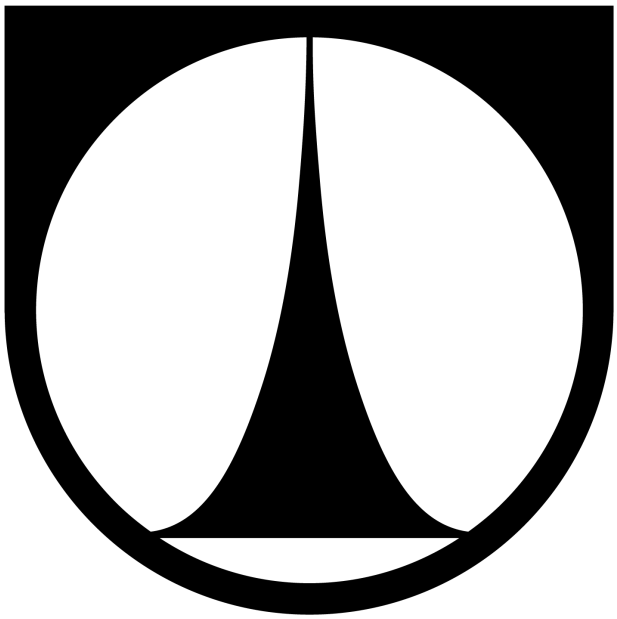
TECHNICKÁ UNIVERZITA V LIBERCI

Ekonomická fakulta



BAKALÁŘSKÁ PRÁCE

2013 **Petr Malina**

TECHNICKÁ UNIVERZITA V LIBERCI

Ekonomická fakulta

Studijní program: B6209 Systémové inženýrství a informatika

Studijní obor: Manažerská informatika

Sociotechnické aspekty komunikačních sítí

Sociotechnical aspects of communications networks

BP-EF-KIN-2013-15

Petr Malina

Vedoucí práce: Ing. Zbyněk Hubínka

Konzultant: doc. Ing. Klára Antlová, Ph.D., Technická Univerzita v Liberci

Počet stran: 62 Počet příloh: 2

Datum odevzdání: 10.5.2013

MÍSTO TÉTO STRANY VLOŽIT ZADÁNÍ

MÍSTO TÉTO STRANY VLOŽIT ZADÁNÍ

Prohlášení

Byl jsem seznámen s tím, že na mou bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, zejména § 60 – školní dílo.

Beru na vědomí, že Technická univerzita v Liberci (TUL) nezasahuje do mých autorských práv užitím mé bakalářské práce pro vnitřní potřebu TUL.

Užiji-li bakalářskou práci nebo poskytnu-li licenci k jejímu využití, jsem si vědom povinnosti informovat o této skutečnosti TUL; v tomto případě má TUL právo ode mne požadovat úhradu nákladů, které vynaložila na vytvoření díla, až do jejich skutečné výše.

Bakalářskou práci jsem vypracoval samostatně s použitím uvedené literatury a na základě konzultací s vedoucím bakalářské práce a konzultantem.

V Liberci, 10. 5. 2013

_____

Petr Malina

ANOTACE

Předmětem bakalářské práce *Sociotechnické aspekty komunikačních sítí* je seznámení se s sociotechnikou a nebezpečí s ní související. Bakalářská práce je rozdělena do tří částí.

Teoretická část se zabývá základními pojmy sociotechniky a obsahuje příklady sociotechnických útoků.

Praktická část se věnuje nejrizikovějším oblastem, které byly nejvíce ohroženy během mé informatické praxe. Tato část obsahuje i způsoby, kterými byla firma zabezpečena proti sociotechnickým útokům.

V poslední části jsou popsány způsoby prevence před těmito typy útoků a způsoby, jak taková zabezpečení vytvořit a ochránit firmu před zbytečnými problémy.

Cílem této práce je analýza komunikačního prostředí, způsoby možných útoků a shrnutí této problematiky v podnikatelské sféře.

KLÍČOVÁ SLOVA

Sociální inženýrství, phishing, elektronické bankovnictví, komunikační prostředí, zabezpečení

ANNOTATION

The subject of the bachelor thesis Sociotechnical aspects of communication networks is an introduction to sociotechnics and its threats. The bachelor thesis is divided into three parts. The theoretical part deals with basic concepts of sociotechnics and contains examples of sociotechnical attacks.

The practical part is devoted to the most dangerous areas that were most at risk during my informatics practice. This section includes the ways in which the company was protected against sociotechnical attacks.

The last section describes how to prevent these types of attacks and ways to create such precautions and to protect a company from unnecessary problems.

The aim of this work is to analyze the communication environment, the possible attacks and to summarize this issue in business.

KEY WORDS

Social engineering, phishing, e-banking, communication environment, security

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM POUŽITÝCH ZKRATEK

CFO	„*Chief financial officer*“; finanční ředitel
CIO	„*Chief information officer*“; ředitel IS/IT
ČSOB	Československa obchodní banka, a.s.
ČSSZ	Česká správa sociálního zabezpečení
ICQ	„*I seek you*“; volně dostupný program umožňující komunikaci mezi uživateli v reálném čase
IRC	„*Internet relay chat*“; systém umožňující komunikaci v reálném čase mezi více lidmi
ISO	„*International standard of organization*“
http	„*Hypertext transfer protocol*“
https	„*Hypertext transfer protocol secure*“
Ssl	„*Secure sockets layer*“; bezpečnostní protokol pro přenos dat přes internet
Tls	„*Transport layer security*“; způsob přenášení a kódování dat při komunikaci přes internet

ÚVOD

Předmětem této bakalářské práce s názvem *Sociotechnické aspekty komunikačních sítí* je získání podvědomí o tom, co samotná sociotechnika je, a nahlédnutí do problémů, které může sociotechnika a její metody způsobit. Bakalářská práce je rozdělena do tří částí. Teoretická část definuje sociotechniku, způsoby jejího použití, využívané metody v sociotechnice a charakterizuje společnost, která může být sociotechnikou zneužita. Praktická část analyzuje používaní bezpečnostních opatření a poukazuje na útoky, které jsou typickými příklady útoku sociotechnika. Poslední část, vyhodnocení, je věnována návrhům bezpečnostních opatření, která by zabránila útokům a dostala do povědomí společnosti následky takové situace.

Cílem bakalářské práce je interpretace analýzy komunikačního prostředí, zda si jsou lidé vědomi, co mohou svými činy způsobit. Je důležité dostat do povědomí společnosti, že sociotechnika vůbec existuje a každý se může stát obětí sociotechnického útoku. Většina obětí si ani neuvědomuje, že by se zrovna ony mohly stát cílem těchto útoků a prozradit důležité informace. S rychlým vývojem moderních technologií by lidé měli být na pozoru a ověřovat si, komu dané informace poskytují. Každá informace, i sebelépe zabezpečená, může být nevědomky zvěřejněna a zneužita neoprávněnými osobami.

1 SOCIOTECHNIKA

Sociotechnika je definována následujícími způsoby:

„*Sociální inženýrství nebo-li sociotechnika je ovlivňování a přesvědčování 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 využít lidi, se kterými hovoří, případnš dodatečné technologické prostředky, aby získal hledané informace.*“ [citováno z 1]

„*Sociotechnia, nebo také sociální inženýrství, je technika, která má za úkol oklamat lidi, zmanipulovat je, přesvědčit je, že činí dobře. Tato negativni manipulace lidí, se zpravidla vykonává v síti internet. Útočník zpravidla používá, ke svým útokům především e-mail, ICQ. V některých případech může útočník použít telefon, nebo dokonce osobní schůzky.“* [citováno z 8]

„Hlavná myšlienka sociotechniky je: "Prečo sa obťažovať používaním brutálnej sily na prelamovanie hesiel, keď je jednoduchšie prinútiť niekoho, kto heslo (a/alebo akúkoľvek žiadanú informáciu) vie, k tomu, aby nám ho povedal?" Navyše pri dobre vedenom útoku si obeť v drvivej väčšine prípadov vôbec neuvedomí, že niečo vyzradila nepovolanej osobe.“ [citováno z 9]

Sociotechnikou můžeme tedy nazvat jakékoliv *informační pirátství*. Informace obdržené tímto způsobem nejsou kradené, ale nečestně získané od obětí. Bohužel zde hraje nejvýznamnější roli lidský faktor, který selže podáním daných informací. Sociotechnici si toto velmi dobře uvědomují, a proto jsou tak nebezpeční. Jsou to lidé, kterým nedělá problém přetvařování, předstírání, lhaní, využívání jiných, někdy i blízkých osob. Sociotechnici mají silně vyvinutou manipulační schopnost, dokáží člověka ovlivnit a přesvědčit o své pravdě. Informace můžeme mít dokonale zabezpečené nejnovějším

bezpečnostním systémem, ale pokud selže lidský faktor, ani nejlepší zabezpečení nepomůže.

Existuje mnoho metod, jak chtěné informace získat. Vždy se jedná o důkladný a propracovaný plán, jak se k těmto informacím dostat. Úspěšní sociotechnici si předem promyslí, co potřebují získat, a podle toho naplánují útok. Dokonale si prostudují prostředí, ve kterém se oběti pohybují, nebo také žargon, aby jejich vstup nebyl nápadný a oni zcela zapadli v okolí. Sociotechnici mají velmi dobré přesvědčovací a manipulační schopnosti.

