří rozpoznali a ohlásili napadení. Každé ocenění pracovníka za zmařený útok by mělo být široce rozhlášeno, například V článku ve vnitřním firemním zpravodaji.

Jedním z cílů informačního programu je diskuse o ohromné váze přikládané bezpečnostním pokynům a o škodách, které mohou nastat, nebudeme-li podle nich postupovat. Lidská přirozenost časem způsobí, že pracovníci budou chtít ignorovat nebo obcházet doporučení, která se zdají být nepodstatná nebo příliš časově náročná. Úlohou vedení je uhlídat, aby pracovníci podstatu těchto doporučení chápali a byli motivováni k jejich dodržování namísto toho, aby je považovali za překážky.

Podrobnosti politiky bezpečnosti nelze vytesat do kamene. Jak se mění firmy i trh, jak se objevují nové bezpečnostní technologie a jak se vyvíjí ohrožení, je vhodné měnit i bezpečnostní politiku. Musí existovat proces pravidelné revize a aktualizace obsahu.

Pokyny a postupy by měly být přístupné na Internetu nebo uložené v obecně přístupném adresáři. To zvyšuje pravděpodobnost jejich častější revíze a zároveň dává pohodlnou metodu hledání odpovědí na ty otázky spojené s bezpečností, které pracovníky trápí nejvíce.

Je dobré provádět také pravidelné penetrační testy a odhady slabin za použití sociotechnických metod a taktik, aby se odhalily všechny slabé stránky v procesu školení nebo tendence k nedodržování jistých pokynů. Před testem je třeba pracovníky informovat, že něco takového může kdykoliv nastat.

Jak používat instrukce

Podrobné instrukce obsažené v této kapitole reprezentují pouze část sestavy nezbytné ke snižování rizika spojeného se všemi typy ohrožení. Proto by zde uvedené instrukce neměly být pokládány za vyčerpávající seznam pokynů. Znamenají spíše základ k vybudování komplexní sbírky pokynů a postupů odpovídající specifickým potřebám naší firmy.

Autoři instrukcí v dané firmě by měli vybrat ty, které jsou v souladu se specifikacemi podniku a jeho cíli. Každá organizace má jiné nároky týkající se otázek bezpečnosti v závislosti na svých potřebách, právních požadavcích, kultuře a používaných informačních systémech; část ze zde uvedených pokynů si přizpůsobí a zbytek pomine.

Je užitečné se také zamyslet, jak přísné mají být pokyny v každé z kategorií. Menší firmy sídlící v jedné budově, kde se všichni znají, si nemusejí dělat příliš starostí s tím, že útočník zavolá a prohlásí se za kolegu z téže firmy (ačkoliv stejně tak se může podvodník vydávat za dodavatele). Kromě toho, nezávisle na existujících hrozbách, může organizace o dost volné a svobodné struktuře chtít přijmout pouze omezenou sadu pokynů, které jí postačí, aby své cíle v oblasti bezpečnosti zajistila.

Klasifikace dat

Politika klasifikace dat představuje základ ochrany firemních informací a určuje kategorie, které řídí způsob poskytování důvěrných informací. Je páteří systému ochrany firemních dat a ukazuje pracovníkům stupeň citlivosti každé informace.

Činnost bez předchozí klasifikace dat — což je dnes stav takřka ve všech společnostech — ponechává většinu rozhodnutí na jednotlivých pracovnících. Jejich rozhodnutí jsou přirozeně založená ve větší míře na subjektivních faktorech než na stupni důvěry, váhy a hodnoty informací. Informace tečou z firem rovněž proto, že si pracovníci neuvědomují, že osoba, která je o informace žádá, může být útočníkem.

Politika klasifikace dat určuje pravidla klasifikace cenných dat na několik úrovní. Po přiřazení každé informace do nějaké kategorie může pracovník postupovat podle pokynů ke zpřístupňování informací, které chrání firmu před neúmyslným a lehkovážným prozrazením důvěrných dat. Tyto procedury omezují možnost podvedení pracovníka osobou, která není oprávněná informaci získat.

Každý pracovník se musí na školení seznámit s politikou klasifikace dat; týká se to také osob, které obvykle nepoužívají počítače nebo firemní komunikační prostředky. Protože každý člen organizace, včetně uklízeček, ochranky, pracovníků u kopírek, jakož i konzultantů, externích pracovníků na dohodu a dokonce i praktikantů, může mít přístup k citlivým informacím a stát se tak terčem útoku.

Vedení musí vyznačit *vlastníky informací* odpovědné za všechny možné informace, které firma používá. Vlastník informace je zodpovědný kromě jiného za ochranu dat. Obvykle právě on rozhoduje, na kterou úroveň je třeba

informaci zařadit v závislosti na stupni potřebné ochrany; občas znovu hodnotí kategorii důvěrnosti a rozhodne, jestli je potřebná změna. Vlastník může rovněž delegovat svou odpovědnost za ochranu dat určeným osobám.

Kategorie klasifikace a jejich definice

Informace by měly být roztříděné na různé úrovně v závislosti na stupni jejich citlivosti. Po sestavení určitého systému klasifikace je proces opětovné klasifikace na nové kategorie nákladný a časově náročný. V našem příkladu byly vytvořeny čtyři úrovně, což je odpovídající řešení pro většinu středních a velkých podniků. V závislosti na počtu a typech důvěrných informací může firma přidat další kategorie, aby mohla s různými typy informací zacházet podrobněji. V menších firmách by měla stačit klasifikace třístupňová. Je třeba mít na paměti, že čím složitější je klasifikace, tím nákladnější bude školení pracovníků a dodržování pokynu.

Tajné. Tato kategorie zahrnuje nejdůvěrnější informace. Tajná informace je určena pouze k vnitřní potřebě firmy. Ve většině případů je dobré ji zpřístupňovat jen velmi omezenému počtu osob, které ji nezbytně potřebují. Povaha tajné informace je taková, že její prozrazení nepovolané osobě může mít vážné důsledky pro firmu, její akcionáře, partnery či klienty. Tajná informace obvykle patří do jedné z následujících tří kategorií:

- Informace o obchodních tajemstvích, proprietární zdrojový kód, technické nebo funkční specifikace, které by mohl využít konkurent.
- Marketingová nebo finanční informace, která není určená veřejnosti.
- Jakákoliv jiná informace, která má pro činnost firmy zásadní význam.

Soukromé. Tato kategorie zahrnuje informace osobní povahy, které jsou určené pro vnitřní potřebu v organizaci. Každé neoprávněné zpřístupnění soukromé informace může mít velký vliv na pracovníka nebo na firmu, pokud byla informace získána neoprávněnou osobou (zejména pak sociotechnikem). Do soukromých informací patří výsledky lékařských prohlídek pracovníků, informace o bankovním kontě, historie výplat a všechny další osobní identifikační údaje, které nejsou určené veřejnosti.

> *Poznámka*
> **********
> Kategorie vnitřních informací bývá také často označována jako „důvěrná" nebo „citlivá". Zvolil jsem však termín „vnitřní", protože vysvětluje, komu jsou tyto informace určené. Termín „důvěrné" je tu používán jako pohodlný způsob odkazující se na informace tajné, soukromé i vnitřní. Jinými slovy, důvěrné jsou všechny informace, které nejsou označeny jako veřejné.
> **********

Vnitřní. Tato kategorie označuje informace, které se smějí zpřístupnit každému zaměstnanci firmy. Zpřístupnění vnitřní informace neoprávněné osobě nemůže způsobit větší škodu firmě, podílníkům, obchodním partnerům, zákazníkům ani pracovníkům. Nicméně zkušený sociotechnik může tuto informaci využít, aby se vydával za oprávněného pracovníka či dodavatele a oklamal nějakého pracovníka, ze kterého vymámí informace o větším stupni důvěry, které mu nakonec mohou umožnit například přístup k firemní počítačové síti.

Před zpřístupněním vnitřní informace třetím osobám, jako jsou představitelé dodavatelů, brigádníci či partnerské firmy, je třeba s nimi podepsat příslušnou smlouvu o důvěrnosti těchto údajů. Vnitřní informace jsou všechny informace, které jsou běžně používané při činnosti a neměly by být známy navenek, například organizační struktura, přístupová telefonní čísla do

počítačové sítě, názvy vnitřních systémů, procedury vzdáleného přístupu, účetní kódy atp.

Veřejné. Informace, které jsou určené veřejnosti. Mohou být libovolně šířené. Jsou to například tisková prohlášení, kontaktní informace pro zákazníky a katalogy výrobků. Je třeba si zapamatovat, že každá informace, která není jednoznačně určená pro veřejnost, by měla být považována za důvěrnou.

Terminologie svázaná s klasifikací dat

Patřičně klasifikovaná data by měla být předávána odpovídajícím kategoriím pracovníků. Část pokynů v této kapitole popisuje poskytování informací *neověřené osobě*. Pro účely těchto instrukcí termín neověřená osoba znamená někoho, koho pracovník nezná osobně jako aktivního pracovníka nebo jako člověka oprávněného obdržet důvěrnou informaci, o kterou žádá.

Důvěryhodná osoba tu označuje osobu, se kterou měl pracovník příležitost se bezprostředně setkat a u které má jistotu, že je zaměstnancem firmy, klientem nebo konzultantem na takové pozici, která mu dovoluje přístup k dané informaci. Důvěryhodná osoba může být rovněž pracovníkem firmy, která má s naší firmou trvalé svazky (například zákazník, dodavatel nebo strategický partner, který podepsal smlouvu o mlčenlivosti).

Zaručení třetí osobou znamená situaci, kdy důvěryhodná osoba ověřuje status nebo skutečnost, že je zde osoba zaměstnána a její právo na žádost o informace nebo o výkon nějaké činnosti. Je třeba mít na paměti, že v některých případech instrukce přikazují dodatečnou verifikaci, jestli důvěryhodná osoba je stále pracovníkem podniku, než se tazateli informace sdělí.

Privilegované konto je účet v počítačovém či jiném systému s přístupovými právy administrátora systému. Pracovníci s privilegovaným kontem mají obvykle možnost modifikace opravném jiných uživatelů a vykonávání činností spojených se správou systému.

Všeobecná hlasová schránka útvaru je hlasová schránka, kde je nahráno obecné uvítací sdělení určitého oddělení. Nahrávka tohoto typu chrání jména a vnitřní linky osob pracujících v daném oddělení.

Ověřovací a autorizační procedury

Aby zloději informací získali přístup k tajným informacím, užívají převážné lsti – vydávají se za pracovníky firmy, subdodavatele, dodavatele nebo obchodní partnery. Aby se zajistila efektivní ochrana informací, musí pracovník žádaný o vykonání nějaké činnosti nebo o sdělení důvěrné informace provést pozitivní identifikaci volající osoby a ověřit, jestli má oprávnění, dříve než žádosti vyhoví.

Doporučené postupy popsané v této kapitole jsou vytvořeny proto, aby pomohly pracovníkovi, který dostává žádost kterýmkoliv z komunikačních kanálu jako telefon, e-mail nebo fax, při kontrole, jestli je žádost odůvodněná.

Žádost důvěryhodné osoby

Žádost důvěryhodné osoby může vyžadovat:

- Ověření, jestli je osoba v současnosti zaměstnancem nebo má nějaké vazby, které by ji opravňovaly k přístupu k údajům, o které žádá. Díky tomu se vyhýbáme situaci, kdy se bývalí pracovníci, dodavatelé a podobně vydávají za aktuálně oprávněné.

- Ověření, jestli daná osoba tuto informaci opravdu potřebuje a zda je oprávněna k přístupu k ní.

Žádost neověřené osoby

Když žádost pochází od osoby neověřené, je třeba uplatnit proces verifikace, aby byla žádající osoba jednoznačně identifikována jako oprávněná obdržet danou informaci, zejména pokud se žádost týká počítače nebo podobného zařízení. Tento proces je základním zabezpečením před sociotechnickými útoky: pokud budou pracovníci postupovat podle ověřovacích procedur, radikálně se sníží účinnost sociotechnických útoků.

Je důležité, aby tento proces nebyl příliš složitý, nerentabilní nebo aby ho pracovníci neignorovali.

Proces ověřování se skládá z následujících kroků:

- Ověření, jestli je osoba tím, za koho se vydává.
- Kontrola, jestli je tazatel ve firmě v současnosti zaměstnán nebo k ní má nějaký vztah, který by vysvětloval potřebu získat informaci.
- Zjištění, jestli má daná osoba oprávněni, aby danou informaci obdržela nebo aby pro ni byla vykonána určitá činnost.

Krok první: ověření totožnosti

Doporučené kroky při verifikaci jsou níže vyjmenovány v pořadí podle efektivnosti. Čím vyšší číslo, tím účinnější metoda. U každé metody jsou uvedeny její slabiny a způsob, jak je může sociotechnik obejít.

1. **Identifikace volajícího** (za předpokladu, že telefonní systém firmy má tuto možnost). Ujisti se pohledem na displej, jestli je telefonát z firmy, nebo zvenku a jestli číslo odpovídá jménu, které volající uvedl.
   Slabina: Vnější identifikátor může být zfalšovaný člověkem, který má přístup k pobočkové ústředně nebo k ústředně telekomunikační firmy napojené na digitální síť.
2. **Zpětné volání**. Vyhledej si volajícího v telefonním seznamu a zavolej mu zpátky, aby ses ujistil, jestli je pracovníkem firmy.
   Slabina: Útočník s příslušnými znalostmi může přesměrovat hovor z dané vnitřní linky. Pak volání na vnitřní linku způsobí přesměrování hovoru na vnější číslo útočníka.
3. **Záruka**. Volajícího ověřuje důvěryhodná osoba, která ručí za žadatelovu identitu.
   Slabina: Útočníci jsou často schopni přesvědčit jednoho zaměstnance o své totožnosti a zařídit, aby se za ně u jiného pracovníka zaručil.
4. **Společné tajemství**. Použití vnitřního společného firemního tajemství, například hesla nebo denního kódu.
   Slabina: Pokud společné tajemství zná mnoho lidí, může být jeho zjištění pro sociotechnika velmi snadné.
5. **Vedoucí či nadřízený volajícího**. Telefonát bezprostředně nadřízenému volajícího s žádostí o ověření.
   Slabina: Pokud volající číslo svého šéfa uvedl sám, pak osoba, které se dovoláme, nemusí být ve skutečnosti jeho šéfem, ale společníkem.
6. **Bezpečný e-mail**. Vyžaduje se elektronický dopis s elektronickým podpisem.
   Slabina: Pokud se už útočník dokázal nabourat do počítačového systému a nainstalovat program monitorující stisknutí klávesy, aby takto

získal pracovníkovo heslo, může sám poslat elektronicky podepsaný e-mail, který bude vypadat, jako by pocházel od pracovníka firmy.

7. **Identifikace hlasu**. Osoba, ke které je směřována žádost, již měla co do činění s volajícím (nejlépe osobně) a tak ví, že osoba je důvěryhodná a zná ji natolik dobře, aby rozeznala její hlas v telefonu.
   Slabina: Je to dost bezpečná metoda, která se nedá snadno obejít. Nelze ji však použít v situaci, kdy se člověk přijímající telefon nikdy s volajícím nesetkal ani s ním nemluvil.
8. **Dynamická hesla**. Žadatel se identifikuje pomocí technologie dynamického hesla (jako je například Secure ID).
   Slabina: Aby útočník toto zabezpečení obešel, musí se dostat k jednomu z identifikačních zařízení a k jemu přiřazenému PIN kódu vlastníka nebo zmanipulovat pracovníka tak, aby mu přečetl kód ze zařízení a sdělil své PIN.
9. **Osoba s identifikátorem**. Osoba, která k nám vznáší žádost, se objevuje osobně a ukazuje nám identifikátor zaměstnance nebo dokument podobného druhu, nejlépe s fotografií.
   Slabina: Útočníci jsou schopni ukrást identifikátor pracovníka nebo si vytvořit falešný identifikátor, který vypadá přesvědčivě. Útočníci se ale takovým metodám vyhýbají, protože osobní přítomnost na firemní půdě je spojena s rizikem odhalení a zadržení.

Krok druhý: ověření statutu pracovníka

Největší ohrožení bezpečnosti informací nepochází ze strany profesionálního sociotechnika nebo počítačového hackera, ale od někoho mnohem bližšího: právě propuštěného pracovníka, který hledá pomstu nebo doufá, že pro sebe využije informace ukradené z firmy. (Verze této procedury může posloužit také k ověření, jestli je daná osoba nadále v nějakém vztahu s firmou, například je dodavatelem, konzultantem nebo pracovníkem na dohodu.)

Před poskytnutím důvěryhodné informace jiné osobě nebo před souhlasem s vykonáním nějaké činnosti na počítači či podobném zařízení je třeba pomocí níže uvedených metod ověřit, zda žadatel je nadále zaměstnancem firmy:

Kontrola seznamu pracovníků. Pokud firma zpřístupňuje ve vnitřní síti seznam pracovníků, který přesně odráží skutečný stav, je třeba ověřit, zda je volající na tomto seznamu.

Ověření u nadřízeného. Je třeba zavolat nadřízenému volajícího na číslo uvedené ve vnitřním telefonním seznamu, nikoli na číslo, které uvedl sám žadatel.

Ověření na oddělení. Je třeba zavolat na oddělení, ve kterém pracuje volající, a zeptat se nějaké osoby, která tam pracuje, jestli je žadatel v současnosti v oddělení zaměstnán.

Krok třetí: ověření oprávnění k informaci

Kromě ověření, jestli je osoba, která se na nás obrací s žádostí, stále zaměstnána ve firmě nebo k ní má nějaké vztahy, zůstává ještě otázka, jestli je tato osoba oprávněná získat informace, o které žádá, nebo jestli je oprávněná vykonávat činnosti (na počítači či podobném zařízení), o které žádá nás.

Kontrolu lze provést jednou z následujících metod:

- **Ověř seznam funkcí, pracovních skupin, pracovišť.** Firma může zajistit přístup k autorizačním informacím tím, že publikuje seznam popisující oprávnění jednotlivých pracovníků k různým informacím. Tyto seznamy mohou být setříděné podle funkcí, oddělení, pracovních skupin nebo jejich kombinace. Tyto seznamy by měly být zpřístupněné ve vnitřní síti, což umožní jejich okamžitou aktualizaci a usnadní přístup. Obvykle jsou vlastníci informací odpovědní za vytvoření a udržování seznamu pro přístup k informacím, nacházejícím se pod jejich kontrolou.

Poznámka
****
Udržování takového seznamu může být ale také pozvánkou pro sociotechnika. Pokud se útočník doví, že takový seznam existuje, bude se usilovně snažit se k němu dostat. Se seznamem v ruce si může otevřít hodně dveří a vystavit firmu vážnému nebezpečí.
****

- **Získej oprávnění od nadřízeného.** Pracovník se kontaktuje se svým nadřízeným nebo nadřízeným žadatele, aby získal autorizaci dané žádosti.
- **Získej autorizaci od vlastníka informací nebo od jím pověřené osoby.** Vlastník informace je konečná autorita v otázce, jestli má daná osoba nárok na informaci, kterou spravuje. V případě žádosti spojené s přístupem k počítači se musí pracovník spojit s bezprostředním nadřízeným volajícího, aby žádost o přístup schválil na základě existujících profilů pracovišť. Pokud takové profily neexistují, je povinností nadřízeného spojit se s vlastníkem informací, aby od něho získal souhlas. Je dobré se držet tohoto řetězu doporučení, aby vlastník informací nebyl příliš zatížen otázkami v situacích, kdy existuje častá potřeba verifikace.
- **Získej autorizaci pomocí odpovídajícího softwaru.** Pro velkou firmu působící v oboru, kde je silná konkurence, může být účelné vytvoření softwarového balíku, který umožní autorizaci. Taková databáze obsahuje seznam pracovníků zároveň s jejich právy k chráněným informacím. Uživatelé databáze nebudou mít možnost prohlížet si oprávnění jednotlivých osob, ale budou moci zadat jméno osoby a identifikaci informace, o kterou žádá. Databáze pak sdělí odpověď, jestli je daná osoba oprávněná informaci získat. Díky tomuto řešení se vyhneme nutnosti vytváření otevřeného seznamu pracovníků s jejich oprávněními, který by mohl být ukraden.

Pokyny pro vedení

Následující pokyny se vztahují na pracovníky na vedoucích pozicích. Byly rozčleněny na otázky klasifikace dat, prozrazování informací, telefonní správu a ostatní. Jak je vidět, každá kategorie pokynů používá vlastní strukturu číslování, což usnadňuje identifikaci jednotlivých instrukcí.

1. Zásady klasifikace dat

Klasifikace dat je způsob rozdělení chráněných informací ve firmě a přístupových práv k nim.

1.1 Roztřiď informace do kategorií

Pokyn: Všechny cenné, důvěrné nebo pro činnost firmy kritické informace musejí být vlastníkem informací nebo určenou osobou roztříděny do konrétních kategorií.

Poznámky: Vlastník informací nebo oprávněná osoba přiřazují do odpovídající kategorie každou informaci, která je běžně při činnosti firmy používána. Vlastník též určuje, kdo má k těmto informacím přístup a jak je lze využívat. Vlastník informací může změnit začlenění nebo určit čas, po kterém už klasifikace přestane platit.

Každá neoznačená informace by měla být pokládána za důvěrnou.

1.2 Publikuj procedury zpřístupňování informací

Pokyn: Firma musí vytvořit postupy řídící zpřístupňování informací v rámci každé kategorie.

Poznámky: Po vytvoření klasifikace je třeba vytvořit postupy zpřístupňování informací pracovníkům i osobám zvenku podle popisu uvedenho v bodě „Ověřovací a autorizační procedury" dříve v této kapitole.

