Kevin Mitnick. Hacker, který vstoupil do dějin. Kolem jeho odsouzení a uvěznění se dodnes vedou – a nejspíš ještě nějaký ten pátek povedou – spory. Jedno je ale jisté: stal se prvním „počítačovým zločincem“, jenž se ocitl na seznamu deseti nejhledanějších osob americkou FBI.

Hacker #1:
Klávesnice jako zbraň

Rozhovor s nejslavnějším hackerem světa Kevinem Mitnickem

Začínal jako phreaker – člověk, který se nabourává do systému telekomunikačních společností. Když získal potřebné znalosti, dokázal s telefonními ústřednami hotové divy. Třeba domácí stanici jednoho svého kamaráda změnil v ústředně na veřejný telefonní automat. Takže když dotyčný kamarád chtěl telefonovat a zvedl sluchátko, ozvalo se: „Vhoďte prosím minci.“ Což u domácího přístroje jde jen velmi těžko.

Od phreakingu pokročil k hackování počítačů – dokázal se dostat prakticky do jakéhokoliv systému. Jeho úžasné schopnosti, kdy využíval jak čistokrevné hackerské techniky, tak metod sociálního inženýrství, mu otevřely cestu do nejpřísněji střežených počítačů. To mu na jedné straně vyneslo obdiv hackerské komunity, na straně druhé ale nenávist mnoha jiných. Navíc se kolem něj vytvořil velkolepý mýtus – zásluhou novináře Johna Markoffa a jeho knihy. Mitnick prý dokázal nemožné kousky. Podařilo se mu nabourat do databází FBI a měnit zde záznamy o své osobě. Dokázal se prý dostat do počítačů amerického Pentagonu, a byl jediné kliknutí myši od rozpoutání jaderné války, apod.

Americká vláda tyto informace nikdy oficiálně nekomentovala. A dodnes je nekomentoval ani Mitnick – po svém uvěznění byl předčasně propuštěn s podmínkou, že příštích sedm let nebude jakkoliv komentovat své bývalé hackerské aktivity. Navíc měl zákaz přístupu k informačním technologiím – ten vypršel letos.

Škoda způsobená Kevinem Mitnickem údajně dosáhla 300 mil. dolarů! On sám ale vysvětluje, jak k tomuto číslu vyšetřovatelé došli: „Protože proti hackerům neexistovaly zákony a mým počínáním žádná prokazatelná škoda nevznikla, vzali v úvahu nejvyšší možnou škodu, která mohla vzniknout. Prostě sečetli částky na vývoj softwaru a produktů, jejichž kódy a plány jsem při svých útocích získal – a došli k oné závratné částce. Byla to ale jen imaginární suma, nikdy se totiž neobjevila v účetních výkazech domněle poškozených firem.“

V rozsudku soudu, který jej poslal za mříže, stálo: „Vyzbrojen klávesnicí je nebezpečím pro společnost.“

Kevin Mitnick zavítal na konci září i do České republiky, aby zde prezentoval svoji knihou „Umění klamu“. Při této příležitosti vznikl i následující rozhovor.

Druzí lidé o vás nejčastěji hovoří jako o „nejslavnějším hackerovi světa“. Jak byste se ale charakterizoval sám v několika větách?

To je velmi obtížné, popsat sám sebe v několika větách. Sám sebe bych popsal jako člověka, který má rád velké výzvy a je velmi rád úspěšný – i v životě. A taky se snaží změnit svět, aby byl lepším místem pro každého.

Slovíčko „hack“ mělo původně pozitivní význam. V současné době ale nikoliv. Sám sebe považujete za hackera v pozitivním, nebo negativním slova smyslu?

Sám sebe považuji za člena „staré školy“. Bohužel ale média časem význam slova hacker překroutila a dnes je jako „hacker“ označovaný každý, kdo provede v počítačovém světě kriminální čin. Myslím ale, že se i nadále mohu považovat za hackera ze staré školy. Další hackeři ze staré školy jsou třeba Steve Wozniak či Steve Jobs – lidé, kteří možná zapadají do jakési „šedé zóny“, ale nevyužívají své zkušenosti k tomu, aby poškodili druhé, aby odcizili peníze, aby měli nějaký osobní prospěch. Prostě si jen chtějí ověřit možnosti techniky a svých vlastních znalostí.

Hackerem se člověk nenarodí. Proč jste začal s hackováním?