Základní postup sociotechniků lze popsat následujícími kroky. Nejprve si sociotechnici vybírají cíl a informace, ke kterým se potřebují dostat. S využitím svých schopností tyto informace ve většině případů získají a shromažďují je. Jako základ sociotechnického útoku výborně poslouží využití veřejných zdrojů, například internetové stránky, které poskytují jména, příjmení a funkce zaměstnanců v dané firmě. Zdálo by se, že tyto informace mají pouze omezený charakter, ale opak je pravdou. Studie struktury zaměstnanců umožní útočníkům vžít se do role vrcholného manažera, kterému se podřízení snaží maximálně vyjít vstříc a nepřidělávat si problémy. Pokud má firma více poboček, zaměstnanci znají často pouze jména svých kolegů, a tak není důvod někoho podezřívat a důležité informace mu neposkytnout. Pokud tento plán zabere, sociotechnici brzy znají nejen informace, které chtěli, ale i ty, o které nežádali.

Mezi důležitou fázi plánu patří vhodné zvolení a rozvrhnutí otázek obětím. Pokud sociotechnik zakomponuje správným způsobem, pro něho důležité, otázky mezi běžný hovor, je velmi těžké takové otázky odhalit. Sociotechnik nikdy neukončuje rozhovor ve chvíli, kdy získá odpověď na svou otázku. Po obdržení důležité informace uvede ještě pár dodatečných zdvořilostních otázek a hovor s přáním příjemného dne ukončí. Tím odvrátí pozornost od skutečného důvodu hovoru. Výsledkem je prakticky nulové podezření oběti a sociotechnik získal potřebné informace.

2 HISTORIE

Sociotechnika prochází vývojem již tisíce let. Od pradávna si lidé na sebe brali podobu jiné osoby, aby zmanipulovali okolní svět. Také rodiče donutí své dítě udělat něco, co původně ani samo nechtělo, a stačilo k tomu použít správného slibu, aj.

Samotný termín začal používat až Kevin Mitnick. Narodil se 6. srpna 1963 v Los Angeles v San Fernando Valley. Již od mládí se učil dělat věci rozdílně od ostatních mladistvých. Mohl jezdit městskými autobusy či telefonovat zdarma. „*Byl označen jako nejlepší hacker v dějinách. Ukradl několik tisíc souborů s daty a nejméně 20 000 čísel kreditních karet. Odcizil tisícovky megabajtů chráněného softwaru. Naboural se do počítače Severoamerické velitelství protivzdušné obrany. Nabourával se do ústředen mezinárodních korporací. Získal přístup k obchodním tajemstvím v hodnotě milionů dolarů. Odcizil data týkající se nejnovější generace elektronických zabezpečení a supertajných nástrojů používaných bezpečnostními orgány. Byl schopen odstranit svá data z elektronických policejních záznamů, naboural se přes bezpečnostní systémy do počítače jednoho z nejlepších odborníků na počítačová zabezpečení. Kevin Mitnick byl jednou z nejhledanějších osob v historii FBI. Po zatčení mu hrozil trest několik set let odnětí svobody, přestože nikdy nebyl obviněn z toho, že by měl z hackerství finanční prospěch. Soudním výrokem mu byl zakázán jakýkoliv přístup k počítači. Soud odůvodnil rozsudek slovy: „Vyzbrojen klávesnicí je nebezpečím pro společnost“. Po propuštění Mitnick úplně změnil svůj život. Stal se nejvyhledávanějším expertem zabezpečení počítačových systémů v USA. Ve své knize “Umění klamu” odhaluje tajemství svého “úspěchu”, popisuje, jak snadné je překonat zábrany a získat přísně tajné informace, sabotovat podniky, úřady či jakékoliv jiné instituce. Několiksetkrát tak učinil za pomoci důmyslných technik ovlivňování lidí. Mitnick dokazuje, jak klamná je představa bezpečnosti soukromých i služebních dat, ukazuje, jak obejít systémy za miliony dolarů zneužitím lidí, kteří je obsluhují.“* [citováno z 10]

3 METODY SOCIOTECHNIKŮ

K tomu, aby byl útok sociotechnika úspěšný, používá několik základních vlastností:

- **Přesvědčivost:** Mezi hlavní vlastnosti patří schopnost přesvědčit cizí osobu, že sociotechnik je ten, za koho se vydává. Čím méně je útočník podezříván, tím větší má pravděpodobnost úspěchu.
- **Přátelskost:** Sociotechnik nesmí být příliš útočný, neboť jakmile je oběť nucena se bránit, není příliš ochotna sdílet informace. Naopak, pokud se útočník bude chovat přátelsky, ke sdílení informací směrem k sociotechnikovi je cesta otevřena, protože ochota sdílet informace s kolegou z práce je možnost ke zlepšení jejich vztahu.
- **Odpovědnost:** Pokud při komunikaci útočník zmíní během rozhovoru jména spolupracovníků, či dokonce jméno nadřízeného, oběť nemá pocit, že veškerá tíha leží jen na něm a je sdílnější. Očekávání odměny od nadřízeného je obrovskou motivací, a tak nic nebrání informace předat. Ve výsledku oběť může dokonce pomoci a prozradit více, než byl původní plán útočníka.
- **Autorita:** Lidé mají tendenci se podřídit či přizpůsobit osobě, která má moc. Může se podřídit žádosti nebo příkazu, pokud uvěří, že osoba je skutečně ta, za kterou se vydává, a zároveň má oprávnění toto žádat. Lidé obecně mají respekt před osobami s vyšším postavením a přizpůsobí se jejich hře.
- **Sympatie:** Každý má sklon vyhovět, pokud je druhá osoba se schopna ukázat jako sympatická osoba. Např. podobné názory, zájmy nebo problémy mohou pomoct k prozrazení důležité informace. Vytváří tím zdání podobnosti a oběť s takovou osobou ráda spolupracuje. Dalším důležitým faktorem je příjemné vystupování. Muži i ženy dokáží zapomenout na přísná opatření, pokud jim protějšek na druhé straně vyjadřuje sympatie.[1,3,4]

3.1 Přímý útok

Útočník přímo požádá o informaci, po které touží. Může se přímo zeptat na uživatelské jméno a heslo. Tento způsob se může zdát riskantní, ale často je velmi účinný. Tento typ útoků se používá především na osoby s nižším postavením v určité časové tísni. Příkladem může být recepční, která v době útoků musí obsluhovat mnoho osob a nemá dostatek času na dodržování všech bezpečnostních postupů.

V současné době je velice populární postupné získávání důvěry pomocí různých sociálních sítí nebo internetových her. Postupem času si útočník vybuduje kybernetické přátelství, které může vyústit ve sdílení přístupu k jejich účtu. Může také navrhnout použití vlastního programu na zlepšení komunikace a získat tak plný přístup k počítači oběti.[1]

3.2 Nový zaměstnanec

Nový zaměstnanec společnosti je pro sociotechnika ideální osobou pro uskutečnění útoku. Neznalost správných bezpečnostních pravidel může zapříčinit lehký přístup k citlivým informacím. Nikoho nenapadne, že by právě on mohl být terčem útoku jen týden po tom, co byl přijat do nového zaměstnání. Útočník se například představí jako pracovník IT oddělení a bude ho seznamovat s bezpečnostní politikou. Zeptá se ho, jaké má heslo, aby zjistil, jestli je dostatečně odolné. Po získání hesla sdělí, že je dostatečně silné a aby dodržoval stejný postup vytváření hesla při jeho další změně.[1]

3.3 Interní zaměstnanci

Interní zaměstnanci nejsou většinou obětí útoků, ale právě těmi, kteří takový útok provedou. Bývalý zaměstnanec se může chtít mstít svému bývalému zaměstnavateli, a tak může smazat důležitá data pro chod firmy nebo prodat data o připravovaném novém produktu konkurenční firmě. Další možností může být konkurenční boj a nasazení zaměstnance do firmy jako černého koně. Ten bude mít za úkol získávat důležité informace a využít je pro vylepšení produktu, bez nutnosti investovat do výzkumů a technologií. Bývalý zaměstnanec také může zatoužit po vlastní firmě, ve které by se mu data z této firmy hodila.[1,2]

3.4 Pracovník oddělení IT

Další typ útoku je veden pod falešným jménem pracovníka oddělení IT. Tyto osoby nejsou většinou známy osobám z jiných oddělení, a tak je nepravděpodobné, že by je mohla oběť osobně znát. Útok může být znovu zacílen na nové zaměstnance, ale ani starší zaměstnanci nemusí být příliš obezřetní a nechají se polapit. Často se jedná o zaslání e-mailové zprávy a kontrolu přístupu na stránky společnosti. Stránka může vypadat stejně jako přihlašovací stránka, a tak bez problému zadají své přístupové údaje.[1]

3.5 Zvědavost

Záznamové médium může být také jednoduchým způsobem, jak získat přístup k informacím. Pokud zaměstnanec najde v blízkosti svého pracoviště CD s nápisem „Výplaty zaměstnanců srpen 2011“, těžko asi odolá pokušení zjistit, kolik bere jeho kolega

nebo jeho nadřízený. Do počítače se po spuštění souboru nainstaluje virus typu trojský kůň[1] a veškerá činnost na počítači je monitorována útočníkem. Zvědavost může být také spojena se sociálními sítěmi. Šokující videa nebo fotky jsou silným lákadlem, kdy tyto stránky mohou také obsahovat trojského koně.