1.3 Označ všechny možné nosiče

Pokyn: všechny tištěné materiály, jakož i počítačová média obsahující důvěrné informace, by měly být zřetelně označené názvem kategorie důvěrnosti, ke které náleží.

Poznámky: Tištěné materiály musejí mít titulní list s výrazným označením stupně důvěrnosti. Toto označení by se mělo rovněž nacházet na viditelném místě na každé straně dokumentu, aby bylo možné ho přečíst, když je dokument otevřený.

Soubory v počítači, které se nedají snadno popsat (databázové soubory nebo binární soubory) je třeba chránit přístupovými právy, aby bylo zajištěno, že informace tohoto typu nebude nesprávně zpřístupněna, a při té příležitosti je zabezpečit před změnou, zničením atp.

Všechna počítačová média jako diskety, pásky, CD-ROM musejí být označené kategorií, která je přiřazena té nejdůvěrnější informaci na nich obsažené.

2. Zpřístupňování informací

Zpřístupňování informací spočívá v jejich předávání osobám na základě Jejich totožnosti a oprávnění.

2.1 Procedura ověřování pracovníků

Pokyn: firma by měla vytvořit přesné postupy určené pracovníkům k ověřování totožností, zaměstnaneckého stavu a oprávnění osoby před zpřístupněním důvěrné informace nebo vykonáním činnosti na počítači.

Poznámky: tam, kde je to odůvodněné velikostí firmy a jejími potřebami v oblasti bezpečnosti, by se měly používat pokročilé bezpečnostní technologie. Nejlepším řešením je použít k ověřování osob osobních zařízení ve spojení se společným tajemstvím firmy. Toto řešení určitě dovolí zmenšit riziko, ale může být pro některé společnosti příliš nákladné. V takovém případě by firma měla používat společné tajemství, jako je každodenně měněné heslo nebo kód.

2.2 Sdělování informací třetím osobám

Pokyn: Je třeba vytvořit soupis procedur zpřístupňování informací a proškolit personál v jeho používání.

Poznámky: Zvláštní postupy distribuce informací musejí být vytvořeny pro:

- Zpřístupňování informací v rámci firmy.
- Zpřístupňování informací osobám a pracovníkům s pracovním vztahem k firmě jako například konzultanti, dočasní pracovníci, zaměstnanci dodavatelů, servisních firem nebo strategických partnerů a podobně.
- Zpřístupňování informací okolnímu světu.
- Zpřístupňování informací z každé úrovně klasifikace v případech: poskytování informace osobně, telefonicky nebo e-mailem, faxem, tradiční poštou, kurýrní zásilkou nebo pomocí elektronického přenosu.

2.3 Distribuce tajných informací

Pokyn: Tajné informace, které mohou v nepovolaných rukou způsobit firmě vážnou škodu, mohou být předávány pouze důvěryhodným a oprávněným osobám.

Poznámky: Tajná informace ve fyzické formě (tzn. výtisk, přenosné médium) může být předávaná:

- osobně;
- vnitřní poštou po zapečetění a označení jako „tajné";
- mimo firmu pomocí důvěryhodné kurýrní služby a proti podpisu příjemce nebo pomocí poštovní služby používající registrované zásilky (například, doporučené).

Tajné informace v elektronické formě (soubory, databáze, e-maily) mohou být předávány:

- jako zašifrovaný obsah e-mailové zprávy;
- v příloze e-mailu jako zašifrovaný soubor;
- elektronickým přenosem na server v rámci vnitřní firemní sítě;
- prostřednictvím programu posílajícího faxy z počítače, pokud je příjemce jediná osoba, která používá fax, na nějž je informace posílána. Alternativně lze faxy posílat, aniž by byl na druhé straně přítomný příjemce, pokud je použito šifrované telefonní spojení a informace je vyslána na faxový server, který je zabezpečený heslem.

Tajné informace mohou být předávány osobně, telefonicky uvnitř firmy, vnějším telefonem (pokud je rozhovor šifrovaný), šifrovaným satelitním spojením, šifrovanou videokonferencí či pomocí šifrovaného přenosu hlasu přes Internet (VoIP).

Při faxových přenosech doporučovaná metoda vyžaduje nejprve poslat titulní stránku. Příjemce po jejím přijetí vysílá odpověd potvrzující jeho přítomnost u přístroje. Teprve potom odesilatel posílá zbytek.

Následující prostředky nejsou pro distribuci tajných dat přijatelné: nešifrovaný e-mail, zpráva zanechaná v hlasové schránce, obyčejná pošta a jakákoliv forma bezdrátové komunikace (mobily, SMS atp.).

2.4 Distribuce soukromých informací

Pokyn: Privátní informace neboli osobní údaje týkající se zaměstnance či zaměstnanců by mohly být v případě vyzrazení využity ke způsobení škody firmě nebo pracovníkům. Lze je poskytnout pouze důvěryhodné osobě, která má oprávnění taková data dostávat.

Poznámky. Soukromé informace ve fyzické formě (výtisk nebo přenosné počítačové médium) mohou být předávány:

- osobně;
- vnitřní poštou po zapečetění a označení jako „soukromé";
- obyčejnou poštou.

Soukromé informace v elektronické formě (soubory, databáze, e-maily) mohou být předávány:

- vnitřní elektronickou poštou;
- elektronickým přenosem na server v rámci vnitřní firemní sítě;
- faxem, pokud je příjemce jediná osoba, která používá fax, na nějž je informace posílána, nebo čeká při konkrétním přístroji. Faxy lze také posílat, aniž by byl na druhé straně přítomný příjemce, pokud je použito šifrované telefonní spojení a informace je vyslána na faxový server, který je zabezpečený heslem.

Soukromé informace mohou být předávány osobně, telefonicky uvnitř firmy, vnějším telefonem (pokud je rozhovor šifrovaný), šifrovaným satelitním spojením, šifrovanou videokonferencí či pomocí šifrovaného přenosu hlasu přes Internet (VoIP).

Následující prostředky nejsou pro distribuci soukromých dat přijatelné: nešifrovaný e-mail, zpráva zanechaná v hlasové schránce a jakákoliv forma bezdrátové komunikace (mobily, SMS atp.).

2.5 Distribuce vnitřních informací

Pokyn: Vnitřní informace je informace určená pouze pro vnitřní potřebu v rámci firmy. Lze ji poskytnout i těm osobám mimo firmu, které podepsaly odpovídající dokument o důvěrnosti dat. Je třeba stanovit odpovídající směrnice popisující distribuci vnitřních informaci.

Poznámky: Vnitřní informace může být předávána jakoukoliv formou, včetně vnitřní elektronické pošty, nemůže však odejít mimo firmu jako nezašifrovaná e-mailová zpráva.

2.6 Probírání důvěrných záležitostí telefonicky

Pokyn: Před poskytnutím informací, které nejsou označené jako veřejné, po telefonu musí osoba, která má informaci sdělit, rozpoznat hlas tazatele nebo musí firemní telefonní systém identifikovat telefonní číslo tazatele jako vnitřní a musí být spojené s jeho jménem.

Poznámky: Pokud není hlas tazatele známý, je třeba zavolat na jeho vnitřní číslo, aby se dal ověřit jeho hlas s hlasem nahrané uvítací zprávy, nebo požádat jeho nadřízeného o potvrzení, že tazatel je oprávněn danou informaci získat.

2.7 Instrukce pro recepce či vrátnice

Pokyn: Personál vrátnice nebo recepce musí zkontrolovat doklad totožnosti s fotografií, než vydá jakoukoliv zásilku osobě, která není známa jako momentálně zaměstnaný pracovník. Je třeba vést knihu a zapisovat do ní jméno, číslo dokladu totožnosti, datum narození a čas převzetí zásilky.

Poznámky: Tento pokyn se vztahuje i na vydávání jakýchkoliv odesílaných kurýrních zásilek. Zásilkové služby vydávají pracovníkům identifikační karty, které mohou být použity při zjišťování totožnosti kurýra.

2.8 Posílání softwaru třetím osobám

Pokyn: Před vysláním nebo zpřístupněním jakéhokoliv programu nebo jeho dokumentace je třeba pozitivně ověřit totožnost žadatele nebo zjistit, jestli je toto zpřístupnění v souladu se zařazením předávané informace do příslušné kategorie. Obvykle je zdrojový kód programů vytvořených ve firmě klasifikován jako přísně tajný.

Poznámky: Určení oprávněnosti osoby k danému programu se obvykle opírá o zjištění, jestli tato osoba konkrétní program ke své práci potřebuje.

2.9 Vymezení obchodních a marketingových informací

Pokyn: Než začne personál zabývající se prodejem a marketingem sdělovat vnitřní telefonní linky, výrobní plány, kontakty na skupiny pracující na konkrétních produktech nebo jiné důvěrné informace jakémukoliv potenciálnímu klientovi, musí vyhodnotit veškeré dostupné informace.

Poznámky: Průmyslovými špiony často používaná taktika spočívá v tom, že se zkontaktují s obchodním zástupcem a rozvinou před ním vizi obrovské transakce. Ve snaze získat tuto zakázku obchodníci často prozrazují informace, které může útočník využít jako trumf při získávání přístupu k tajným informacím.

2.10 Přenos souborů nebo dat

Pokyn: Data a soubory by neměly být kopírovány na žádná přenosná média, ledaže by o to žádala důvěryhodná osoba, jejíž totožnost byla ověřena a jež potřebuje mít data v této formě.

Poznámky. Sociotechnik dokáže lehce oklamat pracovníka a říci mu věrohodný důvod, proč potřebuje zkopírovat důvěrné informace na disketu, CD ROM či jiné přenosné médium a nechat si ho poslat nebo si ho vyzvednout na recepci.

3. Pravidla telefonování

Pravidla telefonovaní zajišťují, aby zaměstnanci dovedli ověřit totožnost volajícího a ochránit svá vlastní kontaktní data před osobami, které volají do firmy.

3.1 Přesměrování hovorů na přístupová čísla k síti nebo na faxy

Pokyn: Na telefonním čísle, které firma používá pro fax nebo modem, nesmí byt možné přesměrování hovorů na vnější čísla.

Poznámky: Rafinovaní útočníci se mohou pokusit oklamat personál telekomunikační firmy nebo pracovníky vnitřní ústředny, aby zapnuli přesměrování vnitřních čísel na vnější čísla, která jsou pod kontrolou útočníků. Takovýto útok umožňuje vetřelci přijímat faxy, formulovat žádosti o vyslání důvěrné informace na vnitřní linku (personál předpokládá, že posílání faxů uvnitř organizace je bezpečné) nebo vymámit od uživatelů připojujících se k síti zvenku přístupové heslo pomocí linky přesměrované na počítač, který simuluje přihlašovací proces.

V závislosti na typu ústředny používané ve firmě může být přesměrování hovorů pod kontrolou vnějšího operátora a nikoliv obsluhy podnikové ústředny. V takovém případě je třeba požádat dodavatele telekomunikačních služeb, aby přesměrovávání čísel, na kterých jsou faxy či modemy, znemožnil.

3.2 Identifikace volajícího

Pokyn: Firemní telefonní systém musí zajišťovat identifikaci volajícího na všech vnitřních telefonních přístrojích a pokud možno umožňovat přiřadit hovorům přicházejícím zvenku, jiný typ vyzvánění.

Poznámky: Pokud si zaměstnanci mohou ověřit totožnost lidí volajících zvenku, může to pomoci předejít útoku nebo identifikovat číslo, ze kterého útočník volal.

3.3 Volně přístupné telefony

Pokyn: Aby se předešlo případům, kdy se návštěvník vydává za zaměstanace firmy, všechny volně přístupné telefony by měly jasně ukazovat umístění přístroje (například vrátnice, chodba, vstupní hala) na displeji telefonu příjemce.

Poznámky: Pokud identifikace volajícího umožňuje zobrazit pouze čísla, je třeba zavést odpovídající opatření pro rozhovory uskutečňované z volně přístupných telefonů nacházejících se na půdě firmy. Je třeba zabránit situaci, kdy by se útočník mohl hovorem z volně přístupného telefonu vydávat za pracovníka a předstírat, že volá z vnitřní linky.

3.4 Počáteční (defaultní) hesla výrobců telefonní systémů

Pokyn: Předtím, než bude zařízení předáno do provozu, musí správce hlasové pošty změnit všechna počáteční hesla.

Poznámky: Sociotechnik může získat seznam defaultních hesel od výrobce a využít je, aby se dostal ke správcovským kontům.

3.5 Hlasové schránky oddělení

Pokyn: Nastav zvláštní hlasové schránky každému oddělení, které má běžně kontakt s veřejností.

Poznámky: Prvním krokem při sociotechnickém útoku je shromažďování informací o firmě a jejím personálu. Omezením dostupnosti jmen jednotlivých pracovníků a jejich telefonních čísel ztěžujeme sociotechnikovi identifikaci cílů útoku a získání jmen zaměstnanců, za které by se mohl při volání jiným osobám vydávat.

3.6 Ověřování servisních pracovníků telefonních systémů

Pokyn: Nelze dovolovat vzdálený přístup servisních techniků telefonního systému bez jejich pozitivní identifikace a kontroly oprávnění k této činnosti.

Poznámky: Počítačoví vetřelci, kteří získají přístup k firemním telefonním systémům, získávají možnost vytvářet hlasové schránky, zachytávat zprávy určené jiným osobám nebo uskutečňovat hovory na náklady firmy.

3.7 Konfigurace telefonního systému

Pokyn: Správce hlasové pošty musí zvýšit bezpečnost nastavením odpovídajících parametrů telefonního systému.

Poznámky: Telefonní systémy lze nastavit na vyšší či nižší úroveň bezpečnosti pro zprávy předávané hlasovou poštou. Administrátor musí mít na paměti bezpečnostní hlediska a spolu s lidmi zabývajícími se bezpečností zkonfigurovat telefonní systém tak, aby byla umožněna ochrana důvěrných dat.

3.8 Zaznamenávání hovorů

Pokyn: Pokud to dodavatel telefonních služeb umožňuje, je dobré všem pracovníkům zapnout možnost nahrávání hovorů, aby ho mohli aktivovat v případě podezření, že volající je vetřelcem.

Poznámky: Pracovníky je třeba proškolit ve využívání služby sledování hovorů a okolností, kdy by měla byt služba použita. Sledování hovoru by mělo být zahájeno, když se volající zjevně pokouší získat neoprávněný přístup k podnikové počítačové síti nebo když žádá o důvěrné informace. Každou aktivaci sledování musí pracovník nahlásit lidem, kteří se zabývají bezpečnostními incidenty.

3.9 Automatizované telefonické systémy

Pokyn: Pokud firma používá automatizovaný telefonický informační systém, musí být naprogramován tak, aby během předávání hovoru na konzultanta nějakého útvaru firmy nebyla sdělována vnitřní telefonní čísla.

Poznámky: Útočníci používají automatizované informační systémy, aby shromaždovali jména a vnitřní linky pracovníků firmy. Znalost vnitřních telefonních čísel jim pomáhá, když přesvědčují příjemce hovorů, že jsou pracovníky téže firmy a mají nárok na vnitřní informace.

3.10 Zablokování hlasových schránek po několika neúspěšných pokusech o přístup

Pokyn: Telefonický systém by měl být naprogramován tak, aby bylo po několika neúspěšných pokusech o přístup do hlasové schránky zablokováno konto.

Poznámky: Správce firemní telefonní sítě musí zablokovat hlasovou schránku po pěti po sobě následujících neúspěšných pokusech o přihlášení. Zablokování může zrušit správce pouze ručně.

3.11 Telefonní linky s omezenou dostupností

Pokyn: Všechny vnitřní linky útvarů a pracovních skupin, které obvykle nemají telefonáty zvenčí (servis, technická pomoc atp.) by měly byt naprogramovány tak, aby se tam bylo možné dovolat pouze z firmy. Volitelně mohou být tyto linky zabezpečené heslem, které musí člověk volající zvenku uvést, aby dostal spojení.

Poznámky: Splnění tohoto pokynu sice zadrží většinu útoků vedených sociotechniky-amatéry, ale odhodlaný útočník dokáže přemluvit pracovníka, aby na takovýto vyhrazený telefon zavolal a požádal osobu, která to zvedne, aby zavolala zpátky útočníkovi. Nebo útočník prostě požádá o uskutečnění telefonické konference s chráněným číslem. Tento trik musí být diskutovaný na školení pracovníků, aby zvýšil jejich povědomí v této oblasti.

4. Ostatní pokyny

4.1 Návrh identifikátoru (visačky)

Pokyn: zaměstnanecké identifikátory musejí být navržené tak, aby se na ně vešla velká fotografie, kterou lze rozeznat z dostatečné vzdálenosti.

Poznámky: Fotografie na standardně používaných identifikátorech v podstatě neplní svou úlohu. Vzdálenost mezi osobou vcházející do budovy a strážným

nebo recepční, která má povinnost identifikátory kontrolovat, je obvykle tak velká, že je obrázek příliš malý, než aby se na něm dala procházející osoba poznat. Aby fotografie plnila svůj úkol, je nutné změnit vzhled identifikátoru.

4.2 Změna přístupových práv při změně místa nebo odpovědnosti

Pokyn: Při každé změně místa nebo při rozšíření či zvýšení odpovědnosti by měl nadřízený dané osoby informovat oddělení informatiky o změnách povinností, aby jí byl přiřazen příslušný nový bezpečnostní profil.

Poznámky: Správa přístupových práv personálu je nezbytná, pokud chceme omezit možnost vyzrazení důvěrných informací. Měla by platit zásada *minimálních práv*; přístupová práva přiřazená uživatelům musí znamenat nezbytné minimum nutné k plnění jejich povinností. Všechny žádosti o změny, jejichž výsledkem je rozšíření přístupových práv, musejí být vyřizovány podle pokynů rozšiřování přístupových práv.

Nadřízený pracovníka nebo osobní oddělení by mělo mít povinnost obracet se se žádostí o příslušné nastavení přístupových práv vlastníka daného konta na oddělení informatiky.

4.3 Speciální identifikátory pro osoby v podniku nezaměstnané

Pokyn: Firma by měla důvěryhodným dodavatelům nebo osobám, které se z pracovních důvodů pravidelně vyskytují v areálu firmy, vydat speciální identifikátory s fotografií.

Poznámky: Osoby nezaměstnané ve firmě, které pravidelně přicházejí do jejího areálu (například dodavatelé zboží do kantýn, servisní technici kopírek nebo telefonní technici) mohou představovat pro firmu ohrožení. Kromě vydání identifikátoru těmto osobám je třeba ještě zajistit vyškolení našich pracovníků, aby si všímali osob, které se pohybují po firmě bez identifikátoru a aby se v takové situaci příslušně chovali.

4.4 Deaktivace kont osob pracujících na základě smlouvy o dílo

Pokyn: Když osoba pracující na základě smlouvy, které bylo v počítačovém systému založeno konto, dokončí svůj úkol nebo když smlouva vyprší, je vedoucí příslušného oddělení povinen informovat o tom oddělení informatiky. To znepřístupní všechna její konta včetně kont umožňujících přístup k databázi, vzdálený přístup přes telefon nebo přes Internet ze vzdálených počítačů.

Poznámky: Po skončení pracovního poměru existuje riziko, že pracovník využije znalost systémů a firemních postupů, aby získal přístup k datům. Všechna počítačová konta používaná pracovníkem musejí být neprodlené zrušena. Týká se to také kont umožňujících přístup do výrobních databází, umožňujících přístup k systému přes modem a všech kont dovolujících přístup k zařízením spojených s počítači.

4.5 Ohlašování incidentů

Pokyn: Měla by být vytvořena struktura, kde by bylo možné hlásit incidenty nebo, v menších firmách, určena osoba, která bude taková oznámení přijímat a její zástupce. Měla by se hlásit veškerá podezření na incidenty narušení bezpečnosti.

Poznámky: Díky centralizaci přijímání hlášení o podezření z narušení bezpečnosti lze odhalit útoky, které by jinak zůstaly nepovšimnuty. Když jsou odhalovány a nahlašovány opakující se útoky, může organizační jednotka, která

hlášení přijímá, odhadnout, o jaké informace se útočník zajímá a učinit dodatečná opatření na jejich ochranu.

Pracovníci určení ke shromaždování hlášení o incidentech se musejí seznámit s metodami a taktikami, které sociotechnici používají, což jim dovolí posoudit hlášení a rozeznat právě probíhající útok.

4.6 Horká linka ohlašování incidentů

Pokyn: Měla by být vytvořena horká telefonní linka na ohlašování incidentů. Její číslo by mělo být snadno zapamatovatelné.

Poznámky: Když mají pracovníci podezření, že se stali cílem sociotechnického útoku, musejí mít možnost dát o tom okamžité vědět příslušným osobám. Aby bylo možné útok ohlásit, všichni lidé používající jakýkoli telefon ve firmě musejí toto číslo znát.

Takto vytvořený systém včasného varování může významně přispět k odhalování právě probíhajícího útoku i k obraně před ním. Pracovníci musejí být dostatečně vyškolení, aby ihned po rozeznání útoku volali na horkou linku. Personál přijímající hlášení by měl ihned informovat skupiny, které jsou oběťmi útoku, že útok může ještě trvat a že je potřeba být ostražitý. Aby toto informování bylo včasné, musí být Číslo horké linky rozšířené po celé firmě.

4.7 Chráněné prostory musejí být střeženy

Pokyn: Ochranka musí monitorovat přístup k chráněným územím firmy a vyžadovat dvě formy ověření.

Poznámky: Jedna z přípustných metod ověření využívá elektronické digitální zámky, které vyžadují přiložení identifikátoru pracovníka ke čtečce (nebo u jiných typů karet protažení čtečkou) a zadání přístupového kódu.