Velmi jsem se zajímal o telekomunikační systémy v telefonních společnostech. A důvodem, proč jsem s hackingem začal, byla snaha mít přístup právě do těchto systémů. A proto jsem se začal koncem sedmdesátých let věnovat počítačům.

Předtím, než jste se věnoval hackingu, měl jste nějaké jiné záliby?

Před skutečným hackováním jsem se věnoval phreakingu. To je zkoumání telefonních sítí přibližně stejným způsobem, jakým dnešní hacker zkoumá sítě počítačové. Navíc jsem se zajímal o rádiové komunikace. A mým koníčkem bylo také kouzelnictví.

Umění klamu

Pokud vás alespoň trochu zajímá počítačová bezpečnost či historie hackingu, jméno Kevina Mitnicka vám nebude neznámé. Překlad jeho knihy k nám dorazil v podobě velké mediální bubliny, ovšem realita je, jak bývá zvykem, poněkud prostší. Mitnick určitě není ani nejlepším, ani nejslavnějším, ani nejchytřejším hackerem. Koneckonců, jak praví v jedné ze svých her génius Jára Cimrman, „Co je to za eso, když se nechá chytit, že?" Autora „proslavilo" to, že jeho tažení skončila několika desítkami měsíců vězení. No, a proč toho nevyužít?

Přes všechno pozlátko je Umění klamu hodně zajímavá knížka, přestože je velmi zavádějící říci, že je o hackingu. Nenajdete v ní ani

UMĚNÍ KLAMU
Autor: Kevin Mitnick a William Simon
Počet stran: 348
Cena: 299 Kč
Vydal: Helion S.A., Polsko (u nás Kanzelsberger)
http://mitnick.helion.pl

řádku kódu, neboť pojednává o jediném úzkém „odvětví" hackerské práce, zato však důkladně. Předmětem 300stránkového výkladu je totiž pojednání o tzv. social engineeringu, překládaném jako sociotechnika. Právě v této oblasti Mitnick svého času dosáhl mimořádných „úspěchů", a dnes v roli poradce předvádí, jak by to mohlo vypadat a co by vás mohlo potkat.

Publikace zahrnuje desítky ukázek reálných postupů, s jejichž pomocí je schopen prakticky kdokoliv zneužít důvěry zaměstnanců a získat privátní informace všemožného charakteru. Tvůrci připravili text velmi dobře, takže příklady působí nesmírně věrohodně, a díky vhodnému sestavení do nápaditě mozaiky se demonstrované postupy velmi blíží realitě. Každý si tak může na vlastní kůži vyzkoušet, kde by jeho nevinný telefonní hovor či přílišná důvěřivost mohly narušit jinak pevnou hradbu firemní bezpečnosti.

Krom toho, že vás autoři přesvědčí o použitelnosti sociotechniky, předají vám mimochodem ještě jednu nesmírně cennou zkušenost. Nejste-li extrémně nechápaví, dojde vám, že opravdový hacker nebude dva měsíce zbytečně prolamovat váš certifikovaný firewall, když mu stačí třeba pár telefonátů. Myslím, že právě toto poselství je nejcennější. A proto knihu všem nedůvěřivcům vřele doporučuji – sociotechnikou totiž každý správný útok začíná.

Ačkoliv je publikace možná o něčem jiném, než jste čekali, je velmi zajímavá a poučná. Jako povinnou četbu bych ji doporučil všem bezpečnostním administrátorům a manažerům u firem s více než 20 zaměstnanci – právě tam je sociotechnik jako doma. Nebo jste si jisti, že od vás únik důvěrných informací nehrozí?

PATRIK MALINA 3 0633/FEL ❑

Žaloba proti Kevinu Mitnickovi se skládala z 25 obvinění: například ilegální vlastnictví počítačových souborů odcizených z takových společností, jako např. Motorola, NEC a Sun, krádeže státních tajemství, proniknutí do národního systému obrany, atd.

Člověk nedělá věci jen tak, bezdůvodně. Co vám osobně hacking přinášel?

Hacking pro mě znamenal rozšíření znalostí, osobní výzvu, možnost dostat se někam, kam bych normálně neměl přístup. A především uspokojoval moji vášeň pro techniku. V žádném případě pro mě hacking nebyl o poškozování někoho, výzvou pro mě bylo pouze překonávání překážek. Byl jsem počítačový nadšenec – a stále jsem. Ale nedělal jsem nic ilegálního, protože když jsem s hackingem poprvé začal, nebylo to nelegální. Prostě nebyl zákon. A taky šlo o pokračování mého zájmu v kouzlení, vytváření iluzí.