3.6 Telefonní útoky

Telefonní útoky patří mezi jednu z nejstarších metod a řadily se mezi nejoblíbenější a nejúčinnější zbraně. Volající útočník je v částečné anonymitě, což mu umožňuje předstírat emoce bez větších problémů a jeho skutečná podoba je skrytá. Sociotechnik použije veřejně dostupné informace, které lze zjistit a využít v jeho prospěch.[1,3]

3.7 Osobní útoky

Mezi velmi časté sociotechnické útoky patří osobní kontakt, kdy sociotechnik využívá svých předností a manipulačních schopností přímo osobně. Stačí se pěkně obléknout, zjistit informace o daném prostředí a nic nebrání k příjmu nových informací.

3.8 Obrácená sociotechnika

Útočník předem zaranžuje problém. Představí se například jako pracovník technické podpory a pomůže tento problém vyřešit. Během odstraňování problémů vyláká

1 Trojský kůň je škodlivý počítačový program, který může bez vědomí uživatele např. krást data,upravovat soubory nebo sledovat veškeré dění na daném PC.

přihlašovací údaje a další důležité informace. Další možnost je navést uživatele, aby sám do počítače nainstaloval program, který budoucím problémům zamezí. Tento program je většinou trojský kůň a útočník tak získá plný přístup do počítače.[1]

3.9 Internetová sociotechnika

Mezi dnešní nejúčinnější a nejnebezpečnější zbraně patří internet. Lidé používající internet jsou v úplné anonymitě a prakticky nemají žádné omezení k získávání dat. Sociotechnik nemusí mít až tak rozvinuté vlastnosti sociotechnika, protože absolutní anonymita zajišťuje bezpečí. Mezi nejznámější internetové útoky patří využívání e-mailových schránek nebo jiných komunikačních nástrojů.[1,2]

4 INTERNETOVÁ KOMUNIKACE

Mezi nejčastější nástroje současné sociotechniky patří internet. Dnešní doba je tomu přímo nakloněná. Dříve byly využívané komunikační nástroje, např. ICQ, IRC nebo i internetové chatovací stránky, např. xchat.cz apod. Metoda však vyžadovala určitou dávku trpělivosti, neboť je potřeba vybudovat si vztah s obětí.

Dnes k tomu přímo vybízí sociální sítě. Facebook, Twitter a jim podobné stránky jsou pro sociotechnika ráj. Lidé dobrovolně na těchto stránkách sdílejí svoje osobní data. Kde bydlí, pracují, s kým se vídají, kam chodí za zábavou. Cizímu člověku na ulici by ani neodpověděli, ale on si je může bez větších problémů najít na jejich profilu sám. Sociální síť Facebook je založena na profilech se skutečnými jmény a pravdivými informacemi. Kdo ale zaručí, že dané jméno skutečně existuje a není to pouze podvod?

Velký podíl má stále elektronická pošta. Využívá se metoda tzn. „phishingu“. Phishing je druh internetového podvodu, kterým se útočníci například snaží z uživatelů internetového bankovnictví vylákat přístupové údaje k účtům a zneužít je pro své obohacení. K získání těchto důvěrných informací využívají podvodné e-maily, které na první pohled vypadají, že jsou odeslány přímo z banky, a snaží se přesvědčit uživatele, aby kliknul na odkaz, který vede na falešné stránky. Žádná instituce operující s osobními daty nikdy nežádá po svých klientech, aby sdělili své přihlašovací údaje. Má vlastní prostředky, jak si je může získat a uživatele k tomu vůbec nepotřebuje.[3,5]

Obr. 1: Phishingový e-mail napodobující komunikaci České spořitelny. [4]

Na obr. 1 lze vidět hromadně zaslaný e-mail. Neznalý uživatel klikne na odkaz a zobrazí se mu napodobenina stránky internetového bankovnictví České spořitelny. Na obr. 2 vypadá tato stránka přesně, jako přihlašovací stránka České spořitelny. Pokud se ale podíváme podrobněji, webová adresa není skutečná stránka České Spořitelny. Další viditelnou chybou je, že stránka není zabezpečena pomocí protokolu https[2] [6]. Často se zde také vyskytující gramatické či stylistické chyby. Jakmile by uživatelé nebyli obezřetní, zadají uživatelské jméno a heslo a majitel falešné stránky získal plný přístup k internetovému bankovnictví daného uživatele.

2 Https je šifrovanou variantou internetového protokol pro přenos webových stránek. Https umožňuje chráněný přístup k serveru pomocí sífrovaných algoritmu SSL nebo TLS.

Obr. 2: Phishingový e-mail napodobující přihlašovací stránky České spořitelny. [5]

5 ADVANCED PERSISTENT THREAT

Dalším důležitým pojmem je Advanced persistent threat (dále jen APT). Útok APT je podle [11] definován následovně:

„An APT is a network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time. The intention of an APT attack is to steal data rather than to cause damage to the network or organization. APT attacks target organizations in sectors with high-value information, such as national defense, manufacturing and the financial industry. In a simple attack, the intruder tries to get in and out as quickly as possible in order to avoid detection by the network's intrusion detection system . In an APT attack, however, the goal is not to get in and out but to achieve ongoing access. To maintain access without discovery, the intruder must continuously rewrite code and employ sophisticated evasion techniques. Some APTs are so complex that they require a full time administrator.“

„An APT attacker often uses spear fishing, a type of social engineering, to gain access to the network through legitimate means. Once access has been achieved, the attacker establishes a back door. The next step is to gather valid user credentials (especially administrative ones) and move laterally across the network, installing more back doors.“ [citováno z 11]

V českém jazyce by se definice APT útoku dala přeložit následovně:

APT je internetový útok, ve kterém útočník získá přístup a zůstane v síti po delší dobu. Úmyslem je ukrást data namísto způsobení škody organizaci nebo síti, kde je útok veden. Cílem těchto útoku jsou sektory s velkým množstvím informaci, tedy národní bezpečnost, výrobní podniky a finanční odvětví. Normální útoky mají za cíl se co nejrychleji dostat do systému a ven, aby se zamezilo jejich odhalení. Naproti tomu APT útoky jsou zacíleny

na získání trvalého přístupu. K dosažení přístupu bez odhalení musí útočník neustále měnit svůj zdrojový kód a techniku skrývání v systému. Některé APT útoky dokonce vyžadují neustálou uživatelskou správu.

Útočník většinou používá „spear phishing“[3], tedy jednu z metod sociotechniky. V okamžiku, kdy útočník získá přístup, vytvaří si „zadní vrátka“.

(*Přeloženo z anglického textu,* [11])

3 Spear phising je speciální druh phishingu, který je přímo určený na konkrétní jednotlivce. Nejedná se tedy o hromadný útok. Útok je většinou veden pod falešným jménem někoho z vedení společnosti a je adresován zaměstnancům s cílem získat důležitá data a informace.

6 ÚTOKY NA KOMUNIKAČNÍ PROSTŘEDÍ

6.1 Důvody pro útok

Hlavní motivací je získat informace, které nejsou útočníkovi přístupné. Získat lze například výhodu před kolegou, před konkurencí nebo jen pro lepší mínění u nadřízeného či zaměstnavatele. Finanční odměna také bývá častou motivací.

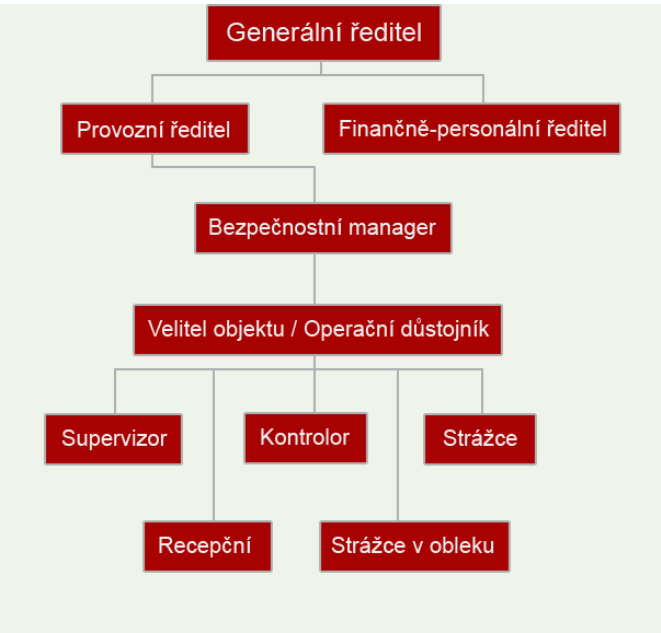
Nejmodernější způsoby zabezpečení počítačových systémů jsou již skoro dokonalé. Jejich rozšíření a dostupnost je masová. Díky nim jsou přímé způsoby[4] útoků málo úspěšné a riziko odhalení je mnohonásobně větší než při využití sociotechniky. Při útoku na propracovaný bezpečnostní systém přímým způsobem je zapotřebí dokonalá technická zdatnost. Pokud však můžeme tyto informace získat pomocí propracovaných triků, stačí pouze důmyslný plán, jak lstí získat informace.

Velkou výhodou je pro útočníky nevědomost oběti. Každý přímý útok je v systému viditelný. Systematicky dobře provedený útok sociotechnika je nedohledatelný a informace může být použita až ve chvíli, kdy je potřebná. Důvodem může být i pouhá zvědavost útočníka či potřeba dokázat si, zda je to možné.

4 Přímé způsoby se označují metody útoky, kdy se útočník naboural do počítače pomocí různých programů nebo díky špatným bezpečnostním opatřením.

6.2 Nejzranitelnější místa

Pro názorné vysvětlení nejzranitelnějších míst informačního systému využiji hierarchii pozic zaměstnanců firmy Komtur security s.r.o (viz. Obr. 3). Na této struktuře lze přehledně popsat rozvržení pozic zaměstnanců, jelikož je jedním z nejčastěji využívaných schémat.