Nejlepší metoda zabezpečení chráněných prostor je však najmout ochrannou službu, která bude hlídat všechny vchody do chráněných prostor. V organizacích, kde by se tato metoda nevyplatila, by se měly používat dvě formy ověřování. V závislosti na finančních možnostech a stupni rizika stojí za to vzít v úvahu biometrické karty.

4.8 Rozvodné skříňky se síťovými a telefonickými zařízeními

Pokyn: Skříňky a místnosti, ve kterých se nacházejí síťové či telefonní kabely nebo síťové přístupové body musejí být neustále zabezpečené.

Poznámky: Do skříněk a místností se síťovými a telefonickými zařízeními může mít přístup pouze oprávněný personál. Každý externí technik musí být pozitivně identifikován podle pokynu vydaných oddělením odpovědným za bezpečnost informací. Přístup k telefonním linkám, *hubům* (rozbočovačům), *switchům* (přepínačům) a *routerům* či *bridgeům* a podobným zatížení by mohl být útočníkem využit k nabourání se do firemní počítačové sítě.

4.9 Vnitřní poštovní přihrádky

Pokyn: Poštovní přihrádky vnitřní pošty nemohou být umístěné ve volně přístupných prostorech.

Poznámky: Průmysloví špióni a hackeři, kteří mají přístup na místa, kde se vyzvedává vnitřní pošta, zde mohou podstrčit padělaný autorizační dopis nebo vnitřní formuláře, které opravňují personál k poskytování důvěrných informací nebo k vykonání činností, které mají útočníkovi pomoci. Kromě toho zde může útočník ponechat disketu či jiný nosič s instrukcemi k instalaci aktualizace softwaru nebo k otevření souboru, která obsahuje útočníkem zapsaná makra.

Každá žádost přijatá vnitřní poštou je pracovníky samozřejmě považována za autentickou.

4.10 Informační tabule, nástěnky

Pokyn: Informační tabule a nástěnky sloužící zaměstnancům by neměly být umístěny na volně přístupných místech.

Poznámky: Mnoho firem věší na nástěnky informace obsahující důvěrné informace týkající se firmy nebo personálu, které si může každý přečíst. Na nástěnkách jsou často vyvěšovány dopisy pracovníků, oznámení zaměstnavatele a podobné informace.

Nástěnky mohou být umístěny v blízkosti podnikových kantýn, závodních jídelen nebo kaváren, tam, kam osoby zvenčí nemají přístup. Informace tohoto druhu by neměly být přístupné hostům navštěvujícím naši firmu.

4.11 Vstup do výpočetního centra

Pokyn: Počítačový sál či serverovna nebo datové centrum by měly být po celou dobu zamčené a personál se musí před vstupem autentikovat.

Poznámky: Firma by měla zvážit používání elektronických identifikátoru nebo čteček přístupových karet, aby byly všechny vstupy automaticky zaznamenány a kontrolovány.

4.12 Objednávání služeb

Pokyn: Personál odpovědný za objednávky nejdůležitějších služeb od dodavatelů musí vytvořit konto chráněné heslem, aby se předešlo objednávkám vytvořeným neoprávněnými osobami jménem firmy.

Poznámky: Dodavatelé služeb a mnoho dalších firem dovoluje klientům založit si pro objednávání vlastní heslo. Firma by měla zavést hesla pro každého dodavatele služeb, které mají pro firmu kritický význam. Tato instrukce se vztahuje zejména na služby spojené s telekomunikacemi a Internetem. Kdykoli by měly být dotčeny kritické služby, je nezbytné pomocí sdíleného tajemství ověřit, jestli je volající oprávněný objednávku vyslat. K tomuto účelu by se neměly používat žádné osobní identifikátory typu DIČ, dívčí jméno matky atp.

Sociotechnik může například zatelefonovat do telekomunikační firmy a zařídit přesměrování hovorů na přístupových linkách do počítačové sítě nebo požádat dodavatele internetových služeb o změnu převodních tabulek, aby byla při vyhledávání jména počítače poskytována nesprávná IP adresa.

4.13 Kontaktní osoba útvaru

Pokyn: Firma může zavést program, v jehož rámci si každý útvar určí kontaktní osobu. Díky tomu bude všechen personál schopný snadno ověřit totožnost neznámých osob, vydávajících se za zaměstnance daného útvaru. Například informatik může zavolat kontaktní osobě z určitého útvaru, aby si ověřil totožnost jeho pracovníka, který telefonuje se žádostí o pomoc.

Poznámky: Tato metoda ověřování totožnosti omezuje počet pracovníků, kteří jsou oprávněni se za osoby zaměstnané v daném oddělení zaručit, když některá z nich žádá o pomoc při zavádění nového hesla nebo při podobných operacích, týkajících se jejího osobního konta v počítačovém systému.

Sociotechnické útoky jsou účinné částečně proto, že personál technické obsluhy často pracuje pod časovým tlakem a neověřuje správně totožnost osob obracejících se na ně se žádostmi o pomoc. Ve větších firmách, které zaměstnávají hodně lidí, nejsou obvykle pracovníci technické podpory schopni všechny oprávněné zaměstnance osobně poznat. Zavedení kontaktní osoby omezuje

počet pracovníků, které musí help desk znát, aby mohl oprávněnost verifikovat.

4.14 Hesla klientů

Pokyn: Pracovníci zákaznického servisu nesmějí znát hesla klientů ani k nim nesmějí mít přístup.

Poznámky: Sociotechnici často volají na zákaznické centrum a pod nějakou záminkou se snaží získat autentikační data nějakého zákazníka, jako je heslo nebo DIČ. S touto informací pak může sodotechnik zatelefonovat jinému konzultantovi ze zákaznického centra, vydávat se za daného klienta a získat žádané informace nebo uskutečnit jeho jménem nějakou objednávku.

Aby se omezila účinnost takovýchto pokusů, musí být software používaný v zákaznických centrech vytvořen tak, aby konzultanti mohli pouze zadávat ověřující informace, které volající uvádí, a obdrželi od systému jen odpověd, jestli jsou tyto údaje správné nebo ne.

4.15 Testování zabezpečení

Pokyn: Pokud má firma v úmyslu provádět testy účinnosti zaváděného bezpečnostního systému založené na používání příslušných sociotechnických taktik, měli by být pracovníci o této možnosti během školení informováni.

Poznámky: Pokud by personál nebyl o možnosti provádění penetračního testu předem informován, mohlo by dojít k situaci, kdy bude pracovník cítit rozpaky, hněv nebo jinou negativní emoci, že je testován jinými pracovníky nebo najatými osobami, které používají sociotechnické metody. Budeme-li o takové možnosti novým pracovníkům říkat během jejich uvádění do pracovních povinností, předejdeme konfliktům tohoto typu.

4.16 Prezentování důvěrných informací

Pokyn: Informace, které nejsou určeny veřejnosti, by neměly být žádnou formou prezentovány na volně přístupných místech.

Poznámky: Kromě tajných informací o produktech a postupech, nesmějí být na očích nepovolaných osob také žádné vnitřní kontaktní informace, jako seznamy pracovníků, vnitřní telefonní čísla nebo harmonogramy obsahující seznamy vedoucích jednotlivých pracovišť.

4.17 Školení bezpečnostního povědomí

Pokyn: Všichni pracovníci firmy, kteří se zapracovávají, musejí projít školením v oblasti bezpečnosti. Navíc musí každý pracovník v pravidelných časových intervalech projít kursy osvěžujícími znalosti. Intervaly mezi kursy určí odbor zabývající se školeními z oblasti bezpečnosti, ale nemají překračovat 12 měsíců.

Poznámky: Mnoho organizací bere problémy bezpečnostního školení na lehkou váhu. Podle výzkumů týkajících se bezpečnosti informací z roku 2001 pouze 30% zkoumaných organizací vyčlenilo prostředky na takováto školení pracovníků na nižších pozicích. Školení tohoto typu je nezbytné, aby se snížila pravděpodobnost úspěšného sociotechnického útoku na firmu.

4.18 Školení o bezpečném přístupu k počítačům

Pokyn: Pracovníci musejí absolvovat kurs bezpečnosti informací, než se jím dá přístup k jakémukoli počítačovému systému.

Poznámky: Sociotechnik si často vybírá za svůj cíl nové zaměstnance, protože vědí, že zpravidla ještě nejsou obeznámeni se zásadami, které popisují, jak je nutno s důvěrnými informacemi zacházet.

Školení by mělo dávat pracovníkům příležitost klást otázky týkající se bezpečnostních zásad. Po absolvování školení by měl vlastník konta podepsat dokument potvrzující, že se s bezpečnostními zásadami seznámil a že s jejich dodržováním souhlasí.

4.19 Barevné označení identifikátorů

Pokyn: Identifikátory by měly být označeny různými barvami, což dovolí rozlišit zaměstnance, externistu, brigádníka, dodavatele, konzultanta a hosta.

Poznámky: Barevný identifikátor umožňuje rozlišit status dané osoby z větší vzdálenosti. Alternativou je používání velkých písmen popisujících status, ale v tomto případě barvy vylučují omyl a je snazší je použít.

Typická taktika, kterou sociotechnici používají, aby se dostali na půdu firmy, je převléci se za dodavatele zboží nebo dočasně zaměstnanou osobu. Když se útočník dostane dovnitř, začne se vydávat za pracovníka nebo bude nějak jinak falešné uvádět svůj status, aby získal pomoc od nic netušících zaměstnanců. Cílem tohoto pokynu je předcházet situaci, kdy sociotechnik vchází do areálu firmy legálně, aby potom slídil v prostorech, kde nemá co dělat. Například osoba, která vstoupila jako telefonní technik, se nebude moci vydávat za pracovníka, protože barva identifikátoru bude jednoznačně ukazovat, že tato osoba nepatří k firmě.

5. Pokyny pro oddělení informatiky

Oddělení informatiky v každé firmě potřebuje pokyny pomáhající chránit informační bohatství organizace. Abych reflektoval typickou strukturu úkolů takového oddělení, rozdělil jsem pokyny na obecné, pro technickou pomoc (*help desk*), správu sítě a práci na počítači.

Obecné

5.1 Kontaktní údaje osob v oddělení informatiky

Pokyn: Telefonní čísla a e-mailové adresy jednotlivých pracovníků oddělení informatiky by neměly být sdělovány žádné osobě, která nemá pádný důvod k tomu, aby je znala.

Poznámky: Účelem tohoto pokynu je vyhnout se situaci, kdy sociotechnik ke svým cílům využije kontaktní informace osob z oddělení informatiky. Tím, že zveřejníme pouze obecné kontaktní číslo a e-mail na oddělení informatiky, zajistíme, že se osoby zvenčí nebudou moci kontaktovat s personálem bezprostředně. E-mailové adresy pro potřeby kontaktu s administrátorem nebo webmasterem by se měly skládat pouze z obecných slov jako *admin@jmenofirmy.cz*. Zveřejněná telefonní čísla by měla být propojena na hlasovou schránku oddělení, nikoliv na konkrétního pracovníka.

Pokud jsou dostupné přímé kontakty, pak se může vetřelec dostat k nějakému pracovníkovi, zmanipulovat ho a získat informace, které se pak hodí během útoku nebo které mu umožní vydávat se v rozhovoru s jinými osobami za informatika.

5.2 Požadavky na technickou pomoc

Pokyn: Všechny žádosti o technickou pomoc musejí být směrované na skupinu či osoby, které mají daný problém na starosti.

Poznámky: Sociotechnici se mohou pokoušet naléhat na informatiky, kteří se obvykle technickou pomocí nezabývají a tak neznají příslušné postupy, upravující způsob poskytování takové pomoci. Proto také musí být personál informatického oddělení proškolen, aby žádosti tohoto typu odmítal a směroval volajícího na skupinu či osoby, které mají tyto záležitostí na starosti.

6. Technická pomoc (help desk)

6.1 Pokyny ke vzdálenému přístupu

Pokyn: Personál technické pomoci nemůže sdělovat podrobnosti nebo návody ke vzdálenému přístupu, včetně přístupových míst do vnější sítě nebo telefonních čísel na modemy, pokud nebyl volající:

- ověřen jako oprávněná osoba, která může dostat vnitřní informace
- ověřen jako oprávněná osoba, která se může připojovat k podnikové síti jako vzdálený uživatel. Pokud pracovník help desku nezná osobu osobně, musí být pozitivně identifikována podle ověřovacích a autorizačních procedur, které jsou popsány na začátku této kapitoly.

Poznámky: Firemní help desk se často stává hlavním cílem sociotechnického útoku nejen z podstaty jeho funkce pomáhat uživatelům v záležitostech spojených s obsluhou počítače, ale i z důvodu vyšších systémových práv, která obvykle pracovníci technické pomoci mají. Všechen personál help desku by měl být vyškolen tak, aby fungoval jako „lidský firewall", předcházející prozrazování informací neoprávněným osobám, kterým by mohly pomoci získat přístup k informacím firmy. Jednoduché pravidlo je zákaz sdělování postupu na vzdálený přístup bez pozitivního ověření totožnosti.

6.2 Změna hesel

Pokyn: Heslo k uživatelskému účtu může být změněno pouze na žádost příslušného uživatele.

Poznámky: Nejčastějším sociotechnickým trikem je změna hesla konta někoho jiného. Útočník se vydává za pracovníka a tvrdí, že ztratil nebo zapomněl heslo. Aby se snížila šance na úspěch takového útoku, informatik, který obdrží takovou žádost o změnu hesla, musí zavolat pracovníkovi zpátky, než vůbec začne cokoliv dělat. Telefonát se musí uskutečnit na číslo, které je u daného pracovníka uvedeno v podnikovém telefonním seznamu a ne na to, které uvede sám volající. Více informací na toto téma lze najít v podkapitole „Ověřovací a autorizační procedury".

6.3 Změna přístupových práv

Pokyn: Všechny žádosti o rozšíření uživatelských nebo přístupových práv musejí být písemně schválené nadřízeným vlastníka konta. Po provedení změny je třeba poslat potvrzení tomuto nadřízenému vnitřní podnikovou poštou. Kromě toho musí být taková žádost ověřena jako autentická pomocí příslušných ověřovacích a autorizačních procedur.

Poznámky: Jakmile se útočníkovi podaří dostat se na standardní uživatelské konto, bude dalším krokem pokus zvýšit svá práva, aby získal kontrolu nad celým systémem. Útočník, který zná autorizační proces, může zfalšovat autorizační žádost, je-li podávána faxem, e-mailem nebo telefonicky.

Například útočník může zavolat na technickou pomoc a pokoušet se přesvědčit konzultanta, aby mu přidělil další přístupová práva na už dříve proraženém kontě.

6.4 Autorizace nových kont

Pokyn: Žádost o vytvoření nového konta pro pracovníka, externistu nebo jinou oprávněnou osobu musí mít písemnou formu a musí být podepsaná nadřízeným dané osoby nebo musí být poslána bezpečným e-mailem s elektronickým podpisem. Takové žádosti musejí být ověřeny též posláním potvrzení o vytvoření nového konta vnitřní poštou.

Poznámky: Protože jsou hesla a jiné užitečné informace, které se hodí při pronikání do počítačových systémů, prvořadými cíli útoků zlodějů informací, je nutné používat určité obranné prostředky. Cílem tohoto pokynu je znemožnit vetřelcům vydávat se za oprávněné osoby a znemožnit falšování žádostí o vytvoření nového účtu. Proto musejí být takové žádosti ověřeny podle příslušných procedur.

6.5 Doručení nového hesla

Pokyn: Nová hesla musejí být považována za tajnou informaci a musejí být distribuována bezpečnými metodami, například osobně, doporučeným dopisem nebo kurýrní zásilkou (viz „Distribuce tajných informací").

Poznámky: Je též možné použít vnitřní poštu, ale pak se doporučuje posílat heslo v zabezpečených obálkách, které znemožňují prohlížet si obsah skrz obálku. Metodou ke zvážení je určení jedné osoby v každém útvaru, která bude mít na starosti distribuci nových detailů týkajících se účtů a potvrzování totožnosti osob, které ztratily nebo zapomněly své heslo. Díky tomu budou pracovníci help desku pracovat s omezenou množinou osob, které mohou znát osobně.

6.6 Blokování kont

Pokyn: Před zablokováním uživatelského konta je třeba ověřit, jestli žádost pochází od oprávněné osoby.

Poznámky: Smyslem tohoto bodu je předcházet útočníkovým neautorizovaným žádostem o pozastavení konta. Po zablokování něčího účtu se bude sociotechnik snažit získat důvěru postižené osoby, nabízí pomoc a řešit problém s přístupem do systému. Když sociotechnik někomu telefonuje jako technik a ví, že se uživatel nemůže přihlásit do sítě, oběť může často přistoupit na prozrazení svého hesla, aby byl problém odstraněn.

6.7 Deaktivace zásuvek a síťových zařízení

Pokyn: Nelze deaktivovat zásuvky a síťová zařízení na základě žádosti neověřené osoby.

Poznámky: Smyslem tohoto bodu je předcházet neautorizovaným žádostem útočníka o deaktivaci zásuvky. Po zablokování něčí zásuvky se bude sociotechnik snažit získat důvěru postižené osoby, nabízet pomoc a řešit problém s přístupem do systému. Když sociotechnik někomu telefonuje jako technik a ví, že se uživatel nemůže přihlásit do sítě, oběť může často přistoupit na prozrazení svého hesla, aby byl problém odstraněn.

6.8 Sdělování postupu na bezdrátový přístup

Pokyn: Nelze sdělovat návod na přístup do firemního systému přes bezdrátové připojení osobám, které nemají oprávnění tento způsob přístupu používat.

Poznámky: Před sdělením návodu na bezdrátové připojení k firemní síti se vždy musí začínat od ověření dané osoby jako oprávněné k připojování se k firemní síti jako vzdálený uživatel (viz „Ověřovací a autorizační procedury").

6.9 Jména osob ohlašujících problémy

Pokyn: Jména osob, které hlásily potíže s počítači, by se neměla dostat mimo oddělení informatiky.

Poznámky: Při typickém útoku bude sociotechnik volat na help desk a žádat o jména osob, které v poslední době hlásily nějaké problémy s počítači. Volající se může představit jako pracovník nebo jako dodavatel. Jakmile získá jména těchto osob, bude se s nimi kontaktovat, vydávat se za pracovníka technické podpory a nabízet svou pomoc. Během rozhovoru útočník vyloudí od oběti informace, které potřebuje k uskutečnění svých záměrů.

6.10 Zadávání systémových příkazu nebo spouštění programů

Pokyn: Pracovníci zaměstnaní v oddělení informatiky, kteří mají privilegovaná konta, by neměli zadávat žádné příkazy ani spouštět programy na žádost někoho, koho osobně neznají.

Poznámky: Známá metoda útočníků je nainstalovat trojského koně či jiný malware, změnit jméno tohoto programu a zatelefonovat na help desk, že se při pokusu o spuštění tohoto programu objevuje chybová hláška. Útočník prosí konzultanta, aby zkusil program spustit sám. Spuštěný program dědí práva uživatele, který ho spustil, a dává tak útočníkovi stejná práva, jaká má konzultant. Díky tomu může útočník převzít kontrolu nad firemním počítačovým systémem.

Tento pokyn zavádí preventivní prostředek proti popsané taktice, když od konzultanta help desku vyžaduje verifikaci statutu volajícího pracovníka před spuštěním jakéhokoliv programu na jeho žádost.

7. Správa systému

7.1 Změna globálních přístupových práv

Pokyn: Žádost o změnu globálních přístupových práv musí být potvrzena skupinou, která spravuje přístupová práva na firemní síti.

Poznámky: Autorizovaný personál by měl provést analýzu každé žádosti tohoto typu, aby určil, jestli změna nemůže způsobit ohrožení bezpečnosti informací. Pokud ano, odpovědná osoba probere příslušné podrobnosti s žadatelem a společně přijmou rozhodnutí o navrhovaných změnách.

7.2 Žádosti o vzdálený přístup

Pokyn: Vzdálený přístup k počítači bude poskytován pouze těm osobám mimo firemní prostory, které mají k používání firemního počítačového systému zjevný důvod. Žádost o poskytnutí takového přístupu musí být podána nadřízeným daného pracovníka a ověřena podle ověřovacích a autorizačních procedur.

Poznámky: Zjišťování skutečné potřeby vzdáleného přístupu a jeho omezení na osoby, pro které je nezbytný, radikálně snižuje riziko a zjednodušuje správu

vzdálených uživatelů. Čím méně lidí má taková privilegia, tím menší je počet útočníkových potenciálních cílů. Nelze také zapomínat, že útočníci se mohou zaměřit na vzdálené uživatele s úmyslem zachytit jejich spojem do firemní sítě nebo se za ně při telefonování do firmy vydávat.

7.3 Změna hesel na privilegovaných účtech

Pokyn: Žádost o změnu hesla privilegovaného konta musí být schválena správcem konkrétního systému, ve kterém dané konto existuje. Nové heslo musí být posláno vnitřní poštou nebo předáno osobně.

Poznámky: Privilegovaná konta umožňují přístup k všelijakým systémovým datům a souborům uloženým v daném systému. Proto také tato konta vyžadují nejvyšší možnou úroveň ochrany.

7.4 Vzdálený přístup pro externí servisní techniky

Pokyn: Nelze umožňovat vzdálený přístup k počítačovému systému ani o něm nelze poskytovat informace vnějším technikům (například představitelům výrobce či dodavatele námi používaného zařízení nebo softwaru) bez ověření jejich totožnosti a bez kontroly, zda jsou oprávněni vykonávat takové služby. Pokud technik potřebuje privilegovaný přístup k systému, aby vykonal svůj úkol, pak by mělo být heslo na jeho kontě změněno ihned po skončení práce.

Poznámky: Hackeři se mohou vydávat za představitele dodavatelů, aby mohli získat přístup k firemní počítačové nebo telekomunikační síti. Proto je důležité ověřit technikovu totožnost a oprávnění vykonávat daný úkol v systému. Navíc dveře do systému musejí být zabouchnuty ihned po skončení jeho práce změnou hesla konta, které používal.