Vzpomenete si ještě na svůj první úspěšný počítačový útok?

Samozřejmě. Studoval jsem na střední škole a naprogramoval jsem simulátor přihlašovacího okna. Takže když pak přišel učitel a zadal přihlašovací jméno i heslo, zadal ho vlastně do mého programu. A já jsem za ním druhý den přišel a jméno i heslo mu řekl. Velmi se podivil a změnil si je. To se pak opakovalo ještě několikrát a jeho hrozně štvalo, že nemohl zjistit, jak to dělám.

V průběhu tiskové konference, která tomuto rozhovoru předcházela, jste se zmínil, že po hackerech vždy zůstávají stopy. Zůstávaly i po vás?

Ano, samozřejmě. V mnoha případech poté, co jsem se dostal dovnitř, už mi bylo jedno, co se stane později. Byly situace, kdy jsem se snažil nezanechávat stopy, a byly situace, kdy mi na tom nezáleželo, takže nějaké nepochybně zůstaly.

Napsal jste knihu. Je to jen komerční tah, kdy se snažíte co nejvíce vytěžit ze svého jména, nebo je za touto knihou něco více?

Osobně si myslím, že ta kniha má fascinující obsah, protože vyplňuje velkou mezeru na trhu. Je to dáno tím, že sociální inženýrství – což je technika používaná VELMI často – nemá v literatuře odpovídající místo. V každé knize je o ní většinou stránka nebo dvě, když moc, tak jedna kapitola. A takto to vypadá ve stovkách knih o počítačové bezpečnosti.

Naštěstí mám ještě mnoho dalších materiálů, které mohu zpracovat k tomuto skutečně aktuálnímu tématu, protože sociální inženýrství není o technikách hackingu, je to o sociální psychologii. A využití vlivu, klamu a dalších záludností je jen prostředkem k získávání citlivých informací.

Klamy a triky jsou prostě způsobem, jakým hackeři a průmysloví špióni kompromitují své cíle. A když ještě k těmto sociálním útokům přidáte útoky technické, mohou se stát velmi, velmi nebezpečnými.

Propuštěn jste byl pod podmínkou, že sedm let nebudete jakkoliv komentovat své bývalé hackerské aktivity. Plánujete po uplynutí této lhůty napsat další knihu – jakýsi skutečný příběh Kevina Mitnicka?

Ano, rozhodně to připravuji poté, co skončí restrikce vůči mé osobě. Možná to nebude až po uplynutí sedmi let, protože hodlám najmout advokáta a těmto omezením se bránit už v dohledné době. To, co je konáno proti mé osobě, je podle zákonů Spojených států neústavní.

V sedmdesátých letech rozvířil dění ve Státech příběh vraha, který zabil několik prostitutek, a byl odsouzený na doživotí. Úřady jej přinutily zastavit psaní knihy a profitovat tak ze svého zločinu. Následně vznikl zákon, že pokud jste usvědčený ze zločinu, nemůžete z něj profitovat. Nejvyšší soud Spojených států to ale zvrátil s tím, že každá osoba má ústavní právo vyjadřovat se. Takže v mém případě je spousta legislativních otázek, zdali jsou restrikce vůči mé osobě oprávněné či nikoliv. Nejpozději za čtyři roky (v roce 2007 vyprší sedmiletá lhůta – pozn. autora) budeme moudřejší.

Ale na konec tohoto roku připravuji ve Spojených státech svoji další knihu – po Art of Deception (Umění klamu) chystám Art of Intrusion (Umění průniku). Je to příběh skutečných útočníků – jak kompromitují své cíle, jaké slabiny systémů využívají a jak zajistit, aby se něco podobného čtenářům knihy nestalo.

Čas od času se objeví informace, že hackeři jsou placeni bezpečnostními firmami. Vás osobně někdy nějaká bezpečnostní firma najala?

Tu a tam se objevují zprávy, že například antivirové firmy najímají programátory, aby psali viry. Ale kdyby to byla pravda a dostalo se to na veřejnost, zruinovalo by to celou firmu. Myslím, že s něčím podobným je spojeno příliš velké riziko.