Obr. 3: Hierarchie zaměstnanců, firma Komtur security s.r.o.

Ačkoliv je sociotechnika v podvědomí každého bezpečnostního manažera, obměna personálu nese velká rizika. Pracovníci na nejnižších postech jsou největším bezpečnostním rizikem. Čas potřebný na proškolení nového zaměstnance je období, kdy zaměstnanec není seznámen s bezpečnostními postupy a útok na něj má velkou pravděpodobnost úspěchu. Terčem útoku jsou také pracovníci tzv. „help desk“[5]. Jsou naučeni asertivnímu chování a jsou školeni, aby se snažili vyhovět veškerým dotazům. Ochota pomoci je jejich pracovní náplní, sociotechnikovi tedy nic nebrání k získání informací.

5 Help desk je systém, která nabízí možnost položit dotaz či sdělit problém a dosáhnout jeho rychlého vyřešení díky vhodnému směrování dotazu.

7 ÚTOKY – HISTORICKÉ I SOUČASNÉ

Mitnick se ve své knize [3] z velké části věnuje úspěšným útokům. Pro představu jich několik uvedu jako příklady a názorně vysvětlím, proč jsou tak úspěšné. Podrobněji jsou příklady popsány v příloze.

7.1 Eric Mantini

Eric byl soukromý detektiv a jeho sociotechnická dovednost mu v práci hodně pomáhala. Využil veřejně dostupné informace, aby z policisty na telefonu získal tajné číslo. Toto číslo bylo policisty využívano pro komunikaci mezi vyšetřovateli a dopravní policií. Nyní už jen potřeboval získat přístup do telefonní ústředny. Zavolal tedy na telefonní ústřednu a představil se jako zaměstnanec společnosti, která tyto ústředny spravuje. Vymyšlená historka o aktualizaci firmwaru na dálku byla zřejmě dostatečně dobře podaná, a tak číslo pro správu ústředny získal. Heslo pro přístup na tuto telefonní ústřednu bylo velice triviální a bylo prolomeno během pár pokusů. Telefonní ústřednu upravil tak, že číslo přesměroval na svůj telefon. Každý policista, který na toto telefonní číslo volal, se představil a legitimoval. Bylo k tomu potřeba jméno policisty, oddělení kde pracuje, číslo řidičského průkazu a datum narození. Soukromý detektiv tedy získal od policistů jejich identifikační údaje. Jakmile získal pár takovýchto přístupů, vrátil nastavení ústředny do původního nastavení, aby nevzbudil podezření. Poté mohl získávat informace o konkrétních osobách pomocí přístupů policistů. [3]

7.2 Craig Cogburn

Craig byl průmyslový špión. Jeho úkolem bylo získat informace o tajném připravovaném projektu *Umělá srdeční chlopeň*. Aby získal informace o členech projektu, stačilo zavolat na ústřednu firmy a zeptat se. Ochotná recepční mu informace předala, aniž by věděla, kdo je na druhé straně telefonní linky. Jednoho z členů požádal o číslo na vedoucího projektu. Ten byl však na dovolené a zaskakovala za něj jeho sekretářka. Zmínil se o specifikacích projektu a sekretářka mu poskytla všechny důležité informace a dokonce i něco navíc. Bez problému poslala neznámému člověku seznam všech e-mailových adres výzkumného týmu. Poté využil pracovníka IT oddělení k nastavení vzdáleného přístupu. Jeden z počítačů nebyl dostatečně zabezpečený, a tak měl nyní plný přístup ke všem informacím. [3]

7.3 Escrow účet[6]

Výstavba nového zdravotního střediska v USA vyžadovala velké množství peněz. Dvě americké společnosti se dohodly na kontraktu této výstavby. K tomuto účelu byl vytvořen escrow účet. Kopie této dohody byla umístěna na internetové stránky jedné ze společností. Na stránkách byly zveřejněny veškeré potřebné informace včetně jmen a podpisových vzorů obou stran. Útočník tedy využil možnosti a postupnými kroky se pokoušel převést peníze. Změnil faxové číslo na žádosti k převodu peněž a správce escrow účtu při jakýchkoliv pochybnostech kontaktoval právě útočníka. Po odcizení částky přesahující 2 miliony dolarů nevzbuzovaly stále žádné podezření. Částky postupně zvyšoval a až při šestém pokusu o útoku byl podvod odhalen. [6]

6 Escrow účet je druh účtu, z něhož je možné čerpat pouze při splnění určitých podmínek stanovených ve smlouvě. Většinou používán při nákupu drahého zboží ze zahraničí nebo při nákupu nemovitostí. O tento účet se stará důveryhodná instituce.

7.4 Test zabezpečení společnosti

Ředitel jedné americké společnosti se rozhodl otestovat svou vlastní firmu. Požádal jednoho z amerických expertů na internetovou kriminalitu. Expert pod jménem hlavního IT administrátora firmy zavolal na menší pobočku a informoval o zavirování systému. Tento virus měl způsobit zpomalení systému v případě velkého zatížení. Tento symptom se samozřejmě objevil, nezávisle na zavirování systému. Navštívil tedy tuto pobočku jako interní zaměstnanec, aby problém odstranil. Nahrál do tohoto počítače vlastní virus. Postup opakoval v dalších menších pobočkách. Po měsíci navštívil opět ředitele, aby vyhodnotili stav zabezpečení. Ze všech navštívených poboček mu přišel e-mail o úspěšném napadení. [7]

Jak můžeme vidět na uvedených příkladech, získat důležité informace nemusí být vždy tak složité. Někdy se stačí přímo zeptat, jindy postačí se jen představit jako ta správná osoba a dozvíme se často i víc, než jsme původně vůbec zamýšleli.

8 SOCIOTECHNIKA BĚHEM INFORMATICKÉ PRAXE

Každý z nás se s útokem sociotechnika s velkou pravděpodobností již někdy setkal, ať vědomě či ne. Jak jsem se již dříve zmínil, jedním z nejčastějších způsobů jsou phishingové útoky. Důvodem pro tyto útoky je především nenáročnost na přípravu takového útoku. Zneužití vzhledu webové stránky velké banky není težké. Během své informatické praxe jsem s takovými útoky měl také zkušenost. Jednalo se však o hromadné zprávy, které byly už od pohledu rozdílné od skutečného vzhledu a dalo se je snadno rozpoznat.

8.1 Informatická praxe

Firma, kde jsem vykonával informatickou praxi, se zabývala především fyzickou ostrahou objektů. Komunikační sítě byly jedním z hlavních způsobů komunikace mezi firmou a zákazníky a bylo tedy potřeba se zaměřit na důkladné zabezpečení. Nejvíce ohroženým prostředím je internet, protože je komunikace prostřednictvím tohoto způsobu je velice rychlá a množství předaných informací je v podstatě neomezené. Nejpoužívanějšími oblastmi byly e- mailové zprávy, internetové bankovnictví, elektronické podpisy a datové schránky. Většina těchto oblastí se prolíná, a tak podcenění zabezpečení v jedné oblasti může mít fatální dopady na ostatní.

8.2 E-mail

Nejpoužívanějším způsobem komunikace prostřednictvím internetu je e-mail. Slouží k elektronické komunikaci, odesílání a přijímání elektronických zpráv včetně přiložených souborů. Výhodou je hlavně rychlost této komunikace, která se většinou blíží k pár

vteřinám. V dnešní době je již skoro samozřejmé, že každý z nás má alespoň jednu e-mailovou schránku. O to větší nebezpečí se za tím skrývá. Čím více aktivních uživatelů vlastní e- mailovou schránku, tím je větší pravděpodobnost selhání jedince, který tento e-mail používá. Druhou bezpečnostní hrozbou je jednoduchost této komunikace. Stačí se přihlásit do své schránky, jednoduše vybrat zprávu, kterou chceme zobrazit, a obsah zprávy nám je zobrazen. Zde platí přímá úměra. Čím je obecně něco jednodušší, tím méně jsme obezřetní.

Nyní popíšu podrobněji nejčastější způsoby, kterými jsou e-mailové zprávy napadeny. Jak jsem již dříve zmínil, phishing patří k nejvíce používaným způsobům. Tato metoda spoléhá na chybu uživatele, který si neověří základní informace o přijaté e-mailové zprávě. Uživatel uvěří zdánlivě stejnému vzhledu stránky a považuje zprávu za důvěryhodnou.

Zjednodušeně řečeno, každá e-mailová zpráva se skládá ze tří částí. Odesílatel, předmět a obsah zprávy. Rád bych rozebral část, kde se zobrazuje odesílatel zprávy. Odesílatel zprávy je většinou zobrazen v normalizovaném formátu, např. *petr.malina@tul.cz*. Znak @ se nazývá oddělovač, část před ním většinou označuje uživatelské jméno, část za oddělovačem určuje server a zemi, ze které daná e-mailová schránka pochází. Většina e- mailových klientů a webových e-mailových stránek má však primárně zobrazeno jméno. Pokud si jméno sami neurčíme, automaticky se zobrazuje *petr.malina@tul.cz*. Pokud si ale své jméno změníme v nastavení, např. na *MUDr. Jan Novák*, příjemce zprávy tedy uvidí, že odesílatel je *MUDr. Jan Novák*.