Technici si nemohou sami vybírat heslo k žádnému kontu, ani dočasnému. Někteří dodavatelé jsou známi tím, že používají stejná hesla ve všech svých produktech. Například jedna z firem zabývajících se zabezpečováním sítí zavedla ve všech systémech svých klientů privilegovaná konta se stejným heslem a ještě ke všemu se na ta konta šlo dostat Telnetem.

7.5 Autentikace při vzdáleném přístupu k firemní síti

Pokyn: Všechna přístupová místa k firemní síti ze vzdálených lokalit musejí být chráněna účinnými ověřovacími mechanismy, jako jsou dynamická hesla nebo biometrická zařízení.

Poznámky: Mnoho firem se opírá o statická hesla jako o dostatečný ověřovací prostředek pro vzdálené uživatele. Tato praxe není moc bezpečná: hackeři si vybírají za cíl jeden ze vzdálených přístupových bodů, který může být slabým článkem sítě oběti. Nikdy nemáme jistotu, jestli někdo jiný nezná naše heslo.

Proto také každý přístupový bod musí být chráněný spolehlivým ověřovacím nástrojem jako jsou časově závislé kódy, speciální biometrické karty nebo podobná zařízení. Díky tomu nebudou mít pro vetřelce získaná hesla cenu.

Pokud není ověřování založené na dynamických heslech možné, musejí uživatelé přísně dodržovat pokyny o vymýšlení těžko uhodnutelných hesel.

7.6 Konfigurace operačních systémů

Pokyn: Správci systému by měli zajistit, aby byly operační systémy zkonfigurovány pokud možno v souladu se všemi příslušnými bezpečnostními procedurami a pokyny.

Poznámky: Vytvoření a distribuce bezpečnostních pokynů je základním krokem směrem k redukci rizika, ale jejich dodržování už ve většině případů závisí na samotných pracovnících. Jistá část pokynů může být vynutitelná příslušnou

konfigurací operačního systému, jako například minimální délka hesla. Automatizování bezpečnostních instrukcí díky konfiguraci parametrů operačního systému efektivně omezuje lidský prvek a zvyšuje celkovou bezpečnost organizace.

7.7 Vypršení účtů

Pokyn: Platnost všech kont na počítačích musí být nastavena na jeden rok.

Poznámky: Smyslem tohoto bodu je eliminace kont, která už nejsou používána, protože ta se často stávají cílem útoku hackerů. Tento proces zajišťuje, že jakákoliv konta patřící bývalým zaměstnancům nebo spolupracovníkům firmy, která nedopatřením zůstala v systému, budou automaticky časem pozastavena.

7.8 E-mailové adresy útvarů

Pokyn: Oddělení informatiky musí vytvořit obecnou e-mailovou adresu pro každý útvar podniku, která bude obvykle používána při komunikaci s vnějším světem.

Poznámky: Obecnou e-mailovou adresu může sdělovat recepční po telefonu nebo může být uvedena na firemní webové stránce. Pracovníci by měli poskytovat své individuální e-mailové adresy, jen pokud je to nezbytné.

V rámci první fáze sociotechnického útoku se útočník často snaží získat telefonní čísla, jména nebo informace o zařazení pracovníků. Ve většině případů jsou tyto informace obecně přístupné na internetových stránkách nebo jsou sdělovány po telefonu. Vytváření obecných schránek hlasové i elektronické pošty ztěžuje spojování jmen pracovníků s konkrétními útvary a pracovními povinnostmi.

7.9 Kontaktní adresy při registraci domén

Pokyn: Při registraci internetových domén by neměly kontaktní informace na administrátorský nebo technický personál obsahovat jména konkrétních osob, ale místo toho by měl být uváděn seznam obecných e-mailových adres a telefonní číslo na ústřednu firmy.

Poznámky: Smyslem tohoto bodu je předejít využití kontaktních informací hackerem. Pokud jsou v kontaktních informacích uvedena jména osob a jejich telefonní čísla, vetřelec se může pokusit zmanipulovat některou z těchto osob a vymámit z ní informace nebo ji přemluvit k nějaké činnosti, která mu pomůže dosáhnout zamýšleného cíle. Sociotechnik se též může vydávat za jmenovanou osobu ve snaze obelstít takto personál firmy.

Kontaktní informace by měly místo individuální e-mailové adresy pracovníka obsahovat adresy například *administrator@jmenofirmy.cz* . Personál telekomunikačního oddělení může vytvořit obecnou hlasovou schránku pro potřebu kontaktů v technicko-administrativních záležitostech, aby omezil oblast zveřejňovaných informací, které se mohou sociotechnikovi hodit.

7.10 Instalace aktualizací zabezpečení a operačních systémů

Pokyn: Všechny aktualizace operačního systému a používaných aplikací by měly být instalovány ihned, jakmile se objeví. Pokud tato instrukce koliduje s funkčností kritických produkčních systémů, měly by být aktualizace uskutečněné, jak jen to bude možné.

Poznámky: Po odhalení díry v systému je třeba se ihned spojit s jeho výrobcem, abychom se dozvěděli, jestli už byla vydána příslušná záplata (*patch*). Neaktualizovaný systém představuje jedno z největších ohrožení bezpečnosti v podniku. Pokud správce systému otálí s instalací nezbytných aktualizací, nechává hackerům otevřené dveře.

Na Internetu jsou každý týden zveřejňovány tucty informací o odhalených děrách v systémech. Pokud není informatický personál bdělý a nehlídá aktuální opravné balíčky systému bez ohledu na jeho druh, bude bezpečnost firemní sítě vždy ohrožena. Je neobyčejně důležité být v obraze ohledně zveřejněných informací o bezpečnostních dírách v operačních systémech i v různých každodenně používaných aplikacích.

7.11 Kontaktní informace na webových stránkách

Pokyn: Internetová stránka určená veřejnosti by neměla obsahovat žádné podrobnosti týkající se struktury firmy ani uvádět jména pracovníků.

Poznámky: Informace o struktuře firmy, například organizační struktura, struktura hierarchie, seznamy pracovníku, struktura odpovědnosti, jména, pracovní zařazení, vnitřní kontaktní čísla, zaměstnanecká čísla a podobně, by neměly byt zpřístupňovány na internetových stránkách určených pro veřejnost.

Hackeři často získávají mnoho užitečných informací přímo na stránkách společností, které chtějí napadnout. Útočník tyto informace využívá, vydává se za pracovníka obeznámeného s chodem firmy a snaží se s jejich pomocí získat důvěru u pracovníka, se kterým hovoří. Kromě toho může útočník zveřejněné informace analyzovat, aby našel osoby, na které by stálo za to zaútočit, protože mohou mít přístup k cenným informacím.

7.12 Vytváření privilegovaných kont

Pokyn: Bez autorizace správou systému by neměla být vytvářena žádná privilegovaná konta ani by neměla být poskytována nějakému kontu systémová práva.

Poznámky: Hackeři se často vydávají za dodavatele softwaru nebo síťových zařízení a pokoušejí se obelstít informatický personál a přesvědčit ho, aby pro ně vytvořili nové konto. Smyslem tohoto bodu je zamezit takovým útokům zavedením větší kontroly nad vytvářením privilegovaných účtů. Každou žádost o vytvoření konta se systémovými právy musí schválit administrátor.

7.13 Konta pro hosty

Pokyn: Konta pro hosty by měla být ve všech počítačových systémech a síťových zařízeních zrušena, kromě vedením schváleného FTP serveru umožňujícího anonymní přístup.

Poznámky: Konta pro hosty se vytvářejí proto, aby se umožnil dočasný přístup do systému osobám, které nemusejí mít vlastní konto. Mnoho operačních systémů se instaluje s implicitně povolenými konty pro hosty. Tyto účty by měly být vždy zablokovány, protože znemožňují jakoukoliv identifikaci uživatele. Informatici musejí mít možnost kontrolovat každou aktivitu na počítačích a spojit si ji s konkrétním uživatelem.

Sociotechnici jsou schopni účet pro hosty jednoduše využít, aby získali přístup do systému.

7.14 Šifrování záložních kopií uložených mimo firmu

Pokyn: Všechna data uložená mimo firmu by měla být zakódována, aby se k nim znemožnil přístup neoprávněným osobám.

Poznámky: Personál odpovědný za šifrování se musí ujistit, jestli se v případě potřeby dají data ze zálohy obnovit. Vyžaduje to pravidelné testy, kdy se budou vybrané části zašifrovaných souborů dešifrovat a kontrolovat, jestli jsou v pořádku. Kromě toho by použité šifrovací klíče měly být svěřeny důvěryhodnému vedoucímu pro případ jejich ztráty nebo zničení.

7.15 Přístup návštěvníků k síťovým zásuvkám

Pokyn: Všechny volně přístupné body k Ethernetu musejí být na segmentu, který neumožňuje přístup do vnitřní sítě.

Poznámky: Smyslem tohoto bodu je předejít možnosti, kdy by se k firemní síti připojili návštěvníci, kteří jsou v areálu společnosti. Ethernetové zásuvky instalované v konferenčních místnostech, bufetech, školicích sálech a jiných prostorách přístupných hostům by měly být filtrované, aby se znemožnil přístup do firemních počítačových systémů neoprávněným osobám. Síťový nebo bezpečnostní administrátor se může — pokud je to možné — rozhodnout nastavit na přepínači (*switch*) vituální LAN, aby získal nad přístupem z těchto míst kontrolu.

7.16 Modemy

Pokyny: Modemy používané na příjem spojení zvenku by měly být nastavené tak, aby nepřijímaly spojení dříve než po čtvrtém zazvonění.

Poznámky: Jak je ukázáno ve filmu *War Games*, hackeři používají techniku zvanou *war-dialing* (skenování čísel), aby lokalizovali telefonní linky, na kterých jsou zapojeny modemy. Proces začíná identifikací prefixů čísel nacházejících se v oblasti sídla firmy. Potom se použije skenovací program, který zkouší všechna telefonní čísla začínající tímto předčíslím. Kvůli urychlení jsou tyto programy konfigurované tak, aby čekaly na odpověd modemu jedno nebo dvě zazvonění a potom přešly na další číslo.

Pokud firma na svých modemech nastaví odpovídání alespoň po čtyřech zazvoněních, skenovací program tuto linku nepozná jako modemovou.

7.17 Antivirové programy

Pokyn: Každý počítačový systém by měl mít nainstalovanou a spuštěnou aktuální verzi antivirového programu.

Poznámky: Ve firmách, kde se automaticky nedistribuuje antivirový software a soubory s definicemi virů (umožňují rozeznávat nové viry) na počítače uživatelů, musejí uživatelé sami převzít odpovědnost za instalaci a udržování antivirového softwaru na svých počítačích, včetně těch, které používají ke vzdálenému připojování do firemní sítě.

Je-li to možné, měl by být software zkonfigurován na každodenní automatickou aktualizaci seznamu virů a trojských koní. Pokud nejsou soubory se seznamy automaticky posílány na počítače uživatelů, měli by být uživatelé sami odpovědni za aktualizaci souborů alespoň jednou týdně.

Tyto pokyny mají být uplatněny na všechny stolní i přenosné počítače, které jsou používány k přístupu do firemního počítačového systému, nezávisle na tom, jestli je počítač firemní, nebo soukromý.

7.18 Přílohy v příchozí poště (požadavky na vysokou bezpečnost)

Pokyn: Ve firmách, kde mají vysoké požadavky na bezpečnost, by měl být firewall zkonfigurovaný tak, aby filtroval všechny přílohy v elektronické poště.

Poznámky: Tento bod se vztahuje na firmy, které mají vysoké požadavky na bezpečnost, nebo na ty, které nemají potřebu přijímat soubory prostřednictvím elektronické pošty.

7.19 Ověřování softwaru

Pokyn: Nové programy, aktualizace či opravy získané na fyzických nosičích nebo stažené z Internetu musejí být před instalací ověřeny jako autentické. Tento bod se týká především informatického oddělení a instalace programů, které vyžadují systémová práva.
¨

Poznámky: Software, o kterém je v tomto bodu řeč, jsou komponenty operačního systému, aplikace, opravy a aktualizace jakýchkoliv programů. Mnoho výrobců softwaru zavedlo metody, pomocí nichž si zákazník může ověřit autentičnost každé distribuce, obvykle pomocí elektronického podpisu. V každém případě, pokud nemůže být autentičnost ověřena, je třeba se spojit s výrobcem, aby ji potvrdil. Hackeři jsou známí tím, že obětem posílají software, který se tváří tak, jako by pocházel od výrobce. Proto je také třeba každý získaný program před jeho instalací ve firemních počítačových systémech zkontrolovat (zvláště pokud nebyl očekáván).

Stojí za to uvědomit si, že se rafinovaný útočník mohl dozvědět, že si naše organizace u výrobce objednala nějaký software. S touto informací může naši objednávku u výrobce stornovat a objednat si jej sám. Pak program modifikuje, aby plnil jím požadovaný úkol, a pošle ho naší firmě v originálním balení, včetně smršťovací fólie. Po instalaci softwaru získává útočník kontrolu nad systémem.

7.20 Implicitní hesla

Pokyn: Všechny operační systémy nebo hardwarová zařízení, která měla na počátku hesla nastavená na implicitní hodnotu, musejí mít heslo změněno podle pokynů týkajících se tvorby hesel.

Poznámky. Mnoho operačních systémů a počítačových zařízení je dodáváno s nastavenými počátečními hesly — tedy stejnými v každém prodaném kusu výrobku. Opomenutí změny implicitního hesla je vážná chyba, která představuje pro firmu kritické ohrožení.

Počáteční hesla jsou široce známa a jsou dostupná na Internetu. Během útoku první heslo, které vetřelec vyzkouší, je obvykle defaultní heslo od výrobce.

7.21 Blokování kont po několika pokusech o přístup (nízké nebo střední nároky na bezpečnost)

Pokyn: Pokud se vyskytnou neúspěšné pokusy o přístup na nějaké konto, mělo by se po určeném počtu pokusů toto konto automaticky na nějaký čas pozastavit.

Poznámky: Všechny pracovní stanice a servery ve firmě musejí mít nastavený limit počtu po sobě následujících neúspěšných pokusů o přihlášení. Tento bod má předejít uhodnutí hesla metodou pokusů a omylů, slovníkovými útoky nebo silovými útoky, které mají za cíl získat přístup do systému.

Správce musí zkonfigurovat zabezpečení tak, aby byl účet po překročení přípustného počtu pokusů pozastaven. Doporučuje se blokovat konto po sedmi neúspěšných pokusech v řadě.

7.22 Blokování kont po několika pokusech o přístup (vysoké nároky na bezpečnost)

Pokyn: V organizacích s vysokými nároky na bezpečnost by měl být účet po překročení přípustného počtu pokusu automaticky zablokován s tím, že odblokovat konto by mohla jedině osoba, která má na starost uživatelské účty.

Poznámky: Všechny pracovní stanice a servery ve firmě musejí mít nastavený limit počtu po sobě následujících neúspěšných pokusů o přihlášení. Tento bod má předejít uhodnutí hesla metodou pokusů a omylů, slovníkovými nebo silovými útoky, které mají za cíl získat přístup do systému.

Administrátor musí zkonfigurovat bezpečnostní nastavení tak, aby bylo konto pozastavené po pěti neúspěšných pokusech o přihlášení. Po takovém útoku se bude muset vlastník účtu kontaktovat s technickou obsluhou nebo skupinou, která má správu kont na starosti, aby konto znovu obnovila. Před povolením konta musí být ověřena totožnost vlastníka konta podle ověřovacích a autorizačních procedur.

7.23 Periodická změna hesel privilegovaných účtů

Pokyn: Hesla na privilegovaných účtech by se měla měnit alespoň každých třicet dnu.

Poznámky: V závislosti na omezeních operačního systému musí administrátor podpořit tento pokyn nastavením příslušných parametrů systému.

7.24 Periodická změna hesel uživatelů

Pokyn: Všichni vlastníci kont si musejí měnit svá hesla alespoň jednou za šedesát dní.

Poznámky: V operačních systémech, které to umožňují, by měl administrátor tento pokyn podpořit příslušným nastavením parametrů.

7.25 Nastavení hesla na novém účtu

Pokyn: Heslo nového konta musí být nastaveno jako prošlé, aby byl uživatel při prvním přihlášení nucen zvolit si nové heslo.

Poznámky: Tento požadavek zajišťuje, že své heslo bude znát pouze vlastník konta.

7.26 Bootovací heslo

Pokyn: Všechny počítačové systémy musejí být zkonfigurovány tak, aby při startu systému vyžadovaly heslo.

Poznámky: Počítače musejí být zkonfigurovány tak, aby po jejich zapnutí a před startováním operačního systému bylo vyžadováno heslo. Předchází to situacím, kdy neoprávněná osoba používá počítač jiné osoby. Tento bod je závazný pro všechny počítače ve firmě.

7.27 Požadavky na hesla privilegovaných účtů

Pokyn: Všechna privilegovaná konta musejí být chráněna heslem splňujícím následující pravidla:

- nemůže to být slovo nacházející se ve slovníku žádného jazyka;
- je třeba používat velká i malá písmena, alespoň jeden symbol a alespoň jednu číslici;
- mělo by být dlouhé alespoň 12 znaku;
- nemůže mít žádný vztah k firmě nebo k vlastníkovi konta.

Poznámky: Ve většině případů se cílem hackerú stávají konta, která mají systémová práva. Občas bude útočník hledat jiná slabá místa, aby získal plnou kontrolu nad systémem.

První hesla, která vetřelec zkusí, budou jednoduché obecně používané výrazy ze slovníku. Volba těžko uhodnutelného hesla zvyšuje bezpečnost, snižuje pravděpodobnost, že se ho hackerovi podaří uhodnout pomocí metody pokusů a omylů či využitím slovníkového nebo silového útoku.

7.28 Bezdrátový přístup

Pokyn: Všichni uživatelé, kteří využívají bezdrátový přístup k síti, by měli používat technologii VPN (virtuální privátní síť).

Poznámky: Bezdrátové sítě se staly předmětem útoků pomocí nové techniky zvané *war driving*. To v podstatě znamená, že se jezdí autem nebo se prochází po ulici s notebookem vybaveným kartou používající protokol 802.11B a hledá se bezdrátová síť.

Mnoho firem si postavilo bezdrátovou síť bez aktivace protokolu WEP (*wireless equivalency protocol*), který slouží k šifrovanému zabezpečení bezdrátových spojení. Ale i když je aktivovaný, tak aktuální verze (z poloviny roku 2002) funguje neefektivně a několik internetových stránek je věnovaných prostředkům, kterak lze lokalizovat otevřené bezdrátové systémy a jak lámat přístupové body zabezpečené protokolem WEP.

V této souvislosti je velmi důležité přidat dodatečnou ochrannou vrstvu okolo protokolu 802.11B použitím technologie VPN.

7.29 Aktualizace souborů s definicemi virů

Pokyn: Každý systém musí být naprogramovaný tak, aby automaticky aktualizoval soubory s definicemi virů a trojských koní.

Poznámky: Aktualizace by měla probíhat minimálně jednou týdně. Ve firmách, kde zůstávají počítače zapnuté přes noc, se doporučuje aktualizace každou noc.

Antivirový software je neúčinný, pokud není aktualizován, aby mohl odhalovat všechny nové formy nebezpečného kódu. Protože se ohrožení viry, červy a trojskými koňmi značně zvyšuje, je důležité, aby antivirový software šel s dobou.

8. Obsluha počítače

8.1 Zadávání příkazů nebo spouštění programů

Pokyn: Operátoři počítačů nemohou zadávat příkazy ani spouštět programy na žádost jim neznámých osob. Dokonce i v případech, kdy se zdá, že žádost neprověřené osoby se opírá o skutečné důvody, nemělo by se jí vyhovět bez souhlasu nadřízeného.

Poznámky: Operátoři jsou typickými cíli sociotechniků, protože jejich práce obvykle vyžaduje privilegovaný přístup do systému a útočník očekává, že budou méně zkušení a méně obeznámeni s firemními procedurami, než ostatní pracovníci oddělení informatiky. Smyslem tohoto bodu je přidání kontrolního prvku, aby byli operátoři zabezpečeni před sociotechnickými útoky.

8.2 Pracovníci s privilegovanými účty

Pokyn: Pracovníci, kteří mají privilegovaná konta, nemohou pomáhat ani poskytovat informace neověřeným osobám. Zejména se to vztahuje na pomoc s obsluhou počítače (ovládání aplikace), přístup k databázi, stanování programů nebo sdělování jmen osob, které mají oprávnění ke vzdálenému přístupu.

Poznámky: Sociotechnici si často vybírají za cíl pracovníky s privilegovanými konty. Smyslem tohoto bodu je vést informatický personál k tomu, aby si poradil s telefonáty, které mohou pocházet od sociotechniků.

8.3 Informace o používaných systémech

Pokyn: Operátoři nemohou sdělovat žádné informace o systémech nebo zařízeních, které se ve firmě používají, aniž by si ověřili totožnost volajícího.

Poznámky: Hackeři často kontaktují operátory, aby získali cenné informace jako jsou přístupové procedury k systému, vnější místa vzdáleného přístupu, přístupová čísla atp.

Ve firmách, kde mají technickou podporu či help desk, by měly být považovány za podezřelé žádosti směrované na operátory o informace spojené s počítačovými systémy nebo podobnými zařízeními. Všechny žádosti o informace by měly být posouzeny podle platné klasifikace dat, aby se určilo, jestli je daná osoba oprávněna tuto informaci obdržet. Pokud nelze zařazení informace určit, měla by být pokládána za vnitřní.