Já osobně v současné době jednám s jistou společností v Londýně, abych otestoval jejich produkt. Je to hardwarové zařízení – přesněji hardwarové bezpečnostní zařízení. Ale na tom není nic nelegálního.

A dříve jsem si za podobnou činnost nenechal platit, nikdo po mě nic podobného nechtěl.

Jste známý tím, že dokážete obratně používat sociálního inženýrství. Jaký je ve vašem případě poměr mezi ním a skutečnými hackerskými technikami?

V mém případě padesát na padesát.

Na světě je mnoho hackerů nebo alespoň lidí, kteří se za hackery považují. Jen málo z nich ale bylo dopadeno a odsouzeno. Nejslavnějším z nich se stal Kevin Mitnick. Proč?

Já myslím, že to má hodně co do činění s mýtem Kevina Mitnicka. Jeden reportér pracující pro New York Times vytvořil senzační příběh, napsal fiktivní sumarizaci mých aktivit a vytvořil neuvěřitelný strach v americké veřejnosti. Stal jsem se tak čítankovým příkladem pro federální vládu jako počítačový hacker a mé jméno proniklo jako velmi známé na veřejnost. A tak jsem se stal odstrašujícím příkladem.

Jak vlastně FBI získala důkazy proti vám?

Na tom nehledejte nic zvláštního. Jakmile jsem byl lokalizován, provedli domovní prohlídku, zabavili počítače – a z nich získali příslušné důkazy.

Dobře, ale proč se FBI rozhodla, že vás bude stíhat? Kde byl prvotní impuls, že na vás přišla?

To nemohu komentovat.

Několik let jste byl ve federálním nápravném zařízení, i po propuštění následoval trest v podobě zákazu používání elektronických zařízení. Neztratil jste za tuto dobu kontakt s novými technologiemi?

Samozřejmě, že když je člověk odříznutý od reálného světa, mnoho věcí zapomene a mnoho se změní. Ale sám jsem na druhé straně překvapený, kolik toho zůstalo a že staré triky fungují i v nové době.

Kdysi jste se věnoval hackingu, nyní se nacházíte takříkajíc „na druhé straně barikády". Udržujete stále ještě kontakty s hackery?

Ano, nějaké kontakty stále mám. Opakuji ale, že nevykonávám žádnou ilegální činnost. Udržuji své kontakty s hackerskou komunitou, protože mě velmi podporovala a také od ní dostávám informace o různých bezpečnostních problémech a nedostatcích dříve, než jsou oficiálně zveřejněné.

Kdybyste měl možnost něco ve svém životě změnit, co by to bylo?

Kdybych měl možnost postavit stroj času, rád bych se vrátil do dob vysokoškolského studia. Ale kdyby to šlo, ponechal bych si své současné znalosti. [Smích.] To bych opravdu rád udělal, ale bohužel je to nemožné.

Asi každý vidí, že současnost počítačové bezpečnosti je – slušně řečeno – tragická. Jak vidíte její budoucnost?

Bude to stále hra kočky s myší. Stále bude skupinka osob schopných najít bezpečnostní nedostatky a využít je. A na druhé straně se budou výrobci softwaru, tvůrci operačních systémů a dodavatelé bezpečnostních řešení pokoušet zastavit tyto průniky a narušení. Nevěřím, že někdy bude nalezeno stoprocentní řešení. Naopak věřím, že přestože se bezpečnostní technologie stávají pokročilými a úspěšnějšími, stále se nacházejí a budou nacházet využitelné nedostatky. Například je-li vaše softwarové bezpečnost na vysoké úrovni, vaše fyzická bezpečnost je velmi slabá. A útočník pak může snadno vstoupit do vaší budovy a připojit se do sítě. Velmi jednoduchý útok. A útočník získá přístupová práva.

Útočník prostě analyzuje celkovou situaci a hledá nejslabší body celého řetězce. Myslím, že největší hrozbou jsou lidé, protože každý sociální útok, který jsem se pokusil v minulosti provést, byl úspěšný. Opravdu věřím, že lidé jsou nejslabším článkem.

Mohl byste nám prozradit, jakým způsobem chráníte svůj osobní počítač?