Proti tomuto způsobu útoku je více možností ochrany. Stačí v e-mailovém klientu nebo na webové stránce nastavit, aby se zobrazovalo jméno i e-mailová adresa. Tímto způsobem rovnou uvidíme, že odesílatel je skutečně ten, za kterého se vydává, a nyní můžeme věřit obsahu zprávy.

Druhou možností je filtrování zpráv. Příkaz filtru by mohl vypadat následovně: *Jakmile zpráva obsahuje text „ČSOB“, ověř, zda odesílatel za oddělovačem obsahuje „csob“.*

Pokud ano, ulož zprávu do normálního adresáře „Doručená pošta“. Jakmile odesílatel text „csob“ za oddělovačem neobsahuje, přesuň zprávy do „Nevyžádaná pošta“. Tyto zprávy je nutné často kontrolovat, zda nebyly chybně přesunuty důležité zprávy. Pokud by ale útočník s tímto krokem počítal, mohl by si založit e-mail, který by byl zdánlivě hodně podobný, ale přesto rozdílný. E-mailová adresa může vypadat např. *csob@csob1.cz*. Je nutné tedy filtrování e- mailových zpráv upravit, aby za oddělovačem zprávy mohly obsahovat pouze *csob*, tedy žádný znak před ani za, pouze přípona příslušného státu, v našem případě tedy *cz.*

Další nebezpečnou částí e-mailové zprávy může být i samotný obsah. Pokud by odesílatel byl někdo jiný, může po nás vyžadovat například přihlášení do internetového bankovnictví. Důvodem pro toto přihlášení může být schválení změny bezpečnostních informací, zamítnutá transakce nebo nutná změna hesla. Odkaz, který bude obsah zprávy obsahovat může vypadat následovně „www.csob.cz“. Tento odkaz však nebude adresovat na stránku, která je nám viditelná. Hypertextové odkazy lze jednoduše upravit, aby odkazovaly na jinou stránku, ale v textu zprávy se bude zobrazovat jako odkaz na stránky ČSOB. Skutečná adresa bude např. http://www.testuk.ru/savedoc.php. Tato stránka bude vypadat přesně stejně jako přihlašovací stránka na internetové bankovnictví. Vyplněním těchto informací by uživatel předal své soukromé přihlašovací údaje útočníkovi.

Nemusí se jednat pouze o cizí e-mailové adresy, které mohou napadnout počítač nebo na takovéto stránky odkázat. V případě, že by některý uživatel uložený v adresáři kontaktů klikl na zavirovaný odkaz, může být jeho počítač použit jako odesílatel viru. Jedná se o virus typu trojského koně. Tento virus poté všem uloženým kontaktům v adresáři odešle znovu tuto zprávu, která obsahuje trojského koně.

Znovu zopakuji základní pravidlo, žádná banka nikdy nepožaduje po svých klientech zveřejnění jejich přístupových údajů. Zároveň nikdy neinformuje o důležitých změnách nebo chybách prostřednictvím e-mailu. Toto samozřejmě platí i pro telefonní hovory.

Právě těmito způsoby jsem během své informatické praxe vytvořil zabezpečení e- mailových zpráv. Firma využívala internetové bankovnictví firmy ČSOB, takže právě proto musel být kladen důraz na bezpečnost této stránky.

8.3 Internetové bankovnictví

Druhou nejvíce ohroženou oblastí v podnikatelské sféře jsou internetové platby. Vyskytují se zde ale značná rizika. Napadení takového systému se může stát různými způsoby. Nejčastější způsob je podlehnutí phishingovému útoku, kdy nepozorností otevřeme e-mail, který obsahuje falešnou adresu a po zadání přístupových údajů je útočník získá a uživateli se nepodaří do internetového bankovnictví přihlásit. Pokud si uživatel tuto chybu uvědomí ihned po útoku, musí bezprostředně kontaktovat technickou podporu dané banky a požádat o okamžité zamezení přístupu a změnu přihlašovacích údajů.

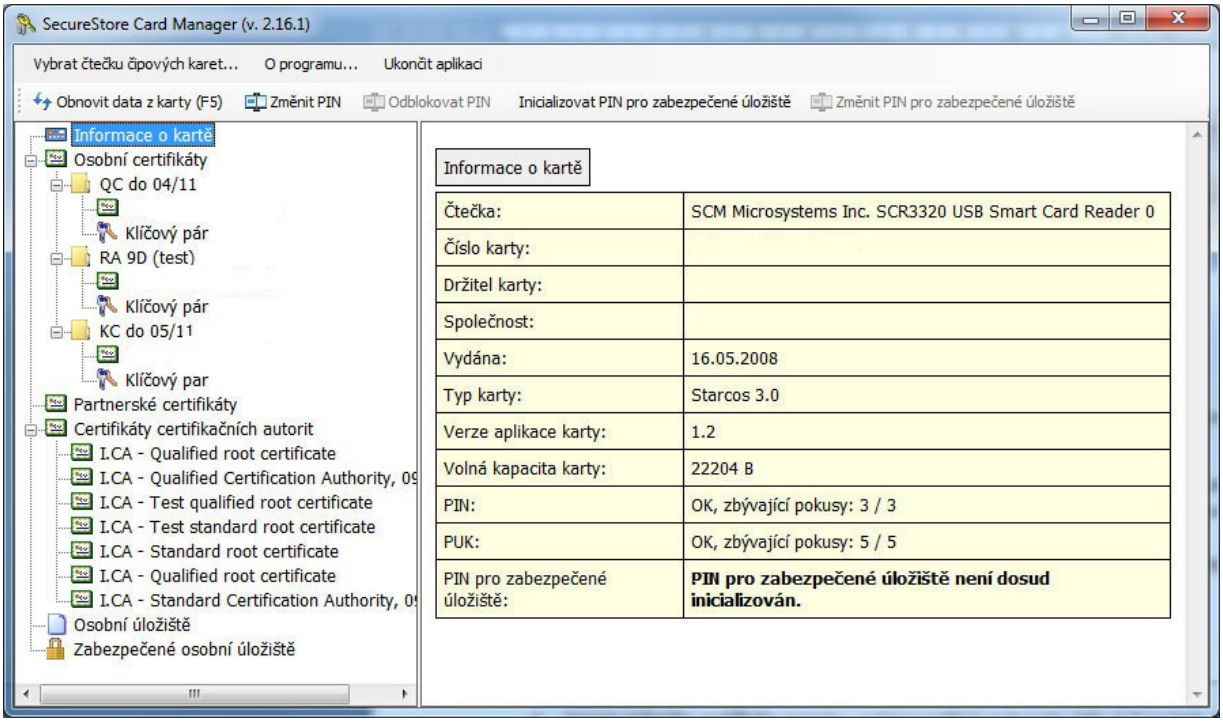
Ve firmě, kde jsem vykonával praxi, bylo dané riziko eliminováno použitím zabezpečeného přístupu pomocí systému SecureStore. Systém přihlášení neprobíhá pomocí přihlašovacího jména a hesla, ale namísto toho je použit osobní certifikát. Tento certifikát obsahuje klíč daného uživatele, zašifrovaný pomocí 1 024 bitového kódování. Osobní certifikát je uložený na čipové kartě. Uživatel se poté přihlašuje pomocí čipové karty a PIN kódu. Tato čipová karta obsahuje digitální podpis jedné osoby a nedá se tedy zaměnit. PIN je chráněn proti zneužití způsobem tzv. „třikrát a dost“. Stejná ochrana je využita i u telefonních sim karet. Pokud uživatel zadá PIN třikrát špatně, zablokuje se. Odblokování je možné pouze pomocí čísla PUK kódu prostřednictvím čipové karty. Po zadání pětkrát špatného PUK(u) se přístup na čipovou kartu zablokuje úplně.

Další způsob zabezpeční se týkal odesílání finančních prostředků pomocí internetového bankovnictví. Firma měla dva jednatele a každý měl vlastní osobní certifikát. Samotný jednatel měl možnost poslat peníze, ale byl limitován částkou 20.000,- Kč. Pokud by se

tedy přes všechna bezpečnostní opatření povedlo útočníkovi odcizit čipovou kartu včetně přihlašovacího PIN kódu, nemohl by způsobit tak velikou finanční ztrátu. Pokud byla převáděna vyšší částka, museli oba jednatelé převod podepsat svým vlastním certifikátem.

Mým úkolem v této záležitosti byla správa čipových karet. Všechny procedury s tím spojené, včetně obnovení osobních certifikátů. Při obnově osobního certifikátu byla provedena změna PIN, aby se zamezilo zneužití. Důležité bylo udržovat počítače, které byly pro tento způsob přihlašovaní určené, bezpečné. Pravidelně aktualizovaný operační systém je základem úspěšné obrany. Správně vybraný antivirový program, který byl pravidelně aktualizovaný, je obzvlášť důležitý. Bylo také nutné vytvořit filtry na přijímané e-mailové zprávy, aby se zamezilo napadení trojským koněm či zobrazení phishingových zpráv.

V současné době bych doporučoval tento způsob přihlašování spojit s využitím USB flash disků. PIN kód je uložen na fyzickém disku a heslo pro přístup na tento disk zná pouze majitel.