V některých případech potřebuje technická podpora dodavatele komunikovat s osobami, které mají přístup k firemním počítačovým systémům. V takové situaci by měl představitel dodavatele znát konkrétní osobu z oddělení informatiky, se kterou bude v kontaktu, aby se mohli vzájemně poznat.

8.4 Sdělování hesel

Pokyn: Operátoři nesmějí pod žádnou záminkou prozrazovat svá hesla nebo hesla jim svěřená bez předchozího souhlasu vedoucího oddělení informatiky.

Poznámky: Obecně platí, že prozrazování jakýchkoliv hesel jiné osobě je přísně zakázáno. V tomto bodě se bere v úvahu možnost, že někdy v naléhavých případech existuje potřeba sdělit heslo třetí straně. Tato výjimka z obecného pravidla zakazujícího sdělování jakýchkoliv hesel vyžaduje souhlas vedoucího oddělení informatiky. Kvůli dodatečné ochraně by měla být odpovědnost za sdělování ověřovacích informací omezena na malou skupinku osob, které byly speciálně proškolené z oblasti ověřovacích postupů.

8.5 Elektronická média

Pokyn: Všechna elektronická média, obsahující informace, které nejsou určeny veřejnosti, by měla být fyzicky zamykána na bezpečném místě.

Poznámky: Smyslem tohoto bodu je předejít fyzické krádeži nosičů dat, obsahujících důvěrné informace.

8.6 Záložní kopie

Pokyn: Operátoři by měli ukládat záložní kopie do firemního trezoru nebo na jiné bezpečné místo.

Poznámky: Nosiče záložních kopií jsou další důležitý cíl počítačových útočníků. Vetřelec nebude ztrácet čas nabouráváním se do firemního systému, když nejslabším článkem mohou být nezabezpečené záložní kopie. Jakmile jsou zálohy ukradeny, má útočník k dispozici všechna důvěrná data, ledaže by byla data zašifrována. Proto je fyzické zabezpečení nosičů se zálohami nutné pro ochranu důvěrných firemních dat.

9. Pokyny pro všechny pracovníky

Část bezpečnostních pokynů platí pro všechny zaměstnance bez ohledu na to, jestli pracují v oddělení informatiky, v osobním oddělení, v účtárně či v údržbě. Tyto pokyny se dělí na následující kategorie: obecné, používání

počítače, používání elektronické pošty, pokyny pro vzdálené pracovníky, používání telefonu, používání faxu, používání hlasové pošty a hesla.

Obecné

9.1 Ohlašování podezřelých telefonátů

Pokyn: Pracovníci, kteří mají podezření, že se mohli stát obětí incidentu narušujícího bezpečnost (například obdrželi podezřelé žádosti o sdělení informací nebo o vykonání jisté činnosti na počítači), musejí tyto události bezodkladně ohlásit určené osobě či skupině.

Poznámky: Když se útočníkovi nepodaří oběť přesvědčit, aby konala podle jeho přání, bude se vždy snažit uspět u další osoby. Pokud pracovník ohlásí podezřelý telefonát nebo událost, učinil tak první krok ve vyhlášení pohotovosti pro případ opakovaného útoku. Proto jsou též jednotliví pracovníci v první linii obrany proti sociotechnickým útokům.

9.2 Dokumentování podezřelých telefonátů

Pokyn: V případě podezřelého telefonu, který vypadá jako možný sociotechnický útok, by se měl pracovník snažit získat od volajícího informace, které by mohly pomoci při odhalení, co je skutečným cílem útoku, a zapsat si tyto údaje do hlášení.

Poznámky: Po ohlášení incidentu příslušné skupině by mohly tyto podrobnosti pomoci zjistit cíl nebo vzorec, podle kterého probíhá útok.

9.3 Sdělování přístupových čísel

Pokyn: Personál firmy nemůže sdělovat přístupová telefonní čísla na modemy a měl by směrovat osoby, které o ně Žádají, na technickou pomoc nebo help desk.

Poznámky: Přístupová telefonní čísla musejí být považována za vnitřní informaci, která je určena pouze těm pracovníkům firmy, kteří tuto znalost potřebují ke své práci.

Sociotechnici často dotírají na zaměstnance či na oddělení, která si obvykle dělají menší starosti s ochranou držených informací. Například muže útočník zavolat na účtárnu a vydávat se za pracovníka telekomunikační firmy, který si chce ujasnit nějakou záležitost týkající se fakturace. Během řešení problému se zeptá na číslo faxu nebo na přístup do sítě. Vetřelec často doráží na zaměstnance, který si moc neuvědomuje nebezpečí spojené s prozrazením takovéto informace nebo není v tomto směru proškolený.

9.4 Firemní identifikátory

Pokyn: Všichni pracovníci firmy včetně vedení a managementu mají za povinnost nosit identifikátory.

Poznámky: Celé osazenstvo firmy i se členy vedení by mělo být proškoleno a motivováno tak, aby pochopili, že nošení identifikátorů je povinné v celém areálu firmy kromě míst volně přístupných veřejnosti a vlastní kanceláře.

9.5 Zastavování osob bez identifikátoru

Pokyn: Všichni pracovníci mají povinnost ihned zadržet neznámou osobu, která nemá identifikátor pracovníka nebo návštěvníka.

Poznámky: Žádná firma nechce dojít do situace, kdy pracovníci čekají na příležitost, aby mohli přistihnout kolegu mimo kancelář bez identifikátoru, na druhou stranu však každá firma, které záleží na ochraně vlastních informací, musí brát vážně nebezpečí spojená s výskytem so-ciotechnika na půdě firmy. Motivací pro pracovníky, kteří při snaze o stálé nošení identifikátorů pomáhají, může být zmínka ve firemním zpravodaji nebo na nástěnkách, pár hodin volna nebo pochvalný list založený do osobních spisů.

9.6 „Proklouzávání" (průchod přes zabezpečené vstupy)

Pokyn: Pracovníci přicházející do areálu firmy nemohou dovolit, aby za nimi vešla dovnitř neznámá osoba, když k otevření vstupu používají bezpečný identifikátor, jako je například magnetická karta.

Poznámky: Pracovníci si musejí uvědomit, že žádost o prokázání se namířená k cizí osobě, která se snaží vejít za nimi přes vstup, není ani v nejmenším projevem nedostatku slušnosti.

Sociotechnici se často pokouší proklouznout skrz branku těsně za osobou, která je oprávněná projít. Většina lidí nerada takové osoby zastavuje, protože předpokládají, že jsou s největší pravděpodobností pracovníky firmy. Při podobném postupu nese sociotechnik několik krabic a nic netušící pracovník mu ještě otevře dveře, aby mu pomohl.

9.7 Skartování důvěrných dokumentů

Pokyn: Důvěrné dokumenty určené na vyhození musejí být zničeny pomocí skartovačky s příčným řezem. Média (včetně pevných disků), která někdy v minulosti obsahovala důvěrné informace, musejí být zničena podle postupu určeného skupinou odpovědnou za bezpečnost informací.

Poznámky: Běžné skartovačky ničí dokumenty nepříliš důkladně. Skartovačka s příčným řezem (řeže ve dvou rovinách) je mění na drť. Nejlepším cvičením bezpečnosti je představit si, že šéf konkurenční firmy bude prohlížet materiály, které vyhazujeme a hledat jakékoliv informace, které by mu mohly pomoci.

Průmysloví špióni a hackeři pravidelně čerpají důvěrné informace z materiálů vyhozených na smetiště. Jsou známé případy uplácení uklízečích part konkurenčními firmami, které touží získat přístup k vyhazovanému smetí z firmy.

9.8 Osobní identifikační údaje

Pokyn: Osobní identifikační údaje jako zaměstnanecké číslo, číslo občanského průkazu, rodné číslo, datum a místo narození, dívčí jméno matky, by nikdy neměly sloužit jako prostředky ověřování totožnosti. Tyto údaje nejsou příliš chráněné a je možné je získat mnoha různými způsoby.

Poznámky: Sociotechnik je schopný za jistou cenu získat osobní identifikační data jiných osob. Vzdor panujícím představám je každý, kdo má kreditní kartu a přístup k Internetu, schopen získat tyto informace. Ale bez ohledu na zjevné ohrožení banky, úřady a telekomunikační firmy obyčejně tyto údaje používají. Z tohoto důvodu se krádež totožnosti stala v posledním desetiletí nejrychleji se rozvíjejícím kriminálním oborem.

9.9 Organizační schémata

Pokyn: Detaily uvedené na organizačních schématech podniků by neměly být prozrazovány nikomu kromě pracovníků firmy.

Poznámky: Informace o organizační struktuře firmy zahrnují organizační schémata, hierarchické vazby, seznamy pracovníků jednotlivých oddělení, jména zaměstnanců a jejich pracovní zařazení, vnitřní kontaktní čísla, zaměstnanecká čísla a podobné informace.

V první fázi sociotechnického útoku je cílem útočníka shromáždění informací o vnitřní struktuře společnosti. Tato informace dovoluje vytvořit strategii útoku. Útočník též může analyzovat tyto informace, aby určil, který pracovník může mít přístup k údajům, které shání. Během útoku tyto informace dovolují sociotechnikovi předstírat, že je zasvěcený pracovník, což zvyšuje pravděpodobnost, že získá spolupráci člověka, kterému volá.

9.10 Soukromé informace o pracovnících

Pokyn: Všechny žádosti o soukromé informace týkající se pracovníků musejí být nasměrované na personální oddělení.

Poznámky: Výjimkou z tohoto pravidla může být telefonní číslo pracovníka, se kterým je třeba se spojit v souvislosti s pracovními záležitostmi nebo který je určen jako „člověk na telefonu". Přesto je však lepší poznamenat si číslo volajícího a požádat hledaného pracovníka, aby mu zavolal zpátky.

10. Používání počítače

10.1 Zadávání příkazů

Pokyn: Personál firmy by nikdy neměl zadávat do počítače příkazy na žádost jiné osoby, ledaže by tato osoba byla ověřena jako pracovník oddělení informatiky.

Poznámky: Typickým sociotechnikovým kouskem je žádost o napsání příkazu, který mění konfiguraci systému a umožňuje útočníkovi přístup k počítači oběti bez ověřování nebo dovoluje získat informace potřebné k zahájení technologického útoku.

10.2 Vnitřní názvosloví

Pokyn: Pracovníci nemohou prozrazovat vnitřní názvy počítačových systémů nebo databází bez předchozí verifikace, zda je tazatel zaměstnancem firmy.

Poznámky: Sociotechnici se občas pokoušejí získat jména firemních počítačových systémů. Když už ta jména znají, telefonují do firmy a vydávají se za pracovníka, který má problém s přístupem k systému. Díky znalosti vnitřního jména systému získává sociotechnik u dotazovaného důvěru.

10.3 Žádosti o spuštění programu

Pokyn: Personál firmy by nikdy neměl spouštět žádnou aplikaci nebo program na žádost jiné osoby, pokud nebyla verifikována jako pracovník z oddělení informatiky.

Poznámky: Žádná žádost o spuštění programu, aplikace či vykonání nějaké činnosti na počítači nemůže být brána v potaz, pokud nebyl žadatel identifikován jako pracovník oddělení informatiky. Pokud se žádost váže s prozrazením tajných informací obsažených v souboru nebo zprávě elektronické pošty, musí být reakce v souladu s procedurou sdělování tajných informací (viz „Zpřístupňování informací").

Hackeři přesvědčují lidi, aby spouštěli programy, které umožňují převzetí kontroly nad systémem. Když nic netušící uživatel spustí program, který mu útočník podstrčil, může mu tím otevřít přístup do svého systému. Jiné

programy umožňují zaznamenávat činnost vykonávanou uživatelem a posílají nashromážděné informace útočníkovi. Během sociotechnického útoku je osoba podváděna, aby vykonala na počítači příkaz, který může způsobit škodu, kdežto během technologického útoku je podváděn operační systém, který vykonává příkazy způsobující analogické škody.

10.4 Stahování nebo instalace softwaru

Pokyn: Personál firmy nemůže stahovat a instalovat software na žádost jiných osob, pokud nebylo prokázáno, že jsou pracovníky oddělení informatiky.

Poznámky: Pracovníci by měli zachovat ostražitost vůči neobvyklým žádostem, které se týkají počítačů.

Obecně používanou sociotechnickou taktikou je zmanipulování oběti tak, aby si stáhla a nainstalovala program, který pomůže útočníkovi dosáhnout cíle, kterým je obvykle nabourání se do firemní počítačové sítě. V některých případech může takový program tajně špehovat uživatele nebo umožňovat útočníkovi převzetí kontroly nad počítačovým systémem díky vzdálenému příkazovému řádku.

10.5 Hesla a e-mail

Pokyn: Posílat e-mailem nešifrovaná hesla se nesmí.

Poznámky: Toto pravidlo může být opominuto internetovými obchody v jistých zvláštních okolnostech jako:

- zasílání hesla klientům, kteří se na stránce zaregistrovali,
- zasílám hesla klientům, kteří své heslo ztratili či zapomněli.

10.6 Bezpečnostní software

Pokyn: Personál firmy nemůže odstraňovat nebo deaktivovat žádný antivirový, firewallový ani jiný bezpečnostní software bez předchozího souhlasu oddělení informatiky.

Poznámky: Uživatelé občas deaktivují software chránici počítač, aby tím zrychlili jeho práci.

Sociotechnik může být schopen přesvědčit pracovníka, aby ukončil nebo smazal program, který je nezbytný pro ochranu systému před ohrožením bezpečnosti.

10.7 Instalace modemů

Pokyn: K počítači nelze připojovat žádné modemy bez předchozího souhlasu oddělení informatiky.

Poznámky: Je důležité si uvědomovat, že modem připojený k jednomu počítači může znamenat vážné nebezpečí pro celý systém, zvláště je-li tento počítač připojený do firemní sítě. Proto toto pravidlo reguluje připojování modemů.

Hackeři využívají techniku skenování čísel (*war dialing*), aby nalezli aktivní modemové linky v určitém rozsahu telefonních čísel. Stejná technika může sloužit k lokalizaci linek, ke kterým jsou připojeny modemy v areálu firmy. Útočník se může jednoduše nabourat do sítě, pokud identifikuje počítačový systém připojený na modem, na němž je spouštění vzdáleného příkazového řádku zabezpečené snadno uhodnutelným heslem nebo je úplně bez hesla.

10.8 Modemy a automatická odpověď

Pokyn: všechny počítače s připojenými modemy na půdě firmy musejí mít vypnutou funkci automatické odpovědi, aby se předešlo připojení nepovolané osoby k systému.

Poznámky: Všude, kde je to jen možné, by mělo oddělení informatiky pro ty pracovníky, kteří se potřebují připojovat přes modem do vnějších počítačových sítí, použít společný odchozí modem.

10.9 Crackerské nástroje

Pokyn: Je zakázáno stahovat si a používat jakékoli crackerské nástroje, které byly vytvořeny k překonávání systémových zabezpečení.

Poznámky: Na Internetu se nacházejí desítky stran věnovaných softwaru, který byl vytvořen k překonávání zabezpečení komerčních programů a programů typu shareware[25]. Používání těchto programů nejenže porušuje autorská práva k programu, ale je neobyčejně nebezpečné. Protože tyto programy pocházejí z neznámých zdrojů, mohou obsahovat tajný nebezpečný kód, který může způsobit škody na počítači nebo zavést trojského koně, který umožní autorovi programu přístup k počítači uživatele.

10.10 Posílání informací o firmě na síť

Pokyn: Pracovníci by neměli prozrazovat žádné podrobnosti týkající se zařízení a softwaru, který firma používá, v žádných diskusních fórech a podobně a ani by neměli sdělovat jiné kontaktní informace než uvádí příslušná procedura.

Poznámky: Každá zpráva poslaná do usenetu (tzv. newsů), internetových fór a mailing listů může být vyhledána s úmyslem shromáždit informace o firmě nebo o osobě, která se má stát cílem útoku. V této fázi může útočník prohledávat síť a pátrat po jakýchkoliv zprávách obsahujících užitečné informace o firmě, produktech či pracovnících.

Některé příspěvky obsahují velmi užitečné informace, které může útočník využít v další fázi útoku. Například správce sítě může poslat dotaz týkající se konfigurace filtrů firewallu konkrétního typu. Útočník, který tuto zprávu vypátrá, najde cennou informaci o konfiguraci firemního firewallu, který mu umožní firewall obejít a připojit se k podnikové síti.

Tento problém může být zredukován nebo odstraněn pokynem přikazujícím posílání příspěvků na diskusní skupiny z anonymních kont, které není možné spojit s firmou. Tento pokyn musí samozřejmě také zakazovat připojování jakýchkoliv kontaktních informací, které by mohly pomoci identifikovat firmu.

10.11 Diskety a další nosiče dat

Pokyn: Pokud jsou ponechána někde v kanceláři nebo na stole pracovníka média používaná na ukládám dat jako diskety nebo CD-ROM, která pocházejí z neznámého zdroje, nesmějí být vkládána do žádného počítače.

Poznámky: Jednou z metod, které útočníci používají, aby nainstalovali nebezpečný software, je podstrčení několika nosičů obsahujících takový software a označených lákavým nápisem (například „Seznam výplat – tajné!"). Pokud je nějaká disketa vložena do počítače a soubory jsou otevřeny,

---

[25] Pozn. překl.: Shareware je způsob šíření programů. Tyto programy, které si člověk může stáhnout třeba z Internetu nebo které najde na CD přiloženém k nějakému časopisu, mohou být dokonce i plně funkční, ale často jsou některé funkce omezené a pokud je uživatel spokojen, zašle autorovi či firmě poměrně nízký poplatek a získá registrační číslo, které program plně zprovozní nebo dostane plnou verzi. Oproti stále ještě tradovanému mýtu neznamená slovo „shareware" programy zadarmo.

nebezpečný program se tím spustí. Může otevřít „zadní vrátka", která umožňují dostat se do firemního systému nebo nějak jinak škodit.

10.12 Jak se zbavit datových nosičů

Pokyn: Před vyhozením datových nosičů, které někdy v minulosti obsahovaly důvěrné informace, je třeba nosič před vyhozením zcela odmagnetizovat nebo zničit, a to i když byla důvěrná data už před tím vymazána.

Poznámky: Zatímco skartace dokumentů je dnes už běžnou praxí, mohou pracovníci firmy podceňovat ohrožení spojené s vyhazováním nosičů, které někdy v minulosti obsahovaly důvěrné informace. Hackeři se mohou pokusit obnovit data, která byla na nosiči. Pracovníci možná předpokládají, že když smažou soubor, tak data zničili, ale tento předpoklad je zcela mylný a může vést k tomu, že se důvěrné informace ocitnou v nepovolaných rukou. Proto musejí být elektronická média, která obsahují nebo někdy v minulosti obsahovala důvěrné informace, znehodnocena nebo zničena metodami, které byly schváleny osobami, zodpovědnými za tuto oblast.

10.13 Šetříce obrazovek chráněné heslem

Pokyn: Všichni uživatelé si musejí nastavit v šetřičích obrazovky hesla a zapnout aktivaci šetřiče po uplynutí určité doby nečinnosti.

Poznámky: Všichni pracovníci jsou odpovědni za to, že si nastaví heslo v šetřiči a aktivaci šetřiče po nečinnosti, která není delší než 10 minut. Smyslem tohoto bodu je předcházet používání počítačů nepovolanými osobami. Navíc tento bod zabezpečuje firemní počítačový systém, kam by se mohl snadno dostat vetřelec, který se dostal do budovy.

10.14 Prohlášení o heslech

Pokyn: Před vytvořením nového konta by měl uživatel podepsat prohlášení, že si je vědom zákazu prozrazování hesel jiným osobám a že jej bude dodržovat.

Poznámky: Prohlášení by mělo obsahovat zmínku o tom, že nedodržování tohoto pravidla může vést k disciplinárnímu řízem, které může skončit i výpovědí.

11. Používání elektronické pošty

11.1 Přílohy

Pokyn: Přílohy k dopisům nesmějí být otevírané, kromě těch, které jsou očekávané a pocházejí od důvěryhodné osoby.

Poznámky: Všechny přílohy musejí být před otevřením důkladně prozkoumány. Lze vyžadovat, aby důvěryhodná osoba nejprve poslala upozornění, že za chvíli pošle přílohu. To omezuje riziko spojené se sociotechnickými útoky, které jsou založeny na poslání přílohy a přesvědčování v těle dopisu, abychom přílohu otevřeli.

Jeden ze způsobů, jak se nabourat do počítačového systému, spočívá v tom, že je pracovník zmanipulován, aby spustil nebezpečný program, který udělá průlom v systému a umožní k němu útočníkovi přístup. Tím, že útočník poslal e-mail s přílohou, která obsahuje program nebo makra, může být schopen získat kontrolu nad počítačem uživatele. Sociotechnik také může poslat nebezpečnou přílohu a potom oběti zavolat a přesvědčit ji, aby přílohu otevřela.

11.2 Automatické přesměrování na vnější adresu (autoforward)

Pokyn: Automatické přesměrování pošty na adresu mimo firmu je zakázané.

Poznámky: Účelem tohoto bodu je znemožnit vetřelci přijímat poštu poslanou na vnitřní e-mailovou adresu.

Pracovníci si občas nastavují přesměrování své příchozí pošty na vnější schránku, když mají být mimo své pracoviště. Útočník může zmanipulovat pracovníka, aby si nastavil přesměrování z firemní schránky na vnější. A pak se může vydávat za pracovníka firmy a žádat o vyslání důvěrných informací na tuto vnitřní adresu.

11.3 Přeposílání pošty (forward)

Pokyn: Všechny požadavky neprověřených osob o předání elektronického dopisu jiné neověřené osobě vyžadují kontrolu totožnosti žadatele.