Jak vidíte, nosím jej stále při sobě, prostě ho nenechávám jen tak v autě. Zálohuji svá data –

Malý slovníček

- **Hacker, hacking** – člověk, který provádí ve světě informačních technologií zásahy do softwaru (anglicky hack – zásek). Původně byli hackeři lidé, kteří upravovali vytvořené počítačové programy pro použití v konkrétním prostředí, postupem času slovíčko získalo jiný význam a označuje všechny vykonavatele nelegálních činností v kybernetickém světě.
- **Malware (Malign Software)** – škodlivý program. Souhrnné označení veškerých nežádoucích programů, které se v kybernetickém prostoru vyskytují (viry, síťoví červi apod.).
- **Phreaker, phreaking** – člověk, který provádí útoky na systémy telekomunikačních firem. Cílem může být osobní zisk (telefonování zdarma, za snížený poplatek apod.) nebo pouhé zadostiučinění (překonání bariér, možnost pohybovat se v „zakázané" zóně aj.).
- **Sociální inženýrství** – technika útoku, která má za cíl získat data a informace z nejslabšího článku bezpečnostního řetězce (což je zpravidla člověk). Vesměs využívá klamu nebo podvodu.
- **Spyware (Spy Software)** – sledovací program. Počítačový software, který je instalovaný v počítači a monitoruje prováděné úkony (veškeré nebo jen některé) – zadávání hesel, spouštěné programy, psané e-maily apod.

mnoho lidí nezálohuje data právě z laptopů, protože je mají stále s sebou – což je minimálně zvláštní. Dále mám personální firewall, antivirový program a snažím se pravidelně záplatovat. Čas od času spouštím programy, které mají za cíl nalézt, zdali se v mém počítači neobjevil nějaký spyware. Jsem opatrný, což ale neznamená, že jsem v bezpečí. Pokud se objeví nový bezpečnostní nedostatek ve službě, kvůli které mám nějaký port otevřený – podotýkám, že firewallem se pokouším mít stále uzavřené všechny nepotřebné porty – samozřejmě může nastat velmi nepříjemná situace. Zvláště nebezpečné jsou nedostatky na klientské straně, kdy vám prohlížeč může nahrát do počítače něco proti vaší vůli. Proto se snažím svůj počítač udržovat co nejvíce s dobou.

Je pravdou, že došlo k hacknutí také vašich osobních stránek?

Ano, to je pravda. Protože jsem dlouho nesměl k počítači a protože jsem měl málo času, jeden nadšenec se nabídl, že se mi bude starat o mé stránky. Jenomže jim nevěnoval odpovídající pozornost a samozřejmě je někdo hacknul. Prostě chtěl získat skalp Kevina Mitnicka. Pochopitelně se tím pochlubil a senzace byla na světě: hacknuté stránky nejslavnějšího hackera! Jak jsem ale uvedl, na těch stránkách jsem osobně neměl žádný podíl – a když jsem je pak chtěl převzít a odstranit bezpečnostní chyby, musel jsem zatelefonovat onomu nadšenci. Já jsem k nim totiž neměl ani heslo.

Tyto stránky jsme pak přesunuli k profesionálnímu poskytovateli služeb a od té doby jsou místem zajímavého střetu. Na jedné straně je komunita hackerů, která na ně usilovně útočí ve snaze se zviditelnit. A na straně druhé je komunita hackerů, která je usilovně brání.

Co hodláte dělat v budoucnosti?

V současné době jsem konzultant přes počítačovou bezpečnost a jsem spoluzakladatel i CEO společnosti Defensive Thinking. Zaměřujeme se na školení počítačové bezpečnosti, připravujeme dvoudenní semináře pro firmy, děláme penetrační testy, bezpečnostní analýzy. Já osobně se navíc věnuji veřejným vystoupením a cestuji s přednáškami o počítačové bezpečnosti po celém světě. Také jsem předsedou dvou bezpečnostních konferencí ve Státech. Jedna se jmenuje „360 Security Summit" a bude se konat koncem roku. Další nazvaná „Access Denied" (Přístup odepřený) se bude konat v roce 2004.

Chtěl byste na závěr něco vzkázat lidem – zejména mladým – kteří vás vidí jako vzor?

Opravdu si myslím, že dnešní mladí lidé se nemusejí vydávat v mých stopách. Když jsem začínal s počítači, nebyly tak jednoduché a dostupné. Primitivní útok? To rozhodně ano. Ale nesmírně účinný, a především funkční. A skutečný sociální inženýr by nad ním nejspíše jen mávnul rukou, protože je schopen vymyslet věci mnohem sofistikovanější a rafinovanější.

Šlo skutečně jen o ilustrační příklad, jakým způsobem lze z veřejně běžně dostupných informací a základních znalostí získat nesmírně cenné informace.