Obr. 4: SecureStore – osobní certifikát

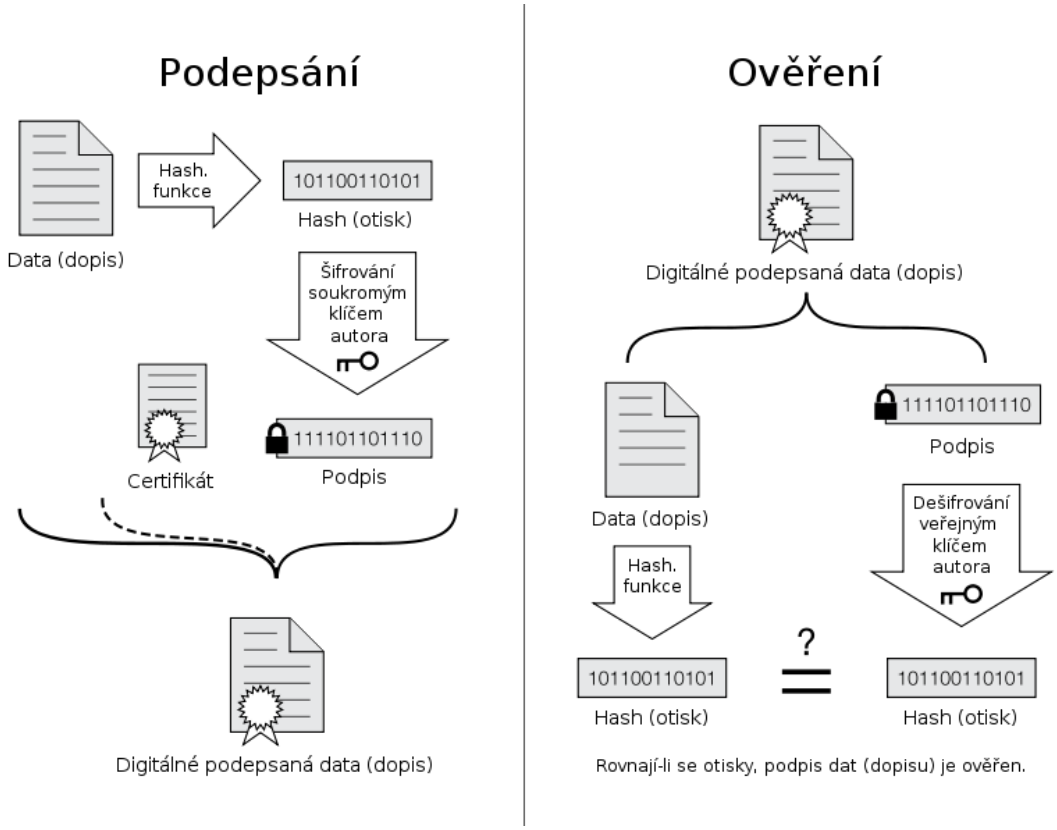
8.4 Elektronický podpis

Elektronický nebo také digitální podpis se stal nedílnou součástí podnikatelského života. Využívá se hlavně jako prostředek pro komunikaci se státní správou. Elektronický podpis nahrazuje vlastnoruční podpis při elektronické komunikaci. Takový podpis je v podstatě nezfalšovatelný a umožnuje ověřit integritu[7] podepsaného dokumentu nebo e-mailové zprávy. Bezpečnost samozřejmě nemůže být stoprocentní, ale jediný způsob zfalšování by spočíval v odcizení daného podpisu z počítače. Útok by musel napadnout samotný počítač a útočník by musel mít přístup k datům v tomto počítači.

Elektronický podpis funguje na principu asymetrické kryptografie[8] (viz Obr. 5). Jedná se o dvojici klíčů - soukromý a veřejný klíč. Vzhledem ke složitosti a náročnosti šifrování není z technických důvodů zašifrována celá zpráva, ale je vytvořen pouze její otisk neboli

7 Integrita znamená celistvost, neporušenost nebo soudržnost

hash. Odesílatel tímto otiskem potvrzuje, že jsou data integritní a jejich původ je pravý. Otisk je složitá matematická funkce, která při každé změně obsahu změní i jeho otisk. Pokud by byl dokument během komunikace změněn, není problém prostřednictvím otisku tuto změnu odhalit. Tento otisk je poté zašifrován pomocí autorova soukromého klíče. Nyní je vytvořena zpráva, která obsahuje elektronický podpis. Příjemce zprávy ověří podpis výpočtem hash funkce. Poté je pomocí autorova veřejného podpisu dešifrován obsah podpisu a porovnán s vypočteným hashem. Výsledky obou vypočtených otisků musí být stejné, jinak je elektronický podpis neplatný. Takto elektronicky podepsaný dokument ale stále není důvěryhodný, neboť nevíme, kdo vydal daný veřejný podpis, pomocí kterého jsme zprávu rozšifrovali. Důvěryhodnost podpisu je dosažena pomocí digitálního certifikátu. Ten vydává důvěryhodná certifikační autorita, která ručí za pravost veřejného dešifrovacího klíče.



Obr. 5: Asymetrické šifrování používané u elektronických podpisů

8 Asymetrická kryptografie je metoda, při které šifrování a dešifrování probíhá pomocí dvou odlišných klíčů.

Elektronický podpis se začal používat pro ulehčení komunikace se státní správou. Není tedy nutné každý měsíc navštěvovat státní instituce, aby byly požadované dokumenty doručeny. Ve většině případů byl využit pro komunikaci s ČSSZ. Pro tyto účely byl během mé praxe využíván program PVS Komunikátor sloužící k zasílání elektronických podání na ČSSZ. Program zasílaný dokument komprimuje, pomocí klíče jej podepíše, zašifruje a odešle na *Veřejné rozhraní elektronických podání*. Instituce dokument zpracuje a odešle odesílateli hlášení o výsledku celé akce. Data, která přicházejí do tohoto programu, jsou vygenerována mzdovým programem. Program se jmenuje *Stereo* od firmy *Ježek software s.r.o.*

Obr. 6: Mzdový program Stereo

Jak je možné vidět na Obr. 6, jsou zde důležité informace o zaměstnanci a údaje, které jsou odesílány na ČSSZ. Tyto informace bylo nutné řádně zabezpečit před jejich zneužitím. Zneužití osobních informací zaměstnanců by rozhodně nepřidalo dobrému jménu firmy. Na druhou stranu, včasné nedodání správně vyplněných informací by mohlo zapříčinit finanční sankce. Opět bylo nutné zabezpečit počítač, na kterém byly tyto programy používány. Jako základ musí být pravidelně aktualizovaný operační systém a funkční

antivirový program. Velmi důležité je v tomto případě zamezit neautorizovanému přístupu. Pouze zaměstnanec se správným heslem měl přístup k tomuto počítači a pouze tento zaměstnanec měl možnost pracovat s těmito daty. Pokud by tedy byl zjištěn únik dat, veškerá odpovědnost by byla na tomto zaměstnanci. A právě zde se naskytuje největší možnost selhání, protože se jedná o lidský faktor.[2]

8.5 Datové schránky

Datová schránka se dá popsat jako elektronické úložiště, které je určeno k doručování elektronických dokumentů mezi orgány veřejné moci a fyzickými nebo právnickými osobami. Pro většinu podnikajicích subjektů je povinná od konce roku 2009. Komunikace probíhá pomocí datových zpráv. Datové zprávy nahrazují doručování důležitých dokumentů v listinné podobě. Datová schránka má své velké výhody, ale existují zde i značná rizika. Mezi hlavní výhody patří závaznost a garantovanost. Pokud je datová zpráva odeslána, je vždy doručena druhé osobě. Ale pouze za předpokladu, že je zadána správná adresa, datová schránka je funkční nebo existuje. Největší výhodou je právní skutečnost, o kterou se datová zpráva opírá. Jakmile se do 10 dnů adresát do datové schránky nepřihlásí, je zpráva automaticky považována za doručenou. Nedá se tedy úspěšně vyhýbat převzetí jako při klasické doporučené zásilce.

Velkou bezpečnostní hrozbou je způsob přihlašování do datových schránek. Přihlašování probíhá přes webového rozhraní za pomoci přihlašovacího jména a hesla. Zde se právě naskýtá největší bezpečnostní riziko. Datové schránky je ideální kontrolovat v pravidelných intervalech, takže většina uživatelů si podle toho zvolí své heslo. Pokud si uživatel zvolí jednoduché heslo, nebude složité ho odhalit. Na druhou stranu, jakmile bude heslo příliš složité a uživatel bude schránku přesto navštěvovat, nejspíš ho bude mít zaznamenané na dobře přístupném místě a hrozí, že si ho někdo všimne.

Přihlašování pomocí uživatelského jména a hesla bylo během mé praxe nahrazeno použitím osobního certifikátu. Toto řešení zaručovalo, že do datové schránky se podívá jen oprávněná osoba a heslo nebude napsáno na papíře vedle počítače.

9 OCHRANA PROTI ÚTOKŮM

Tato část je věnována prevenci proti sociotechnickému útoku. Při dnešním způsobu života využíváme komunikační sítě každým okamžikem, aniž bychom to vnímali. Je tedy nutné si uvědomit, jaké hrozby na nás na každém kroku číhají a být na ně připraveni. Každá chyba nás nebo zaměstnavatele může stát ztrátu mnoha prostředků, jako například finanční ztráta, ale i čas, který jsme pracovali na novém projektu.

9.1 Znalost

O sociotechnických útocích se začalo mluvit až v posledních několika letech. Vzhledem ke značnému rozšíření tohoto fenoménu poslední doby je potřeba chápat jeho vážnost. Jedním z hlavních způsobů ochrany je uvědomění si problému samotného. Ve chvíli, kdy se s tímto útokem setkáme, ale nezpozorujeme, že se jedná právě o útok sociotechnika, zaděláváme si na velký problém. Je potřeba si uvědomit skutečnost, že těchto útoků bude přibývat a musíme na ně být připraveni. Musíme vědět, že současný internet nemusí obsahovat pouze užitečné informace, ale může obsahovat velké množství nedůvěryhodných zdrojů.