11.4 Verifikace pošty

Pokyn: Elektronická zpráva, která se zdá pocházet od důvěryhodné osoby a obsahuje žádost o sdělení důvěrných informací nebo o vykonání činnosti na počítači, vyžaduje dodatečné formy autentikace (viz „Ověřovací a autorizační procedury").

Poznámky: Útočník může jednoduše zfalšovat e-mail a jeho hlavičky, aby vypadal, jako že pochází z jiné adresy. Útočník může poslat také zprávu ze stroje, do kterého se naboural už dříve, čímž si zajistil falešné oprávnění k příjmu důvěrných informací a k vykonávání činností. Ani analýza hlaviček dopisu pak nedovolí odhalit, že dopis byl poslán z už ovládnutého počítačového systému.

12. Používání telefonu

12.1 Účast v telefonických průzkumech

Pokyn: Pracovníci se nemohou účastnit telefonických průzkumů a nemohou odpovídat na žádné otázky osob či organizací zvenčí. Žádosti tohoto typu je třeba směrovat na oddělení public relations nebo na určenou osobu.

Poznámky: Jednou z metod, které sociotechnici používají během útoku na organizaci, je telefonát zaměstnanci se žádostí o účast v anketě. Je až zarážející, kolik lidí ochotně poskytuje informace o sobě nebo o firmě, ve které pracují, úplně cizím lidem, když uvěří, že jde o anketu. Tazatel propašuje mezi nevinné otázky i několik pro něj klíčových a takto získané informace mu mohou pomoci dostat se do firemní sítě.

12.2 Poskytování vnitřních telefonních linek

Pokyn: Pokud neověřená osoba žádá pracovníka o jeho telefonní linku, pracovník musí posoudit, jestli je poskytnutí telefonu opravdu nutné.

Poznámky: Účelem této instrukce je vyžadovat od zaměstnanců promyšlená rozhodnutí, jestli je sdělení jejich telefonní linky nezbytné. Když žádost o kontaktní číslo přichází od osoby, která nemá zvláštní důvod znát vnitřní linku, je nejlepší požádat ji, aby volala přes ústřednu.

12.3 Zanechávání hesel v hlasové schránce

Pokyn: Zanechávat v hlasové schránce zprávy obsahující hesla je zakázáno.

Poznámky: Sociotechnik často dokáže získat přístup do hlasové schránky zaměstnance, protože je slabě zabezpečena snadno uhodnutelným přístupovým kódem. Rafinovaný hacker je schopen si vytvořit vlastní falešnou hlasovou schránku a přesvědčit pracovníka, aby mu tam zanechal informace týkající se hesel. Tento pokyn takovým uskokům zabraňuje.

13. Používání faxu

13.1 Předávání faxu

Pokyn: Přijímání a předávání faxu třetím osobám je zakázáno bez ověření totožnosti osoby, která s takovou žádostí přichází.

Poznámky: Zloději informací mohou přesvědčit zaměstnance, aby poslal důvěrné informace na fax, který se nachází ve firmě. Ještě než uvede své oběti číslo faxu, telefonuje podvodník nic netušící sekretářce či asistentce a ptá se, jestli by pro něj mohla přijmout fax, který by si později vyzvedl. Jakmile sekretářka přijme fax, útočník jí znovu volá a prosí, jestli by nemohla fax předat dál, protože ho, například, naléhavě potřebuje na důležité jednání. Protože osoba, která je žádána o předání faxu dále, si obvykle neuvědomuje hodnotu informací, obyčejně bez ptaní činí to, oč byla požádána.

13.2 Ověření instrukcí obdržených faxem

Pokyn: Před vykonáním jakékoliv instrukce obdržené faxem musí být odesílatel ověřený jako pracovník nebo jiná důvěryhodná osoba. K ověření žádosti obvykle postačuje telefonát odesílateli.

Poznámky: Pracovníci si musejí neustále dávat pozor na neobvyklé žádosti o zadání příkazů do počítače nebo o sdělení nějakých informací. Údaje v hlavičce faxu mohou být zfalšované změnou nastavení faxu, ze kterého byl dokument poslán. Proto také hlavička faxu nemůže být nástrojem zjišťování či ověřování totožnosti odesilatele.

13.3 Posílání důvěrných informací faxem

Pokyn: Před odesláním důvěrných informací na fax, který se nachází na místě, které je dostupné i jiným pracovníkům, by odesílatel měl poslat titulní stranu. Příjemce po obdržení titulní strany pošle odpověď, která dokazuje, že je fyzicky přítomen u přístroje. Teprve pak odesílatel faxuje zbytek.

Poznámky: Tato potvrzující procedura ujišťuje odesílatele, že je příjemce na druhé straně fyzicky přítomen. Kromě toho tento proces slouží jako kontrola, jestli nebylo číslo faxu přesměrováno někam jinam.

13.4 Zákaz faxování hesel

Pokyn: Hesla nesmějí byt pod žádnou záminkou faxována.

Poznámky: Posílání ověřovacích informací faxem není bezpečné. K většině faxu má přístup větší skupina lidí. Kromě toho faxy využívají veřejnou telefonní ústřednu, kde lze zavést přesměrování telefonního čísla přijímacího přístroje tak, aby faxy šly do rukou útočníka.

14. Používání hlasové pošty

14.1 Hesla hlasových schránek

Pokyn: Hesla chránící schránky hlasové pošty nemohou byt pod žádnou záminkou prozrazována. Navíc se tato hesla musejí měnit alespoň jednou za 50 dnú.

Poznámky: Zprávy zanechané v hlasové poště mohou obsahovat důvěrné inforamce. Proto by si pracovníci měli často měnit své heslo a nikomu by ho neměli sdělovat. Kromě toho by uživatelé neměli používat stejné nebo podobné heslo dříve než po uplynutí 12 měsíců od jeho posledního použití.

14.2 Hesla ve více systémech

Pokyn: Uživatelé hlasové pošty by neměli používat stejné heslo v žádném jiném telefonickém nebo počítačovém systému, ať už firemním, nebo soukromém.

Poznámky: Používání stejných nebo podobných hesel ve více systéme například v hlasové schránce a na počítači, usnadňuje sociotechnikovi odhadnutí ostatních hesel uživatele po uhodnutí jednoho.

14.3 Výběr hesla pro hlasovou poštu

Pokyn: Uživatelé a administrátoři hlasové pošty si musejí vymýšlet hesla, která lze těžko uhodnout. Nemohou být v žádném vztahu k osobě, která je používá, ani k firmě a neměla by obsahovat snadno uhodnutelné šablony.

Poznámky: Hesla nemohou obsahovat posťupky nebo opakující se číslice (například 1111, 1234, 1010), nemohou být stejná či podobná jako je telefónní linka schránky a nemohou se vztahovat k adrese, poštovnímu směrovacímu číslu, datu narození, státní poznávací značce, telefonnímu číslu, hmotnosti, IQ či jiným osobním informacím.

14.4 Zprávy označené jako „staré"

Pokyn: Pokud nejsou zprávy, které jsme si ještě nevyslechli, označeny jako „nové", musí být správce hlasové pošty informován o podezření na vloupání se do hlasové schránky a heslo musí být neprodleně změněno.

Poznámky: Sociotechnici mohou získat přístup k hlasovým schránkám několika různými způsoby. Pracovník, který si všimne, že zprávy, které slyší poprvé, nejsou označené jako nové, musí předpokládat, že někdo získal přístup k jeho schránce a poslechl si zprávy dříve než on.

14.5 Úvodní zpráva v hlasové schránce

Pokyn: Pracovníci firmy by měli omezit sdělování informací v nahraných úvodních vzkazech hlasové pošty. Neměly by být sdělovány informace spojené s rozvrhem dne nebo plánováním cesty.

Poznámky: Externí uvítání (přehrávané lidem volajícím zvenku) by nemělo obsahovat jméno, telefonní linku, důvod nepřítomnosti (služební cesta, dovolená, rozvrh dne), protože útočník by mohl takovou informaci využít k vytvoření přesvědčivé historky, aby mohl zmanipulovat jiné lidi.

14.6 Hesla podle šablon

Pokyn: Uživatelé hlasové pošty by si neměli dávat heslo, kde jedna část zůstává beze změny a druhá se mění podle předvídatelného vzorce.

Poznámky: Nelze například používat hesla 743501, 743502, 743503 atd., kde poslední dvě číslice představují číslo aktuálního měsíce.

14.7 Tajné nebo soukromé informace

Pokyn: Tajné a soukromé informace nemohou být hlasovou poštou předávány.

Poznámky: Telefonní systém je obvykle hůř zabezpečený než systém počítačový. Jako hesla jsou převážně řetězce číslic, což značně omezuje množství možných kombinací. Navíc mohou být v některých organizacích hesla zpřístupněná sekretářkám nebo dalším administrativním silám, které mají za povinnost přijímat vzkazy určené šéfovi. Z tohoto důvodu by se v hlasové poště neměly zanechávat tajné informace.

15. Hesla

15.1 Hesla a telefony

Pokyn: Pod žádnou záminkou nesmějí byt hesla sdělována po telefonu.

Poznámky: Útočníci si mohou najít způsob, jak odposlouchávat hovory osobně nebo pomocí nějakého technologického řešení.

15.2 Sdělování přístupových hesel k počítačům

Pokyn: Počítačový uživatel nemůže nikomu pod žádnou záminkou sdělit své heslo bez písemného souhlasu odpovědného vedoucího z oddělení informatiky.

Poznámky: Cílem mnoha sociotechnickych útoků je zmanipulovat pracovníka tak, aby sdělil své uživatelské jméno a heslo. Tato instrukce znamená velký krok směrem k omezení hrozby úspěšného sociotechnického útoku na firmu. Proto také musí být v celé firmě přísně dodržována.

15.3 Internetová hesla

Pokyn: Pracovníci nemohou na internetových stránkách nikdy používat stejná nebo podobná hesla, jako mají ve firemním počítačovém systému.

Poznámky: Podvodníci mohou na Internetu vytvořit stránku, kde mají nějakou lákavou nabídku a možnost výher. Při registraci musí návštěvník stránek uvést e-mail, uživatelské jméno a heslo. Protože mnoho lidí používá při registraci na různých stránkách stejné nebo podobné informace, autor této stránky se bude pokoušet použít zvolené heslo a jeho varianty při útoku na domácí nebo firemní počítačový systém dané osoby. Počítač, který tato osoba používá v práci, lze občas identifikovat pomocí e-mailové adresy, která byla uvedena při registraci.

15.4 Hesla ve více systémech

Pokyn: Personál firmy nikdy nemůže používat stejné nebo podobné heslo ve větším počtu systémů. Tento bod se týká různých typu zařízení (počítač, hlasová pošta), různých lokalit (práce, domov), různých systémových zařízení (*router, firewall*) nebo různých programu (databáze/aplikace).

Poznámky: Útočníci, kteří se nabourávají do počítačových systémů a sítí, využívají vlastností lidské povahy. Vědí, že mnoho lidí používá stejná nebo podobná hesla v každém systému, kam mají přístup, aby se vyhnuli potížím s pamatováním několika hesel. Nejprve se bude vetřelec snažit prolomit heslo na jednom ze systémů, kde má daná osoba účet. Je velmi pravděpodobné, že stejné heslo nebo jeho obměna otevře přístup k jiným zařízením a systémům, které tato osoba používá.

15.5 Opakované používání stejných hesel

Pokyn: Žádný uživatel nemůže znovu použít stejné nebo podobné heslo dříve než po osmnácti měsících od jeho posledního použití.

Poznámky: Pokud se útočníkovi podaří odhalit heslo uživatele, jeho časté změny snižují velikost potenciálních škod. Nová hesla, která nemají žádný vztah k předchozím, jsou hůře uhodnutelná.

15.6 Hesla podle šablon

Pokyn: Uživatelé si nemohou dávat heslo, kde jedna část zůstává beze změny a druhá se mění podle předvídatelného vzorce.

Poznámky: Nelze například používat hesla Kevin01, Kevin02, Kevin03 atd., kde poslední dvě číslice znamenají číslo aktuálního měsíce.

15.7 Volba hesel

Pokyn: Počítačoví uživatelé by si měli volit hesla, která vyhovují následujícím požadavkům:

- Musí se skládat z alespoň osmi znaků v případě běžného uživatelského účtu a alespoň dvanácti znaků u privilegovaných kont.
- Musí obsahovat alespoň jednu číslici, alespoň jeden symbol (například, $, _, %, !), alespoň jedno malé a alespoň jedno velké písmeno (pokud to umožňuje operační systém).
- Nemůže to být žádný výraz z libovolného jazyka, výraz spojený s rodinou, koníčkem, autem, prací, registračními značkami, rodným číslem, jménem psa či jiného domácího mazlíčka, datem narození, ani to nemůže být fráze obsahující tyto výrazy.
- Nemůže to být obměna předchozího hesla s jednou částí neměnnou a s druhou měnící se například podle aktuálního měsíce: Kevin01, Kevin02, Kevin03 nebo KevinLeden, KevinUnor, KevinBrezen.

Poznámky: Heslo vytvořené při dodržování výše uvedených směrnic bude pro sociotechnika těžkým oříškem. Jinou možností je použití metody souhláska-samohláska, díky které obdržíme heslo, které jde snadno vyslovit i zapamatovat. K sestrojení takového hesla můžeme použít šablonu „XYXYXYXY", kde místo X budeme dávat souhlásky a Y nahradíme samohláskami. Příkladem by mohla být hesla MIXOCASO, CUSOJEMA.

15.8 Zapisování si hesel

Pokyn: Pracovníci si mohou poznamenat heslo jen tehdy, pokud je mají uschováno na bezpečném místě daleko od počítače nebo jiného heslem chráněného zařízení.

Poznámky: Zaměstnanci by měli být odrazováni od zapisování si hesel. Někdy je to však bohužel nutné, například když má pracovník mnoho kont na různých systémech. Každé poznamenané heslo musí být uložené na bezpečném místě daleko od počítače. V žádném případě se nesmí heslo schovávat pod klávesnici nebo dokonce mít papírek s heslem přilepený na monitoru.

15.9 Hesla ve formě prostého textu

Pokyn: Hesla ve formě prostého textu by neměla být uložená v žádném souboru na počítači nebo jako text objevující se po stisku funkční klávesy. V případě

nutnosti lze hesla zapsat pomocí šifrovacího nástroje schváleného oddělením informatiky a vyhnout se tím hrozbě, že heslo odhalí neoprávněná osoba.

Poznámky: Pokud jsou hesla uložená v nešifrované formě v datovém souboru, dávkovém souboru, přístupná pod funkčními klávesami, logovacích souborech, makrech, skriptech nebo v souborech obsahujících hesla na ftp servery, může se k nim útočník dostat.

16. Pokyny pro vzdálené uživatele

Vzdálení uživatelé se nacházejí mimo ochranu firemního firewallu a jsou proto zranitelnější. Zde jsou popsány pokyny, které by měly sociotechnikům znemožnit využívat vzdálené pracovníky jako brány k vašim datum.

16.1 Tenký klient

Pokyn: Všichni pracovníci, kteří jsou oprávněni používat vzdálený přístup, by se měli připojovat pomocí *tenkého klienta.*

Poznámky: Když si útočník vybírá strategii útoku, může se rozhodnout k identifikaci uživatelů se vzdáleným přístupem. Ti jsou prvním cílem útoku. Jejich počítače nejsou obvykle dobře zabezpečené a mohou být slabým článkem, který umožní přístup k firemní síti.

Každému počítači, který se připojuje k důvěrné síti, lze podstrčit program, který skenuje klávesnici, nebo se zmocnit jeho autentikovaného připojení. Abychom se tomuto problému vyhnuli, lze použít strategii *tenkého klienta.* Tenký klient připomíná bezdiskovou pracovní stanici nebo „hloupý" terminál (*dumb terminál*). Vzdáleny počítač nemá disky – operační systém a aplikační programy sídlí ve firemní počítačové síti. Přístup k síti pomocí tenkého klienta značně snižuje riziko, které představuje používání „nezalátaných" operačních systémů a nebezpečné programy. V souladu s tím je řízení bezpečnosti vzdálených uživatelů díky jeho centralizaci snazší a účinnější. Než abychom se spoléhali na to, že nezkušení vzdálení uživatelé budou schopni pečovat o bezpečnost svého systému, je lepší přenést tuto zodpovědnost na patřičně vyškolené správce sítě.

16.2 Zabezpečovací software pro vzdálené uživatele

Pokyn: V každém externím počítačovém systému, který slouží k připojování se k firemní síti, musí být nainstalován antivirový software, který odhaluje i trojské koně, a firewall (softwarový nebo hardwarový). Definice virů musejí být aktualizovány alespoň jednou týdně.

Poznámky: Obvykle vzdálení uživatele neprocházejí školením z bezpečnosti a mohou neúmyslně nebo lehkomyslně ponechat své počítače vystavené různým útokům. Proto právě vzdálení uživatelé představují pro bezpečnost firmy velké ohrožení, pokud nejsou patřičně proškoleni. Kromě instalace antivirového programu je kvůli nebezpečným programům nutný i firewall, který by zablokoval nepřátelským uživatelům přístup ke službám běžícím na počítači vzdáleného uživatele.

Jak dokazuje útok na firmu Microsoft, není vhodné brát na lehkou váhu riziko způsobené nepoužíváním minimálních bezpečnostních prostředků, které by nám pomohly vyhnout se šíření malwaru. Počítačový systém jednoho ze vzdálených uživatelů vnitřní sítě firmy Microsoft byl infikován trojským koněm. Vetřelec nebo vetřelci byli schopni využít připojení onoho vzdáleného uživatele k vývojářskému systému ke krádeži zdrojového kódu.

17. Pokyny pro personální útvar

Personální oddělení má zvláštní povinnost chránit pracovníky před osobami, které se pokoušejí získat osobní údaje zaměstnanců. Odborníci z personálního odpovídají rovněž za ochranu firmy před nespokojenými bývalými pracovníky.

17.1 Odchod pracovníků z firmy

Pokyn: Když nějaký pracovník odchází z firmy, personální útvar musí bezodkladně:

- odstranit jméno této osoby z telefonního seznamu, který je na vnitřní síti a zablokovat či přesměrovat jeho hlasovou poštu;
- informovat personál hlídající vstupy do budov firmy;
- dodat jméno pracovníka do seznamu odcházejících, který by měl být rozesílán všem pracovníkům alespoň jednou týdně.

Poznámky: Pracovníci, kteří hlídají vchody do budov by měli být informováni, aby nevpouštěli bývalého zaměstnance do areálu firmy. Informování ostatního personálu může zmařit pokusy propuštěného předstírat, že je zde stále zaměstnán a zmařit tak i případné pokusy o sabotáž za nevědomé pomoci zaměstnanců.

V jistých případech je nutné doporučit všem pracovníkům z oddělení propuštěné osoby, aby si změnili hesla. (Když jsem byl propuštěn z GTE z důvodu mé hackerské pověsti, firma nařídila změnu hesla všem zaměstnancům.)

17.2 Informování oddělení informatiky

Pokyn: Vždy, když firma někoho propouští, měl by o tom personální útvar neprodlené uvědomit oddělení informatiky, aby byla zrušena jeho konta včetně kont k databázím a k připojování se přes modem či Internet ze vzdálených lokalit.

Poznámky: Velmi důležitá je deaktivace všech možných přístupů bývalého pracovníka do firemních počítačových systémů, síťových zařízení, databází a podobně hned v okamžiku jeho propuštění. Pokud to firma neudělá, nechává otevřené dveře nespokojeným bývalým zaměstnancům, kteří se tak mohou dostat do systému a způsobit značné škody.

17.3 Důvěrné informace používané při náboru

Pokyn: Inzerce a jiné formy veřejného náboru kandidátů na volná pracovní místa by se měly pokud možno vyhýbat identifikaci počítačového zařízení a softwaru, který firma používá.

Poznámky: Vedení a zaměstnanci personálního oddělení by měli sdělovat jen tolik informací o hardwarovém a softwarovém vybavení, které firma používá, kolik je nutné, aby obdržela přihlášky od patřičně kvalifikovaných uchazečů.

Hackeři čtou noviny, informace publikované firmami a navštěvují internetové stránky, aby našli seznam pracovních nabídek. Firmy často sdělují hodně informací o používaném zařízení a programovém vybavení, aby povzbudily potenciální uchazeče. Vetřelec, který se dozvěděl o informačních systémech firmy, je připraven k druhé fázi útoku. Například se znalostí, že firma používá systém VMS, může útočník uskutečnit telefonát, aby vymámil číslo používané verze systému, a následně poslat falešný servis pack, který zdánlivě pochází od výrobce systému. Po jeho nainstalování je útočník uvnitř.

17.4 Osobní údaje pracovníka

Pokyn: Osobní oddělení nemůže sdělovat osobní údaje zaměstnanců současných ani bývalých, pracovníků na dohodu, konzultantů, brigádníků, ledaže by dotyčný pracovník nebo šéf personálního k tomu předem dali písemný souhlas.

Poznámky: Lovci mozků, soukromí detektivové a zloději totožností často shánějí osobní údaje pracovníka, jako jsou zaměstnanecké číslo, rodné číslo, datum narození, historie výplat, finanční údaje včetně informací o spoření a údaje o pojištění a zdravotním stavu.

Sociotechnik se díky těmto informacím může vydávat za danou osobu. Jména nových zaměstnanců mohou kromě toho být cennou kořistí pro zloděje informací. Noví pracovníci se obvykle podřizují žádostem osob s vyšším postavením a větší mocí a každé osoby, která prohlásí, že má na starosti bezpečnostní záležitosti.

17.5 Prověrky pracovníků

Pokyn: Minulost každého nově přijatého pracovníka, konzultanta i brigádníka by měla být před tím, než jim bude nabídnuta smlouva, prověřena.