Sociální inženýrství funguje tak, že má za úkol snížit pozornost člověka, aby vykonal úkon, který by za normálních okolností neprovedl, nebo by dokonce pojal podezření a přijal by odpovídající protiopatření. V předchozím případě uživatel nejenže pravděpodobně nepojal podezření, že vyzradil citlivé informace (protože na něj nebyl vyvíjen nátlak, ale on sám se rozhodl tyto údaje poskytnout), ale navíc měl dobrý pocit, že zabránil hrozící škodě. Jak kruté pak bylo po několika dnech vystřízlivění!

K základním metodám používaným sociálním inženýrstvím patří:

- **Stres** – člověk pod tlakem reaguje jinak než člověk v pohodě, který má čas nad věcmi přemýšlet. Zvláště ve velké firmě platí, že ne každý zná každého, a když zazvoní telefon, že je potřeba vykonat tu a tu činnost či sdělit takovou informaci, aby se zabránilo velkému průšvihu, asi jen málokdo zaváhá.
- **Nebezpečí** – krásný a jednoduchý příklad už byl uveden na předchozích řádcích. Vaší peněžence hrozí nebezpečí. Když nechcete, nic neděl ejte. Ale kdybyste se přece jen rozhodli něco udělat.
- **Vydávání se za někoho/něco známého** – opravdu je osoba v e-mailu nebo v telefonu skutečně tím, za koho se vydává? Zvláště v armádě se hierarchie hodností dodržuje více než důsledně. Ale i v civilu platí, že když zavolá nová asistentka generálního ředitele, asi jen největší odvážlivec by jí odmítl sdělit požadovanou informaci.
- **Důvěryhodná činnost** – útoky není potřeba provádět pouze vzdáleně. Člověk s brašnou a v montérkách propluje hlavně do objektu velké firmy zpravidla bez větších potíží. A když se předtím ještě třeba telefonicky objednal (nebo když ho dokonce objednal někdo jiný), má dveře otevřené prakticky všude.
- **Lákavá činnost** – lidé zpravidla nejsou příliš složitými osobnostmi, alespoň ne v základních potřebách. A tak není divu, že třeba e-mailoví červi, vydávající se za soubory s lechtivým obsahem, dosahují větší úspěšnosti než jejich „serióznější" kolegové. Viz třeba červ Anna Kurnikovová – antivirové programy jej znaly už mnoho měsíců, a přesto slavil obrovský úspěch. Člověku pak není problém jakýmkoliv způsobem podstrčit něco „lechtivého", a téměř určitě sedne na vějičku.
- **Tajemství** – na chodbě firmy leží disketa a na ní je samolepka „Výplaty 2002/03". Dříve či později ji někdo zvedne a je velká pravděpodobnost (skoro až jistota), že příslušnou disketu vloží do počítače. Zvědavost vítězí. Samozřejmě jediný program na disketě spustí – a zároveň s tím si v příslušném okamžiku mohl nainstalovat do počítače nějaký nástroj pro útočníka.

Takto bychom mohli pokračovat – cílem předcházejícího seznamu nebyl výčet úplný, ale jen naznačení nejčastějších směrů, jimiž se sociální inženýři ubírají. Zkrátka a dobře, sociální inženýrství je metoda, která (ať se nám to líbí nebo ne) funguje.

Na sociálním inženýrství je přitom nejhorší skutečnost, že se proti němu špatně brání. Útočník si volí podobně jako v reálném světě čas, místo a způsob útoku, ale navíc to provádí způsobem, který na první pohled nemusí vypadat jako útok. A v tom je největší nebezpečí sociálního inženýrství – jedná se skutečně o manipulaci s lidmi. Některé tipy a triky, jak se bránit, ale přece jen existují:

- **Zachovejte si chladnou hlavu.** Nic není horší, než zbrklé chování – útočník to ví a počítá s tím. Opravdu je nějaký důvod ke spěchu?
- **Ověřujte, ověřujte, ověřujte.** Nikdy sice nedokážete ověřit všechny informace, ale v případě některých je to velice jednoduché a rychlé (jsou předkládaná tvrzení pravdivá/reálná?, je dotyčná osoba tím, za koho se vydává?).
- **Získejte informace a čas.** Někdo telefonuje a má neobvyklý požadavek? Vezměte si od něj číslo a zavolejte mu za pět minut (pokud nepracujete u hasičů, záchranky nebo na policii, pak se zpravidla nic nestane).
- **Buďte obezřetní.** I zdánlivě bezvýznamné informace mohou být v nesprávných rukou nebezpečné. Mám/mohu to dotyčné osobě sdělit?