Neméně důležitým pojmem je počítačová gramotnost. Obecně se dá říci, že je to soubor všech dovedností, schopností a znalostí na ovládání počítače v běžném životě. Do toho samozřejmě již dnes patří využití internetu a zároveň by měla patřit i schopnost správného jednání uživatele na internetu. Podle toho se také uživatel musí chovat, neboť ve skutečném životě je většina z nás velice opatrná a tento stav bychom měli přenést i pro práci s počítačem a internetem. Současně by to mělo také znamenat, že každý uživatel na internetu vystupuje jako samostatný jedinec a měl by odpovídat za svoje činy. Nikdo by také neměl zapomínat, že internet je místem, kde se setkává s dalšími jedinci, kteří nemusí

být těmi, za koho se vydávají. Počítačová gramotnost by měla úměrně stoupat s rostoucím počtem uživatelů. Realita je však jiná a je tedy nutné se chránit, přizpůsobit a nenechat se oklamat možnými útočníky.

Jako příklad je možné použít přihlašovaní do internetového bankovnictví nebo jiných důležitých stránek. Každý uživatel by měl vědet, že přihlašování probíhá prostřednictvím zabezpečeného protokolu https a nikoliv pomocí obyčejného protokolu http.

9.2 Školení

Nejdůležitějším způsobem prevence je školení zaměstnanců. Prvním krokem musí být školení nově přijatých zaměstnanců. Nově přijatý zaměstnanec nemusí mít znalost dané problematiky a je tedy pro sociotechnika nejsnažším cílem. Školení by mělo probíhat okamžitě po nástupu do zaměstnání a v předstihu před dosazením na danou pozici.

Další krok by se měl věnovat pravidelnému proškolování veškerého personálu, včetně zaměstnanců na nejvyšších pozicích. Takové školení by mělo probíhat alespoň dvakrát ročně, aby se předešlo případným problémům. Častá frekvence školení dokáže vrýt do pamětí důležité informace. Každá informace, která není často opakována, je většinou brzy zapomenuta.

Takové školení by mělo zahrnovat následující údaje :

- ISO normy vztahující se k dané problematice;
- bezpečnostní opatření dané firmy;
- popis fyzické bezpečnosti a ochrany prostředí;
- způsob přenosu informací, dat a komunikace;

- praktické ukázky včetně nejnovějších útoků.

Praktickým příkladem může být např. test zaměstnanců, který jsem uvedl v podkapitole s názvem *Test zabezpečení* (viz výše podkapitola 7.4 na straně 30). Každé školení by mělo být zakončeno výstupním testem, aby došlo k ověření dosažených znalostí.

9.3 Kontrola

Kontrola je velmi důležitá pro ověření celistvosti zabezpečení. Kontrolu je potřeba zaměřit na celý systém, jednotlivé zaměstnance, vypracovaný plán bezpečnosti a ověřování úrovně zabezpečení. Příchod nových technologií způsobuje skoro každodenní inovace, které je potřeba sledovat a přizpůsobit se jim v systému.

Systém by měl být zabezpečený pomocí správných aplikací a vhodném aplikování zvolených filtrů. Integrita systému by měla být pravidelně kontrolována z různých úhlů. Způsoby kontroly systému by měly být prověřovány hlavně proti útoku vně a uvnitř firmy. Okolí firmy může obsahovat různé druhy nebezpečí hlavně při konkurenčních bojích. Ochrana proti útoku mimo firmu může také obsahovat náhodně vedené hromadné útoky. Takový útok je z velké většiny veden pod údajnou hlavičkou finančního institutu. Zabezpečení sytému proti útoku zevnitř vyzaduje hlavně důkladnou kontrolu jednotlivých zaměstnanců.

Každý zaměstnanec ze systému plní svoji roli a tyto role je potřeba kontrolovat. Pokud jeden zaměstnanec útočníka označí jako důvěryhodného, ostatní věří úsudku daného zaměstnance a dále útočníka neprověřují. Ten má poté možnost získat důležitá data. Jakmile by nebyla kontrola prováděna dostatečně kvalitně, mohlo by dojít ke ztrátě důležitých dat a informací. Bude-li však kontrola správně a často prováděna, každý zaměstnanec bude mít znalosti, které mohou předejít chybnému rozhodnutí. Kontrola

zaměstnanců musí obsahovat i kontrolu přístupů. Pravidelná změna přístupových údajů a složitost hesel může rozhodnout o úspěšnosti útoku.

Vypracování bezpečnostního plánu, který bude pravidelně kontrolován, je ideální volbou, jak dosáhnout kvalitního zabezpečení. Změna hesla je doporučována alespoň jednou za tři měsíce. Na druhou stranu málokdo toto doporučení dodržuje a ke stávajícímu heslu přidá například jednu číslici, což se považuje za chybu a nezodpovědnost, která může zapříčinit obrovské problémy.

9.4 Pravomoce

Sociotechnický útok skýtá řadu kroků, které postupně směřují od získání základních informací až k získání chtěné informace. Proto je důležité správně rozdělit pravomoce mezi různé úrovně zaměstnanců. Ve chvíli, kdy útočník dokáže přelstít zaměstnance na nízké úrovni a zaměstnanec na vyšší úrovni tento útok odhalí, problém je z velké části vyřešen. Právě proto je důležité pravomoce rozdělovat přesně podle postavení zaměstnance. Nikdy se nesmí stát, aby jeden zaměstnanec měl přístup ke všem datům.

Rozdělení pravomocí je ideální při přístupu k internetovému bankovnictví. Pokud se pravomoce přerozdělí mezi dva lidi, je prakticky nemožné, aby útočník získal plný přístup k možnému převodu peněz.

Velice důležitou roli představují v tomto případě zaměstnanci IT oddělení. Tito zaměstnanci mají kontrolu nad veškerými uživatelskými účty a je potřeba, aby byli stoprocentně bezchybní. Ačkoliv si to málo zaměstnavatelů uvědomuje, tato role je jednou z klíčových rolí, co se týče celkového zabezpečení. Všechny technologické novinky a bezpečnostní hrozby musí vyřešit právě tito zaměstnanci. Tedy veškerá zodpovědnost za

případný únik informací leží právě na nich. Pokud je firma malá, doporučil bych mít alespoň dva IT pracovníky, aby se mohla zodpovědnost rozdělit mezi ně. Poté zde nemusí být tak velký tlak na jediného zaměstnance, který odpovídá za veškerou bezpečnost systému.

9.5 Moderní technologie

Jak jsem již dříve zmínil, vývoj moderních technologií je velice rychlý a je potřeba sledovat nejnovější trendy. Na prvním místě je vývoj bezpečnostních systémů. Tyto inovace se týkají především způsobu zabezpečení, technického vývoje a programů zajišťujících ochranu systému.

Způsob zabezpečení se vždy odvijí od technologické úrovně. Dřívě se považoval antivirový program za ideální způsob ochrany systému. Dnes je zcela nezbytné sledování kvality jednotlivých antivirových programů a doplňovat je o důležité prvky bezpečnosti. Může jím být správně nastavený firewall nebo dobře zacílený antispyware program odhalující trojské koně. Další novinkou, která byla dříve velice opomíjena, je zálohování důležitých souborů.

Budoucnost je směr, na který je třeba se důkladně zaměřit. Vývoj bezpečnostních systémů dosáhl prakticky dokonalosti a úroveň zabezpečení hesel pomocí 1 024-bitového kódování je pro běžné uživatele nepřekonatelná. Je důležité se především zaměřit na jednotlivce, kteří se pohybují uvnitř bezpečnostního systému a užívají ho. Lidský faktor se stal nejslabším článkem bezpečnosti, a proto je potřeba se na něj zaměřit.

9.6 Zabezpečení

Poslední z hlavních způsobů ochrany je fyzická ochrana. Přístup na pracoviště smí být povolen pouze legitimním osobám. Čím větší nároky na fyzickou ochranu dat a informací se vynaloží, tím menší je pravděpodobnost jejich ztráty. Jednou z možností ochrany je kontrola přístupů na pracoviště firmy. Takováto kontrola může probíhat za pomoci fyzické ochrany. Tedy pracovníka, který bude kontrolovat přístupy do dané firmy. V případě, že je tato firma menší, postačí zavedení čipových karet pro přístup do kanceláří. Tyto čipové karty jsou nutností u větších firem. Druhotnou výhodou je logování přístupů. Díky němu je možné kontrolovat, zda všichni zaměstnanci dodržují řádnou pracovní dobu.

V okamžiku, kdy je zabezpečen fyzický přístup na pracoviště, je nezbytné zabezpečit i data v počítačích. Jako základní opatření by měly být použity následující nástroje:

- Kvalitní antivirový software
- Spolehlivý antispyware[9] software
- Správně nastavená brána firewall[10]

Výše uvedené nástroje jsou nezbytné pro každodenní fungování. Tyto programy ochrání proti programům, které mohou napadnout počítač nebo i celou počítačovou síť. Další nástroje zamezí chybě na straně uživatele. Jedná se většinou o otevírání příloh v e- mailových zprávách, nebo otevření odkazů z e-mailových zpráv.

- Zamezení přístupu na stránky – většina škodlivých programů pochází ze zahraničí, velmi často se využívají servery z asijského kontinentu

9 Antispyware je program, který brání odesílání dat z počítače bez vědomí uživatele.

10 Firewall je software nebo hardware. Kontroluje informace přicházející z internetu nebo sítě. Dle uživatelského nastvení je zablokuje nebo jim umožní projít do počítače.