Poznámky: S ohledem na náklady lze průzkum omezit na některé pracovní funkce, kde se musejí nacházet spolehliví lidé. Na druhou stranu je třeba mít na paměti, že každá osoba, které poskytujeme fyzický přístup do kanceláří, znamená potenciální ohrožení. Například uklízeči mají přístup do kanceláří zaměstnanců a tím pádem také k jejich počítačům. Útočník, který má fyzický přístup k počítači, může během jedné minuty nainstalovat program snímající klávesnici a tedy také hesla.

Počítačoví vetřelci jsou občas připraveni nechat se ve firmě zaměstnat, aby získali přístup k počítačovým systémům a k síti. Útočník může jednoduše získat jméno firmy, která v organizaci uklízí. Může například zatelefonovat osobě, která má tyto záležitosti na starosti a vydávat se za zástupce obdobné úklidové firmy, aby získal jméno společnosti, která v současné době uklízí v organizaci, která ho zajímá.

18. Pokyny týkající se fyzického zabezpečení

Sociotechnici se sice snaží osobně se neukazovat ve firmách, na které se chystají zaútočit, ale občas se stávají nějaké výjimky. Zde uvedené pokyny pomohou ochránit firmu před takovým ohrožením.

18.1 Identifikace osob nezaměstnaných v organizaci

Pokyn: Dodavatelé či jiní lidé, kteří ve firmě nejsou zaměstnáni a kteří potřebují pravidelně vstupovat do areálu firmy, musejí mít speciální identifikátory nebo jinou formu identifikace podle pokynů stanovených útvarem ochrany dané firmy.

Poznámky: Osoby ve firmě nezaměstnané, které musejí pravidelně docházet do firmy (například dodavatelé potravin a nápojů do kantýn, technici od kopírek nebo telefonní technici), by měly dostat k těmto účelům vytvořené identifikátory. Jiné osoby, které potřebují jít do firmy jen občas nebo jednorázově, musejí být pokládány za hosty a měly by jít vždy s doprovodem.

18.2 Identifikace návštěvníků

Pokyn: Každý návštěvník musí ukázat občanský průkaz nebo jiný doklad s fotografií, aby mohl být vpuštěn dovnitř.

Poznámky: Pracovníci ochrany nebo recepční by měli udělat kopii dokladu totožnosti než vydají identifikátor. Kopie by měla být uložena v návštěvní knize. Alternativně mohou strážní či recepční zapisovat identifikační údaje do knihy návštěv. Nemělo by se návštěvníkům dovolovat, aby své údaje do knihy zapisovali sami.

Sociotechnici, kteří hledají možnost vstupu do budovy, budou do knihy vždy zapisovat falešné údaje. Přestože získání falešné totožnosti a zapamatování si jména pracovníka, kterého navštěvujeme, není těžké, dodává požadavek registrace vcházejících osob ještě jeden prvek do systému bezpečnosti.

18.3 Doprovázení návštěvníků

Pokyn: Návštěvníci musejí být po celou dobu doprovázeni nebo musejí pobývat ve společnosti zaměstnance firmy.

Poznámky: Jeden z oblíbených sociotechnických triků je domluvit si schůzku s jedním pracovníkem firmy (například s výrobním inženýrem pod záminkou, že je pracovníkem strategického partnera firmy). Na místo jednání ho dovede doprovod, ale po schůzce sociotechnik ujišťuje, že cestu ven najde sám. Tímto způsobem získává sociotechnik volnost pohybovat se po budovách firmy a možnost získat důvěrné informace.

18.4 Dočasné identifikátory

Pokyn: Pracovníci firmy z jiné lokality, kteří u sebe nemají identifikátor, se musejí prokázat platným občanským průkazem nebo jiným dokladem s fotografií, aby mohli dostat dočasný identifikátor návštěvníka.

Poznámky: Útočníci se často vydávají za zaměstnance z jiné lokality firmy, aby se dostali do areálu.

18.5 Evakuace

Pokyn: Během ohrožení nebo evakuačních cvičení se musí ochranka ujistit, že všichni opustili areál firmy.

Poznámky: Personál odpovědný za bezpečnost musí ohlídat, jestli v kancelářích nebo na toaletách nezůstali nějací opozdilci. Po získání souhlasu hasičů nebo jiné osoby odpovídající za průběh evakuace musí ochranka zkontrolovat, jestli někdo nezůstává v budově dlouho po evakuaci.

Průmysloví špioni nebo rafinovaní hackeři jsou schopni způsobit diverzi, aby získali přístup do zabezpečených prostor firmy. Jednou z používaných forem diverze je rozprašovat do vzduchu nějaký neškodný prostředek, který vyvolává dojem, že uniká plyn. Jakmile se začne osazenstvo firmy evakuovat, útočník se bude pokoušet ukrást nějaké informace nebo se dostat do firemního počítačového systému. Jiná taktika je zůstat v úkrytu, například na toaletách nebo ve skříni, v době plánovaných evakuačních cvičení nebo po zapálení dýmovnice či po podobné akci, která může vyvolat evakuaci lidí z budovy.

18.6 Návštěvníci v podatelně

Pokyn: Vpouštět návštěvníky do podatelny bez dozoru pracovníka firmy není dovoleno.

Poznámky: Smyslem této instrukce je předejít záměně, podstrčení nebo krádeži vnitřní korespondence firmy.

18.7 Registrační značky

Pokyn: Pokud má firma hlídané parkoviště, měli by hlídači zapisovat čísla registračních značek (dříve státních poznávacích značek) automobilů vjíždějících na parkoviště.

18.8 Popelnice

Pokyn: Odpadkové kontejnery musejí být po celou dobu v areálu firmy a neměly by být volně přístupné.

Poznámky: Hackeři a průmysloví špioni dokáží získat z firemních popelnic cenné informace. Americké soudy se drží zásady, že odpadky jsou opuštěný majetek a jejich prohledáváni je zcela legální. Proto je důležité, aby se odpadkové nádoby nacházely na území firmy, kde je má firma právo chránit i s obsahem.

19. Pokyny pro recepční

Recepční jsou často při kontaktech se sociotechnikem první na ráně, ale jsou jen zřídka školené, aby uměly rozpoznat a zadržet vetřelce. Zde uvedené zásady pomohou recepčním lépe chránit firmu a její data.

19.1 Vnitřní telefonní seznam

Pokyn: Sdělování informací uvedených ve vnitřním telefonním seznamu by mělo být omezeno pouze na pracovníky firmy.

Poznámky: Všechna jména, funkce, telefonní čísla a adresy obsažené v telefonním seznamu by měly být pokládány za vnitřní informace a měly by být sdělovány podle instrukcí popisujících klasifikaci dat a sdělování vnitřních informací.

Navíc musí volající znát jméno nebo linku pracovníka, se kterým se chce spojit. Recepční sice může přepojit hovor na někoho, koho volající nezná, ale pak nemůže sdělovat jeho linku. (Zvědavcům, kteří se chtějí učit na konkrétních příkladech, doporučuji získat vlastní zkušenost zavoláním na nějakou státní instituci a zeptat se telefonistky na nějakou linku.)

19.2 Telefonní čísla na specifické útvary či skupiny

Pokyn: Pracovníci by neměli nikomu sdělovat přímá čísla na technickou podporu, telekomunikační oddělení, počítačové operátory nebo správce systému bez ověření skutečné potřeby kontaktu s těmito osobami. Recepční, která přepojuje hovory některé z těchto osob, by měla uvést jméno volající osoby.

Poznámky: Ačkoliv se může zdát tento pokyn příliš přísný, ztěžuje sociotechnikovi vydávat se za zaměstnance firmy tak, že navede skutečného pracovníka, aby hovor přepojil dál (v některých telefonních systémech je takový hovor brán už jako vnitřní), nebo demonstrovat svou znalost vnitřních linek a předstírat tak autentičnost.

19.3 Vzkazy

Pokyn: Telefonistky a recepční by neměly přijímat vzkazy nebo předávat informace jménem neznámých osob.

Poznámky: Sociotechnik je schopen zmanipulovat nějakou osobu tak, aby se neúmyslně zaručila za jeho totožnost. Jeden z typických triků je získat telefonní číslo recepční a poprosit ji, aby přijala vzkazy, které by nám mohly přijít. Později během telefonického rozhovoru s obětí se útočník vydává

za pracovníka, žádá o důvěrné informace nebo o vykonání nějakého úkolu a jako zpáteční číslo sdělí číslo na recepci. Útočník si později na recepci zavolá a nechá si přečíst vzkazy, které pro něj zanechala nic netušící oběť podvodu.

19.4 Věci k vyzvednutí

Pokyn: Před vydáním jakékoliv věci kurýrovi nebo jiné neověřené osobě musí recepční nebo strážný vidět doklad totožnosti s fotografií a zapsat podle schválených pokynů údaje z průkazu do výdejní knihy.

Poznámky: Jednou se sociotechnických taktik je přesvědčit pracovníka, aby předal důvěrné informace jinému, zřejmě oprávněnému zaměstnanci k vyzvednutí v recepci. Recepční nebo strážný samozřejmě předpokládají, že zásilku mají vydat tomu, kdo se o ni přihlásí. Sociotechnik se bud přihlásí osobně, nebo využije služeb kurýra, který pro něj zásilku vyzvedne.

20. Pokyny pro útvar přijímající hlášení incidentů

Každá firma by měla učit centrální skupinu, která má být informována v případě odhalení nějaké formy ohrožení bezpečnosti firmy. Níže jsou uvedeny směrnice týkající se vytvoření útvaru a jeho úkolů.

20.1 Ohlašovací místo

Pokyn: Je třeba určit osobu nebo skupinu, které budou oznamovány všechny incidenty narušující bezpečnost firmy. Všichni pracovníci by měli být vybaveni kontaktními informacemi na tuto skupinu.

Poznámky: Pracovníci musejí chápat, jak identifikovat ohrožení bezpečnosti a musejí být vyškolení, aby ohlašovali všechna vzniklá ohrožení na ohlašovací místo. Stejně důležité je vytvoření procedur popisujících činnost útvaru v případě obdržení oznámení o ohrožení.

20.2 Probíhající útoky

Pokyn: Pokud útvar ochrany přijme hlášení o probíhajícím sociotechnickém útoku, měl by neodkladně zahájit kroky k varování všech pracovníků, kteří patří do ohrožených skupin.

Poznámky: Skupina, které jsou hlášeny incidenty, nebo by její vedoucí měl přijmout rozhodnutí, zda vydat v celé firmě varování. Pokud jsou odpovědné osoby přesvědčené, že probíhá útok, musí být za účelem předejití eventuálním škodám prioritou varování pracovníků, aby si dávali pozor.

Přílohy

Bezpečnost v kostce

Dále uvedené seznamy a tabulky představují přehled sociotechnických metod probíraných v kapitolách 2 až 14 a ověřovacích procedur diskutovaných v 16. kapitole. Tyto informace je třeba upravit podle potřeb vlastní organizace a zpřístupnit pracovníkům, aby je mohli v příslušných situacích použít.

Identifikace útoku

Zde uvedené tabulky a body pomohou zjistit, zda probíhá sociotechnický útok.

Sociotechnický cyklus

Činnost	Popis
Průzkum	Muže se začít od zevrubné analýzy volně přístupných informací jako jsou finanční výsledky, katalogy, patentové přihlášky, články v odborném tisku, obsah internetových stránek a také obsah popelnic.
Budování vztahů a důvery	Používání vnitřních informací, vydávám se za někoho a jiného, zmiňování jmen, která oběť zná, žádosti o pomoc nebo vyvolávání dojmu autority.
Využití důvěry	Žádost o informaci nebo o činnost, adresovaná oběti. Zmanipulování oběti, aby sama poprosila o pomoc.
Využití informace	Pokud je získaná informace pouze dalším krokem přibližujícím útočníka k cíli, vrací se k předchozím bodům cyklu tak dlouho, dokud nedosáhne svého cíle.

Typické sociotechnické metody

- Vydávání se za pracovníka téže firmy.
- Vydávání se za zástupce dodavatele, partnerské firmy nebo státního úřadu.
- Vydávání se za někoho, kdo má moc.
- Vydávání se za nového pracovníka, který prosí o pomoc.
- Vyydávání se za představitele či dodavatele operačního systému a doporučování neodkladné aktualizace.
- Nabízení pomoci v případě nějakého problému, vyvolání tohoto problému a ovlivnění oběti, aby sama zatelefonovala s prosbou o pomoc.
- Zaslání bezplatné aktualizace programu k instalaci.
- Zaslání viru nebo trojského koně v příloze pošty.
- Použití falešného dialogového okna, zobrazujícího žádost o opakované přihlášení nebo o zadání hesla.
- Zaznamenávám stisknutých kláves pomocí speciálního programu.
- Podstrčení disket nebo CD-ROM s nebezpečnými programy (*malware*) v okolí pracoviště oběti.

- Používání vnitrní terminologie a hantýrky s úmyslem vybudovat si důvěru.
- Nabízení odměny za registraci na internetové stránce, spojenou s vložením uživatelského jména a hesla
- Podstrčení dokumentu nebo souboru v podatelně firmy, aby dorazil na určené místo jako vnitřní pošta.
- Změna hlaviček faxu, aby vypadal, jako by pocházel zevnitř firmy.
- Žádost na recepční, aby přijala fax a poslala ho dále.
- Žádost o přenos souboru na zdánlivě vnitřní adresu.
- Nastavení hlasové schránky tak, že je při zpětném volání útočník identifikován jako osoba zevnitř.
- Vydávání se za zaměstnance z jiné lokality a žádost o dočasné e-mailové konto.

Varovné příznaky útoku

- Odmítnutí sdělit zpáteční číslo.
- Neobvyklá žádost.
- Ohánění se autoritou.
- Zdůrazňování naléhavosti záležitosti.
- Hrozba důsledky nevyhovění žádosti.
- Neochota volajícího odpovídat na dotazy.
- Zmiňování mnoha jmen.
- Komplimenty či pochlebování.
- Flirtování.

Typické cíle útoku

Typ cíle	**Příklady**
Neznalý hodnoty informace	Recepční, telefonní spojovatelka, administrativní asistenti, ochranná služba
Se zvláštními právy	Technická podpora či help desk, správci počítačových systémů, operátoři, správci telefonních systémů
Výrobce, dodavatel	Výrobci či dodavatelé hardwaru, softwaru, hlasové pošty
Specifické útvary	Účtárna, personální oddělení

Faktory usnadňující útok

- Veký počet zaměstnanců.
- Více lokalit.
- Informace o tom, kde se pracovníci nacházejí, zanechávané v hlasových schránkách a na záznamnících.
- Sdělování vnitřních telefonních linek.
- Chybějící školení z oblasti bezpečnosti.
- Chybějící systém klasifikace dat.
- Neexistence místa, kam hlásit incidenty a neexistence plánů, jak reagovat.

Ověřování a klasifikace dat

Zde uvedené tabulky mají za úkol pomoci reagovat na žádosti o informace nebo o činnosti, které by mohly být sociotechnickým útokem.

Postup pro ověřování totožnosti

Identifikační prostředek	Popis
Identifikace volajícího (na displeji telefónu)	Zkontroluj, zda hovor pochází z firmy a zda zobrazené číslo odpovídá osobě, která volá.
Zpětné volání	Najdi volajícího v podnikovém telefonním seznamu a zavolej mu na uvedené číslo.
Záruka	Požádej důvěryhodného pracovníka,aby se zaručil za totožnost volajícího.
Společné tajemství	Požádej o uvedení společného firemního tajemství, jako je heslo nebo denní kód.
Nadřízený či šéf	Kontaktuj bezprostředního nadřízeného pracovníka a požádej ho o ověření pracovníkovy totožnosti a statutu.
Bezpečný e-mail	Požádej o dopis s elektronickým podpisem
Rozpoznání po hlase	Pokud znáš volajícího, poznej ho po hlase.
Dynamická hesla	Ověř pomocí zařízení generujícího dynamická hesla nebo použij jiné silné autentikační řešení.
Osobně	Požádej volajícího, aby tě navštívil osobně se identifikátorem či jiným dokladem totožnosti

Postup při ověřování statutu pracovníka

Ověřovací prostředek	Popis
Seznam pracovníků	Zkontroluj, jestli se volající nachází na seznamu pracovníků.
Šéf	Zavolej šéfovi volajícího na číslo uvedené ve vnitřním telefonním seznamu.
Útvar	Zavolej na útvar, ve kterém volající pracuje a zeptej se, jestli je pracovníkem firmy.

Postup při ověřování potřeby informace

Zkontroluj pracovní zařazení a oblast působení	Zkontroluj v publikovaných seznamech, kteří pracovníci jsou oprávněni dostávat příslušné tajné informace.
Získej potvrzení od šéfa	Kontaktuj svého šéfa nebo šéfa volajícího, aby vyřízení žádosti schválil.
Získej potvrzení od vlastníka informace nebo od osoby jím pověřené	Zeptej se vlastníka informace, zda Žadatel potřebuje informaci, o kterou prosí.
Získej potvrzení od speciálního systému	Zkontroluj ve speciální databázi, jestli je žadatel oprávněn konkrétní informaci dostat.

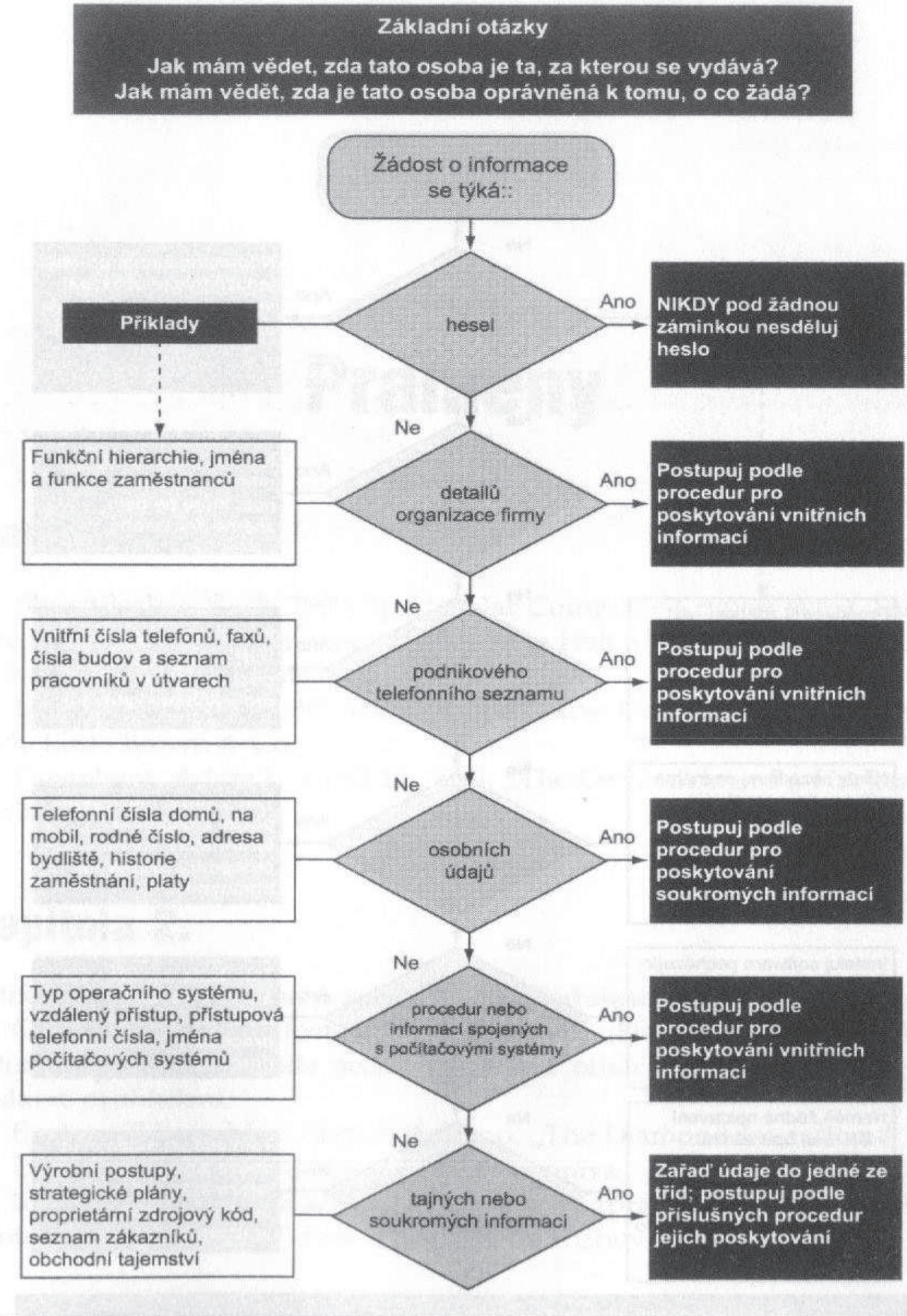
Kritéria při ověřování osob nezaměstnaných ve firmě

Kriterium	**Činnost**
Vztah	Zkontroluj, jestli je firma, kterou žadatel reprezentuje, dodavatelem, strategickým partnerem nebo má jiný odpovídající vztah.
Totožnost	Ověř totožnost osoby a stav zaměstnání v její firmě.
Mlčenlivost	Zkontroluj, jestli osoba podepsala závazek mlčenlivosti.
Přístup	Pokud je informace označena jako důvěrnější než vnitřní, předej záležitost vedení.