Další opatření jsou pak spíše organizačního charakteru a měla by být řešena na úrovni organizace, nikoliv jednotlivce: vypracovat a dodržovat komunikační kanály, zajistit roztřídění informací (tajné, důvěrné, veřejné apod.), ověřování totožnosti zákazníků/dodavatelů atd.

Podtrženo, sečteno – sociální inženýrství bývá velmi často podceňovanou, a stejně tak nedoceňovanou metodou získávání informací. Velmi správně totiž předpokládá, že nejslabší články počítačových systémů se nacházejí mezi židlí a klávesnicí.

TOMÁŠ PŘIBYL

Útok na nejslabší článek – sociální inženýrství

Social engineering. Sociální inženýrství, nebo někdy také sociotechnika. Nesmírně nebezpečná technika (nejen) počítačového útoku, protože je zaměřena na nejslabší článek celého systému, kterým bývá až na čestné výjimky potvrzující pravidlo člověk. Jakmile selže „lidský faktor", jsou všechna implementovaná bezpečnostní opatření zbytečná.

Sociální inženýrství vychází z filozofie, že není nutné hledat žádné složité cesty, jak se dostat do počítačových systémů, když existují způsoby jednoduché. V reálném světě také není nutné vylamovat dveře od třinácté komnaty, když máte v ruce klíč. A proč se v informačních technologiích pokoušet o časově a znalostně náročné útoky, když se do systému lze dostat veskrze jednoduchým způsobem? Stačí přece znát heslo.

Že byste heslo nikdy nikomu neřekli? Za normálních okolností asi těžko. Když vás na ulici zastaví neznámá osoba a vybafne na vás „Heslo!", zřejmě odejde s nepořízenou. Ale pokud to provede poněkud rafinovanějším způsobem, má na úspěch velkou šanci. A dokonce si třeba ani neuvědomíte, že jste heslo prozradili. Sociální inženýrství je zkrátka umění. Umění s velkým „U".

Představte si následující případ. Přijde vám e-mailem zpráva, že jste si v internetovém obchodě E-Kvelb objednali to a to zboží v té a té ceně. Obchodní server ale potkal výpadek, takže si nejsme jisti správností našich dat a nabízíme vám možnost zrušit objednávku na alternativní adrese. Pokud ale objednávku nezrušíte do určeného času, bude příslušná částka stržena z vašeho bankovního účtu a zboží zasláno poštou. Vy se vyděsíte. Nic jste si neobjednali – a za to byste měli platit? Navíc je zde časový limit, takže je nutné jednat rychle. Alternativní web? Jaképak podezření, „spadlé" počítače jsou běžnou součástí kybernetického prostoru. Tak honem zadat požadované informace, hlavně abychom se vešli do časového limitu (který zpravidla není nikterak velkorysý). Sláva, stihli jsme to a zachránili své drahocenné finance!

Anebo to bylo úplně jinak? Vžijte se nyní do role útočníka, který potřebuje vyzískat třeba jakékoliv přihlašovací jméno a heslo pro přístup do internetového obchodu E-Kvelb. Získat e-mailové adresy (některých) zákazníků není tak složité, jak by se na první pohled mohlo zdát. Většina webových obchodů má u svých produktů i diskusní fóra, kde mohou zákazníci vyjádřit své názory. Vytvořit e-mail s falešnou adresou odesílatele (třeba obchod@e-kvelb.com) také není žádným problémem. Ostatně, dokáží to i primitivní počítačové viry jako třeba Sobig.F nebo Swen, tak proč by to nedokázal průměrně vzdělaný uživatel? A vytvořit webovou stránku s rozhraním, které se tváří jako přihlašovací formulář, jistě není na maturitu z programování, stejně jako její umístění na nějaký veřejně přístupný server.

Hotovo. Stačí jen odeslat e-maily a následně si z databáze vybírat přihlašovací jména i hesla, na jejichž kontu hodlám v E-Kvelbu nakupovat, a zboží si nechávat posílat na nějakou nastrčenou adresu (P.O.Box). Jakmile mám k dispozici heslo, mohu zpravidla změnit adresu odběratele i komunikační e-mail – ale byl bych blázen, kdybych měnil fakturační údaje.

Jak vytvořit opravdu dobré heslo

Vytvořit heslo? Nic složitého – vždyť je kolem nás tolik krásných věcí, jejichž jména můžeme použít. Stop! No právě!

Proč nemůžete jako heslo použít třeba jméno své babičky? Vždyť je nepravděpodobné, že by ho někdo znal. To je sice pravda, ale útočník stejně tak dobře nemusí a nepotřebuje vědět, že máte jako heslo nastavené právě jméno babičky. Prostě vyzkouší většinu běžně používaných slov – a mezi ně ženská jména rozhodně patří (tedy pokud vaše babička nepocházela z nějakého indiánského kmene). Že je to zdlouhavé a náročné? Omyl na druhou – v současném světě informačních technologií může potencionální útočník vyzkoušet tisíce slovíček během několika sekund.

Pokud chceme získat přístup do nějakého systému, je nejjednodušší získat právě heslo – a pak máte přístup otevřený. A jak se k heslu dostat? Je to celkem jednoduché. Lidé jsou líní a pohodlní – někdy nezadávají heslo žádné (prázdné heslo). Jindy zadají jako heslo slovíčko „heslo" (na to hned tak někdo nepřijde, že?). Velice často se lze setkat s tím, že jako přihlašovací login je příjmení a jako heslo křestní jméno (nebo naopak). Mnoho aplikací má zase defaultně nastavené heslo, a administrátoři se zpravidla neobtěžují jej měnit.

Chceme-li ale vytvořit heslo opravdu bezpečné, musíme si tyto skutečnosti uvědomit – útočníci si jich jsou každopádně vědomi. Zároveň je dobré si uvědomit, jakým způsobem se útoky provádějí. V prvé řadě je to tzv. slovníkový útok. Útočník prostě nasadí specializovaný software, který během krátké doby (desítek sekund či několika málo minut) vyzkouší většinu běžně používaných slov (v angličtině, v mateřském jazyce apod.).

Druhým typem útoku je tzv. útok hrubou silou. Ten je časově výrazně náročnější a dříve nebo později je úspěšný. Problém je v tom, že při použití dostatečně silného hesla (nebo ještě lépe password_phrase – heslové fráze či věty) může jeho prolomení trvat nereálně dlouhou dobu. Třeba i tisíce či statisíce let. Útok hrubou silou prostě zkouší všechny přípustné možnosti hesla. Pokud máte jednoznakové heslo, je otázkou kratičké doby vyzkoušet všechny možnosti. Pokud je heslo dvouznakové, už je možností, které je nutné vyzkoušet, na druhou tolik. V případě tří znaků na třetí atd. Jak vidno, počet možností roste geometrickou řadou.

Z těchto poznatků vyplývá několik pravidel pro vytvoření bezpečného i silného hesla a jeho každodenního používání:

- Heslo by mělo být dostatečně dlouhé (zpravidla se doporučuje osm znaků).
- Heslo by nemělo být tvořeno jakýmkoliv běžně používaným slovem.
- Heslo by nemělo být vytvořeno ve vztahu k uživateli (aby nešlo odhadnout).
- Heslo by mělo být co nejpestřejší (mělo by obsahovat číslice, speciální znaky, velká i malá písmena).
- Heslo si nikde nepoznamenávejte!
- Heslo pravidelně obměňujte!
- Heslo **nikomu za žádných okolností nesdělujte!!!**

A jeden drobný tip na závěr: snažte se nepoužívat v hesle písmena „z" a „y". Zvláště, pokud se pokaždé přihlašujete z jiného počítače (např. freemailová poštovní schránka). Nikdy nevíte, jaká je kde klávesnice a nepoznáte, zdali je správné heslo „********" nebo „********".

TOMÁŠ PŘIBYL

stupné. Osobně jsem já a mí rodiče kdysi vydali za počítač mnoho a mnoho peněz, ale dnes… Systémy jsou nyní k dispozici za zlomky ceny. A tak když chce někdo hackovat, není problém pořídit si dva počítače a dělat útoky mezi nimi. Já vím, není to ono, ale skutečné hackování nikomu nedoporučuji – následky mohou být velmi tvrdé.

Za rozhovor poděkoval a co nejméně bezpečnostních incidentů popřál

TOMÁŠ PŘIBYL 3 0628/FEL ❑