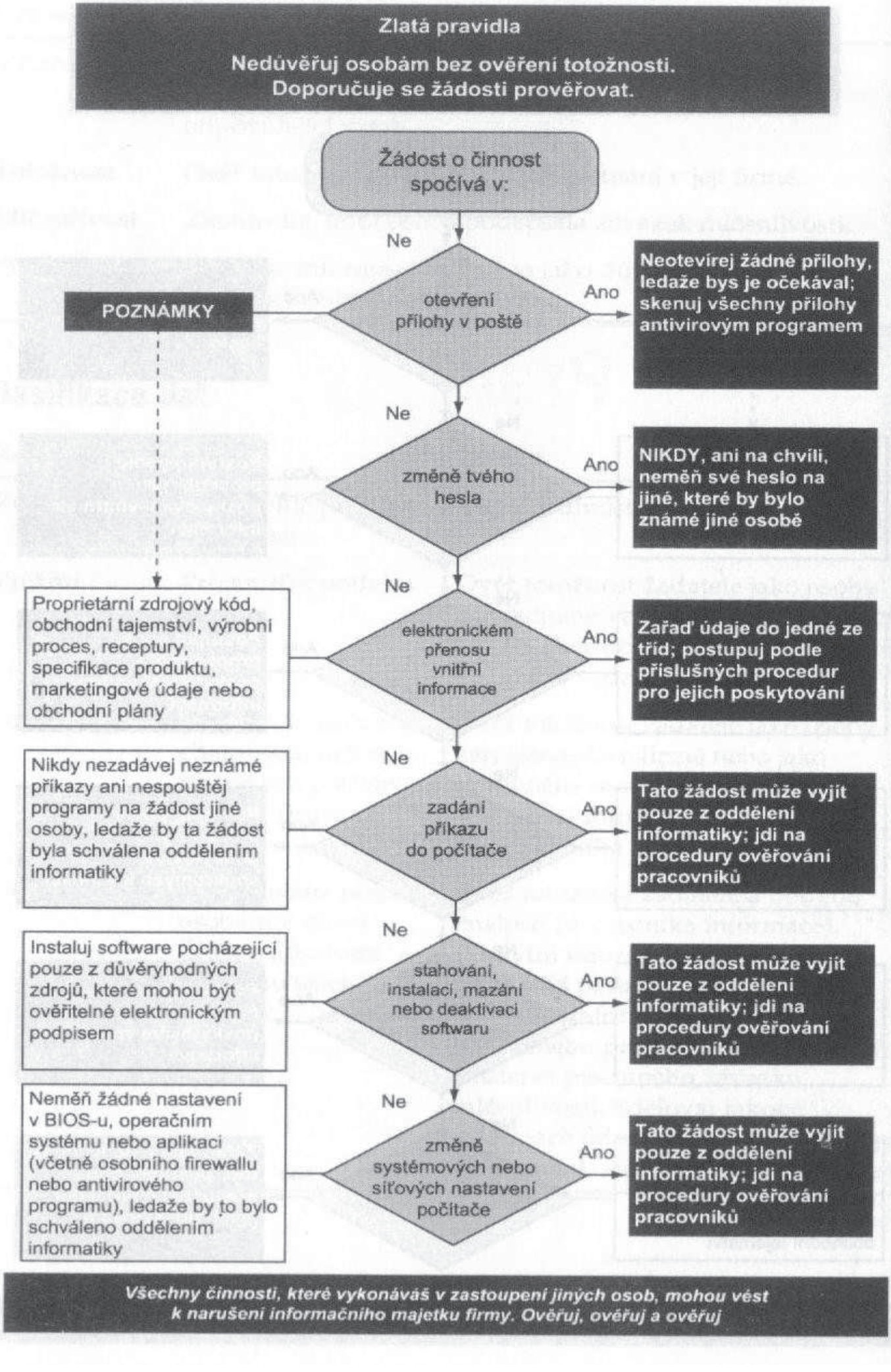
Klasifikace dat

Kategorie	**Popis**	**Postup**
Verejná	Data volně přístupná veřejnosti	Žádná nutnost ověřování
Vnitřní	Pro vnitřní potřebu.	Ověř totožnost žadatele jako osoby zaměstnané ve firmě. V případě osoby zvenčí zkontroluj závazek mlčenlivosti a souhlas vedení.
Soukromná	Informace osobního charakteru určeně pouze pro potřeby v rámci firmy.	Ověř totožnost žadatele jako osoby zaměstnané ve firmě nebo jako oprávněné osoby zvenčí. Než poskytneš informaci, poraď se s personálním útvarem.
Tajná	Poskytovaná pouze osobám v rámci firmy s absolutní potřebou jejich znalosti	Ověř totožnost žadatele a potřebu znalosti (u vlastníka informace). Poskytni informaci pouze tehdy, když máš písemný souhlas šéfa, vlastníka informace nebo jím pověřeného pracovníka. Zkontroluj existenci písemného závazku mlčenlivosti. Sdělovat takové informace lidem, kteří nejsou ve firmě zaměstnáni, může pouze management.

Reagování na žádost o informace



Reagování na žádost o vykonání činnosti



Prameny

Kapitola 1.

BloomBecker, Buck. 1990. Spectacular Computer Crimes: What They Are and How They Cost American Business Haif a Billion Dollars a Year. Irwin Professional Publishing.

Littman, Jonathan. 1997. The Fugitive Game: Online with Kevin Mitnick. Little Brown & Co.

Penenberg, Adam L. April 19,1999. „The Demonizing of a Hacker." Forbes.

Kapitola 2.

Příběh Stanleyho Rifkina je založen na následujících zprávách:

Computer Security Institute. Nedatováno. „Financial losses due to Internet intrusions, trade secret theft and other cyber crimes soar." Tiskové prohlášení.

Epstein, Edward Jay. Nepublikováno. „The Diamond Invention."

Holwick, Re v. David. Nepublikovaná zpráva.

Mr. Rifkin sám s potěšením kvitoval, že se zprávy o jeho činu různí, protože svoje soukromí chránil odmítáním rozhovoru.

Kapitola 15.

Cialdini, Robert B. 2000. Influence: Science and Practice, 4th edition. Allyn and Bacon.

Cialdini, Robert B. Únor 2001. „The Science of Persuasion." Scientific American. 284:2.

Kapitola 16.

Některé pokyny v této kapitole jsou založené na myšlenkách obsažených ve:

Wood, Charles Cresson. 1999. „Information Security Policies Made Easy." Baseline Software.

Poděkování

Od Kevina Mitnicka

Opravdové přátelství bývá definováno jako jedna mysl ve dvou tělech; jen nemnoho z lidí, které v životě poznáme, si zasluhuje označení opravdový přítel. Jack Biello byl přející a starostlivý člověk, který se odvážil vystoupit proti způsobu, jakým se mnou zacházeli neetičtí novináři a příliš fanaticky naladění žalobci. Právě on stál v čele hnutí za moje osvobození a byl autorem článku zveřejňujících informace, které byly pro vládu nepohodlné.

Jack byl vždy připraven odvážně promluvit mým jménem a spolupracovat se mnou na přípravě proslovů a článků, aby se v jistém okamžiku stal mým tiskovým mluvčím.

Proto tuto knížku s hlubokým přátelstvím věnuji mému nejdražšímu příteli Jacku Biello, jehož úmrtí na rakovinu nedlouho po dokončení rukopisu této knihy ve mně zanechalo pocit velké ztráty a hlubokého smutku.

Tato kniha by nemohla vzniknout bez lásky a podpory mé rodiny; mé maminky Shelly Jaffe a babičky Reby Vartanian, jejichž láska a podpora mne provázejí celým mým životem. Je to velké štěstí být vychován tak milující a oddanou matkou, kterou považuji rovněž za svého nejlepšího přítele. Moje babička mi byla druhou mámou prokazující mi lásku a péči. Tyto zázračné a soucítící bytosti mne naučily, jak se starat o jiné a nabízet pomocnou ruku těm, kterým se nedařilo. A tak tedy když kráčím cestou dávání jiným a starostí o druhé, ubírám se v jistém smyslu cestou, kterou mi obě ukázaly. Doufám, že mi prominou, že jsem je během psaní trochu zanedbával, nenavštěvoval je a vysvětloval to množstvím práce a napjatými termíny. Tato kniha by nemohla vzniknout bez jejich neustálé lásky a podpory — navždy budou blízké mému srdci.

Jak bych si přál, aby se můj táta Alan Mitnick a bratr Adam Mitnick dožili této chvíle a mohli si se mnou připít šampaňským v den, kdy se tato kniha objevila v knihkupectvích. Jako obchodník a podnikatel mne můj otec naučil hodně věcí, které nikdy nezapomenu. Během posledních měsíců jeho života jsem měl to štěstí být po jeho boku a dodávat mu naději, jak jen jsem mohl nejlépe. Jeho smrt pro mne byla velmi bolestnou zkušeností, z níž jsem se ještě dodnes nevzpamatoval.

Má teta Chickie Laventhal bude vždy mít v mém srdci zvláštní místo. Přestože jsem ji zklamal několika hloupými chybami, kterých jsem se dopustil, byla vždy při mně se svou láskou a podporou.

Během mého intenzivního psaní této knihy jsem promeškal mnoho příležitostí připojit se k ní, k mé sestřenici Mitch Laventhal a jejímu příteli dr. Robertu Berkowitzovi na každotýdenní oslavu šábesu.

Musím také vzdát vřelé díky matčinu příteli Stevenu Knittleovi, který mne zastoupil a poskytoval mé matce lásku a podporu.

Také bratr mého otce si rozhodně zaslouží zmínku. Možná jsem zdědil své sociotechnické schopnosti právě po strýci Mitchellovi, který vždy věděl, jak manipulovat lidmi a světem takovým způsobem, o kterém jsem nikdy ani nedoufal, že ho pochopím a už si ho určitě nikdy neosvojím. Ke svému štěstí se v době, kdy využíval své okouzlující osobnosti k ovlivňování lidí nikdy nenadchl počítači tak jako já. Titul velmistra sociotechniky bude vždy náležet jemu.

Když píšu tato poděkování, uvědomuji si, že je hodné osob, kterým bych chtěl poděkovat a projevit vděčnost za jejich lásku, přátelství a podporu. Nejsem schopen si pamatovat jména celého toho množství úžasných lidí, se kterými jsem se seznámil v posledních letech — nedokážu je nijak vyjmenovat. Tolik lidí z celého světa mi psalo slova odvahy, uznání a podpory. Tato slova pro mne znamenala hodně, zejména ve chvílích, kdy jsem je nejvíce potřeboval.

Obzvláště jsem zavázán mým stoupencům, kteří se postavili na mou stranu a věnovali svůj cenný čas a energii, aby vyjádřili svoji starost o mne a postavili se proti tomu, jak se mnou bylo nakládáno a proti zveličování, vyvolaném těmi, kdož byli hnáni vidinou zisku z „mýtu Kevina Mitnicka".

Měl jsem neobyčejné štěstí spolupracovat s autorem bestselleru — Billem Simonem. Pracovali jsme bok po boku nehledě na rozdíly, které mezi námi existují. Bili je neobyčejně organizovaný, ráno brzy vstává a pracuje promyšleně a plánovitě. Jsem mu vděčný, že se přizpůsobil mému nočnímu stylu života. Moje angažovanost v tomto projektu a přetahování pracovní doby způsobovaly, že jsem občas končil až ráno, což kolidovalo s Billovým pravidelným rozvrhem dne.

Bill dokázal přetvořit mé nápady do vět hodných zralého čtenáře a prokazoval (téměř vždy) trpělivost při zápolení s mým programátorským viděním podrobností. Na tomto místě bych se chtěl Billovi omluvit a říci, že vždy budu litovat svého přístupu k práci, protože právě moje pedantství při uvádění detailů zapříčinilo, že Bill poprvé ve své dlouhé spisovatelské kariéře nedodržel dohodnutý termín. Nakonec jsem pochopil, v čem spočívá práce spisovatele a ocenil jsem ji. Doufáme, že společně napíšeme další knihy.

Pobyt v Simonově domově na Rancho Santa Fe, kde jsme pracovali a byli rozmazlováni jeho ženou Arynne, pokládám za nejpříjemnější aspekt psaní. Rozhovory s Arynne a její kulinářské dovednosti spolu bojují o první místo v mé paměti. Můj obdiv vzbuzuje její úroveň, moudrost a smysl pro humor. Vytvořila domov plný tepla a krásy. A kromě toho se stále nemohu napít dietní limonády, aniž bych v duchu neslyšel hlas Arynne, připomínající škodlivost aspartamu.

Hodně pro mne znamená Stacey Kirkland. Věnovala hodně hodin svého času, aby mi pomohla vytvořit na Macintoshi tabulky a schémata, která pomáhala vizualizovat mé nápady. Obdivuji její nádhernou povahu. Je to opravdu milá a soucítící bytost, která si v životě zaslouží jen samé dobré věci. Slyšel jsem od ní mnoho povzbuzujících slov a je to člověk, na kterém mi velmi záleží. Chtěl bych jí poděkovat za její láskyplnou podporu a za to, že se mi věnovala, kdykoliv jsem potřeboval.

Alex Kasper, „Nexspace", není jen můj nejlepší kamarád, ale také obchodní partner a kolega. Spolu jsme vytvářeli oblíbené rozhlasové talk show *Temná strana Internetu* na rádiu KFI AM 640 v Los Angeles, pod obratným vedením programového ředitele Davida G. Halla. Alex mi poskytl cennou pomoc a dal mi v souvislosti s knihou hodně rad. Jeho vliv na mne byl vždy pozitivní a jeho laskavost a pohostinnost nekončila dokonce ani v pozdních nočních hodinách. Spolu s Alexem jsme nedávno dokončili film, který má firmám pomoci při školení jejich zaměstnanců, jak předcházet sociotechnickým útokům.

Paul Dryman je víc než rodinný přítel. Tento uznávaný a důvěryhodný soukromý detektiv mi pomohl pochopit, v čem spočívá opravdové pátrání. Paulovy znalosti a zkušenosti mi usnadnily tvorbu doporučení týkajících se bezpečnosti, která se nacházejí ve čtvrté části této knihy.

Candi Layman mi neustále prokazovala podporu a sympatie. Je to úžasná osoba, která si v životě zasluhuje jen to nejlepší. Během tragických chvil mého života mi Candi vždy dodávala odvahu a přátelství. Mám štěstí, že jsem se mohl setkat s tak úžasnou, starostlivou a soucitnou bytostí. Chtěl bych jí poděkovat, že byla při mně.

Mé první peníze vydělané prodejem této knížky určitě padnou na uhrazení účtů za dlouhé hovory s Erin Finn. Je to bezpochyby má spřízněná duše. Jsme si v mnoha věcech tak podobni, až je to zarážející. Oba chováme lásku k technologiím, máme rádi stejná jídla, stejnou hudbu a stejné filmy. AT&T rozhodně prodělává, když mi v rámci tarifu dává bezplatné noční a víkendové hovory a já volám Erin do Chicaga. Ale pracovníci té firmy jsou určitě rádi, že už nevyužívám „Tarifní program Kevina Mitnicka". Erinino nadšení a její důvěra v tuto knížku mne pozvedávaly na duchu. Jsem rád, že můžeme být přátelé.

Chtěl bych poděkovat všem, kteří mi pomáhají v mé profesionální kariéře. Organizací přednášek se zabývá Amy Gray (poctivá a starostlivá žena, které si cením a kterou zbožňuji). David Fugate z Waterside Productions je můj agent, který vystupoval na mou obranu mnohokrát před i po podepsání smlouvy na tuto knihu. Gregory Vinson je právník z Los Angeles, který byl jedním z mých obhájců během dlouhého boje s vládou. Určitě by si mohl s Billem popovídat na téma pochopení a trpělivosti, které je třeba prokazovat mému puntičkářství, protože zažil to samé, když mým jménem psal různé dopisy a podání.

Měl jsem příliš mnoho zkušeností s právníky, ale chtěl bych poděkovat těm, kteří mi během mého boje s justicí nabídli svou pomoc, kterou jsem zoufale potřeboval. Setkal jsem se s mnoha právníky, kteří popírají zažitý stereotyp egocentrického advokáta — milými slovy, která jsem od nich slyšel, počínaje a hlubokým angažováním v mé záležitosti konče. Vážím si jich a obdivuji je. Oceňuji také jejich přejícnost a morální podporu, kterou mi mnoho z nich nezištně vyjádřilo. Každá z těchto osob by si určitě zasloužila vlastní odstavec. Chtěl bych je tu alespoň vyjmenovat: Greg Aclin, Bob Carmen, John Dusenbury, Sher-man Ellison, Omar Figueroa, Carolyn Hagin, Rob Hale, Alvin Michael-son, Ralph Peretz, Vicki Podberesky, Donald C. Randolph, Dave Roberts, Alan Rubin, Steven Sadowski, Tony Serra, Ruchard Sherman, Skip Slates, Karen Smith, Richard Steingard, ctihodný Robert Talcott, Barry Tarlow, John Yzurdiaga a Gregory Vinson.

Velmi si cením příležitosti, kterou mi jako autorovi této knihy dalo nakladatelství John Wiley & Sons. Chci poděkovat následujícím osobám z nakladatelství, které uvěřily debutantovi a dovolily mu uskutečnit svůj sen: Fllen Gerstein, Bob Ipsen, Carol Long (můj redaktor) a Nancy Stevenson.

Chtěl bych poděkovat také lidem z rodiny, přátelům a spolupracovníkům, kteří mi vyjádřili podporu, poskytli rady, nabízeli pomocnou ruku. Jsou to: J. J. Abrams, David Agger, Bob Arkow, Stephen Barnes, dr. Robert Berkowitz, Dále Coddington, Eric Corley, Delin Cormeny, Ed Cummings, Art Davis, Michelle Delio, Sam Downing, John Draper, Paul Dryman, Nick Duva, Roy Eskapa, Alex Fielding, Lisa Flores, Brock Frank, Steve Gibson, Jerry Greenblatt, Greg Grunberg, Bili Handle, David G. Halí, Dave Harrison, Leslie Herman, Jim Hill, Barry Krugel, Earl Krugel, Adrian Lamo, Leo Laporte, Mitch Leventhal, Cynthia Levin, CJ Little, Jonathan Littman, Mark Maifrert, Brian Martin, Forrest McDonald, Kerry McElwee, Alan McSwain, Elliott Moore, Michael Morris, Eddie Munoz, Patrick Norton, Shawn Nunley, Brenda Parker, Chris Pelton, Kevin Poulsen, Scott Press, Linda a Art Pryor, Jennifer Read, Israel a Ráchel Rosencrantz, Mark Ross, William Royer, Irv Rubin, Ryan Russell, Neil Saavedra, Wynn Schwartu, Pete Shipley, Joh Siff, Dan Sokol, Trudy Spector, Matt Spergel, Eliza Amadea Sultán, Douglas Thomas, Roy Tucker, Bryan Turbow, Ron Wetzel, Don David Wilson, Dárci Wood, Kevin Wortman, Steve Wozniak a všichni mí známí z kanálu W6NUT (147,453 MHz) z Los Angeles.

Zvláštní poděkování si zaslouží můj kurátor Larry Hawley za to, že mi usnadnil práci na knížce.

A konečně děkuji všem policistům. Nechovám k nim žádnou zášť, protože oni jen konají svou práci. Věřím, že obětovat vlastní soukromý život službě a dávat přednost veřejnému zájmu nad vlastním je něco, co si zasluhuje úctu. Ačkoliv jsem k vám byl občas arogantní, chtěl bych, abyste věděli, že miluji tuto zemi a udělám všechno, co je v mých silách, abych ji učinil nejbezpečnějším místem na světě. Proto jsem vlastně napsal tuto knížku.

Od Billa Simona

Zdá se mi, že pro každého někde existuje ta *pravá* osoba. Problém je v tom, že ne každý má tolik štěstí, aby ji našel. Někteří ho mají. Mně se to poštěstilo už dávno a stihl jsem prožít mnoho let (a počítám s mnoha dalšími) s jedním pokladem — mou ženou Arynne. Pokud bych snad někdy na chvíli zapomněl, jaké štěstí mne potkalo, stačí, když si všimnu, kolik lidí

vyhledává její společnost a cení si jí. Arynne — děkuji ti za to, že kráčíš životem se mnou.

Během psaní této knihy jsem využíval pomoc skupiny oddaných přátel, kteří mne ujišťovali, že spolu s Kevinem směřujeme k předpokládanému cíli — směsici faktů a fascinace, ze které se skládá tato neobvyklá knížka. Každá z těchto osob je pro mne neobyčejně cenná a vím, že mohu znovu očekávat pomoc, až přijde čas na novou knížku. V abecedním pořadí to jsou: Jean-Claude Beneventi, Linda Brown, Walt Brown, generálporučík Don Johnson, Dorothy Ryan, Guri Stark, Chris Steep, Michael Steep a John Votaw.

Zvláštní výraz uznání bych chtěl vyjádřit Johnu Lucichovi, prezidentu Network Security Group, který se uvolil věnovat svůj čas prosbě „přítele přítele" a Gordonu Garbovi, který trpělivě snášel nesčíslné telefonáty s dotazy týkající se fungování oddělení informatiky.

Občas jsme vděčni známým, že nás seznámili s lidmi, kteří se pak stali našimi velkými přáteli. David Fugate z literární agentury Waterside Productions z Cardiffu v Kalifornii byl iniciátor této knihy. Právě on mne seznámil se spoluautorem, který se stal mým přítelem — Kevinem. Děkuji ti, Davide. Děkuji též šéfovi Waterside, nedostižnému Billu Gladstoneovi, který mne zahrnuje novými nápady — jsem rád, že tě mám.

Doma a v mé domácí kanceláři pomáhá mé ženě Arynne schopný personál, který se skládá z asistentky Jessiky Dudgeon a hospodyně Josie Rodriguez.

Děkuji svým rodičům Marjorie a I. B. Simonovým. Kdyby žili, jistě by měli radost z mé spisovatelské kariéry. Děkuji rovněž své dceři Victorii. Když jsem s ní, uvědomuji si, jak moc ji obdivuji, ctím a jak jsem pyšný na to, kdo je.

* * *