- Blokování portů – povolení přístupů pouze na webové stránky a porty pro poštovního klienta

Poslední z hlavních nástrojů je zamezení odcizení dat. Tato situace nastává při neuváženém nahrávání důležitých dat a následné jejich ztráty.

- Nemožnost nahrávat data z počítače na fyzické přenosné disky – USB disky, CD disky
- Blokace ftp portů
- Blokace stránek, kde je možné uložit data

Tyto nástroje jsou většinou použity pouze při nebezpečí průmyslové špionáže.

9.7 Srovnání zabezpečení

Různé firmy v rozdílných odvětvích upřednostňují jiné způsoby zabezpečení. Je tedy potřebné se zaměřit na porovnání způsobů, které mohou být někde úspěšné a naopak jinde absolutně neúspěšné a zbytečné.

Povědomí o sociotechnice je všeobecně potřebné. Bez tohoto základu budou ostatní způsoby zabezpečení kontraproduktivní. Školení je hlavní způsob, jak získat povědomí o celém problému. Díky této nabyté znalosti si zaměstnanci uvědomí vážnost sociotechniky. Také si pomocí praktických příkladů vytvoří představu, jakými nejčastejšími způsoby mohou být ohrožení.

Finanční sektor je místo, kde je nejvíce potřebné rozdělení pravomocí. Naopak rozdělení pravomocí může být při kontrole zaměstnanců kontraproduktivní. Zaměstnanci mohou kontrolovat stejnou část a jiná potřebná oblast je ponechána bez kontroly. Zabezpečení počítače a počítačových sítí je přímo úměrné dostupnosti a vývoji moderních technologií.

Čím více budou moderních technologie součástí našich životů, tím více bude potřeba se zaměřit na zabezpečení.

Důležitost základních způsobů zabezpečení bych srovnal následovně.

1. Povědomí
2. Školení
3. Zabezpečení
4. Kontrola
5. Moderní technologie
6. Rozdělení pravomocí

(pozn. důležitost klesá se rostoucím číslem)

Při sestavování plánu pro řádný způsob zabezpečení je tedy žádoucí, aby se postupovalo ve stejném pořadí. Jedná se o detailní rozpracování od nejzákladnější části až po komplexní bezpečnostní systém.

ZÁVĚR

Hlavním cílem bakalářské práce bylo analyzovat komunikační prostředí dané firmy, ve které jsem byl na praxi, a zjistit, zda je obeznámena s možnými riziky sociotechnických útoků.

V teoretické části je proveden rozbor základních způsobů a metod, jakým jsou útoky vedeny. Je zde uveden životopis jednoho ze zakladatelů sociotechniky, který se po pobytu ve vězení stal jedním z uznávaných expertů na bezpečnost. Uvedl jsem praktické ukázky útoků, které byly přinosem pro praktickou část, neboť diky nim bylo možné se na tyto útoky připravit. Praktická část této práce je zaměřena na zjištění stávajících způsobů zabezpečení v dané firmě, jejich analýzu a vylepšení jich. Během mé informatické praxe jsem získal mnoho nových zkušeností, které byli později využity pro vylepšení stávájícího způsobu ochrany. Původní ochrana určitě nebyla na špatné úrovni, ale zaměstnanci nebyli pravidelně proškolováni o dané problematice. Během mé praxe se školení prováděla častěji a důkladněji. Zaměstnanci byli po školení kontrolováni výstupními testy. Kvůli rychlému vývojí informačních technologií bylo potřeba způsoby zabezpečení podrobněji rozpracovat a vytvořit ucelenější způsob ochrany. Detailnější způsob ochrany byl aplikován během praxe v dané firmě.

Závěrečná část obsahuje způsoby prevence proti sociotechnickým útokům. Tyto způsoby jsem využil během mé informatické praxe a díky rozšíření povědomí o daném tématu bylo riziko úspěšného útoku sníženo na minimální možnou hranici.

Na závěr konstatuji, že ochrana proti sociotechnickým útokům se musí neustále obnovovat a inovovat, neboť se technika rychle vyvíjí a je tedy nutné s tímto vývojem postupovat vpřed.

ZDROJE

[1] JIROVSKÝ, V. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. 1 vyd. Praha : Grada Publishing, a.s., 2007. ISBN 978-80-247-1561-2.

[2] MLÝNEK, J. Zabezpečení obchodních informací. 1. vyd. : Computer Press, 2007. ISBN 80-251-1511-9

[3] MITNICK, K., et al. Umění klamu : Nejslavnější hacker na světě. Přel. L. Vlašta. 1. vyd.: Helion, 2003. ISBN 83-7361-210-6

[4] HARPER, A., et al. Gray Hat Hacking : The Ethical Hacker's Handbook. McGraw-Hill Osborne Media. 2004. ISBN 978-0072257090.

[5] *Phishing*, HOAX [online] [cit. 2013-01-20] . Dostupné z: http://www.hoax.cz/phishing/

[6] Zorz, Z., *$2.1 milion stolen with clever social engineering*, HELP NET SECURITY [online], [cit. 2013-02-27]. Dostupné z : http://www.net-security.org/secworld.php?id=12516

[7] Layton, T., *Social engineering a real world example*, TIM LAYTON ASSOCIATES [online], [cit. 2013-03-08]. Dostupné z : http://www.timlaytonassociates.com/2012/04/15/social-engineering-a-real-world-example/

[8] *Sociotechnika (Sociální inženýrství)*, MOZEKTEVIDI [online], [cit. 2013-02-12]. Dostupné z : http://mozektevidi.cz/sociotechnika-socialni-inzenyrstvi/

[9] *Kyberšikana, kybergrooming, stalking, sociotechnika*, SME [online], [cit. 2013-01-20]. Dostupné z : http://nanicmama.sme.sk/node/37551

[10] *Kevin Mitnick*, OSOBNOSTI [online], [cit. 2013-03-26].

Dostupné z : http://zivotopis.osobnosti.cz/kevin--mitnick.php

[11] ROUSE, M., *Advanced persistent threat*, TECHTARGET [online], [cit. 2013-03-20]. Dostupné z : http://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT

ZDROJE OBRÁZKŮ

Obr. 1: Internetové stránky Pooh.

Dostupný online z: http://www.pooh.cz/pooh/a.asp?a=2014744

Obr. 2: Internetové stránky Maxiorel. Dostupný online z:
http://www.maxiorel.cz/ceska-sporitelna-phishing-kdy-uz-skonci

Obr. 3: Internetové stránky Komtur s.r.o. Dostupný online z:
http://www.komtur.cz/struktura-spolecnosti.html

Obr. 4: Internetové stránky I.C.A. Dostupný online z:

http://www.ica.cz/Secure-Store.aspx

Obr. 5: Internetové stránky Wikipedia. Dostupný online z:
http://cs.wikipedia.org/wiki/Elektronick%C3%BD_podpis

Obr. 6: Internetové stránky Jezek SW. Dostupný online z:
http://www.jezeksw.cz/stereo/popis-programu/otazky/5/

SEZNAM PŘÍLOH

Příloha I: Příklady sociotechnických útoků

Eric Mantini

Eric zavolal na informace a požádal o telefonní číslo na státní dopravní policii. Dostal číslo 503-555-5000, což je číslo pro veřejnost. Poté 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. „A kdo jste?" zeptal se policista od dálnopisu. „Tady je Allan. Volal jsem na 503-555-5753," řekl. Do místnosti s dálnopisem nevolá nikdo zvenku. Očividně to byla osoba zevnitř. Alespoň si to policista myslel. „Číslo je 503-555-6127," řekl policista. Eric získal speciální číslo pro vyšetřovatele na kontakt s dopravní policií. Nyní zbývalo už jen získat přístup k telekomunikační ústředně. Zatelefonoval na státní telekomunikační úřad a představil se jako někdo, kdo volá z firmy Nortel, která vyrábí DMS-100, jeden z nejrozšířenějších modelů 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. „Potřebuji ale přístupové číslo na ústřednu, aby mohli vykonat aktualizaci přímo od sebe“ řekl Eric. Znělo to docela věrohodně. Technik sdělil Ericovi číslo.

Teď telefonovat přímo na jednu ze státních telefonních ústředen. Ústředny tohoto typu jsou chráněné heslem. Každý dobrý sociotechnik zabývající se také phreakingem[] ví, že ústředny firmy Nortel mají pro aktualizaci softwaru defaultní uživatelské jméno NTAS. Jakmile získal číslo, pokusil se Eric několikrát připojit a zkoušel různá typická hesla. Heslo stejné jako uživatelské jméno — NT AS — nefungovalo, a další obvyklá hesla „helper" či „patch".

Zkusil ještě „update" (aktualizace) a ... byl tam. Používání jednoduchých hesel je prakticky totožné, jako kdyby zde žádné heslo nebylo. 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. 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 po dokončení práce zahodí. Následující telefon už nezazvoní v kanceláři dopravní policie — bude to Ericův mobil. Krátce před osmou hodinou ráno zazvonil mobil. To byla ta nejrafinovanější část akce. Eric bude hovořit s policistou, který by ho mohl potencionálně zatknout. Takových hovorů však bude mnohem víc. Dobrý sociotechnik se ani trochu neobává rozhovoru s policií. Rozhovory probíhaly následujícím způsobem.

„Dopravní policie, co pro vás mohu udělat?" řekl Eric.

„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.

„Hned si vyhledám seznam," odpovídal Eric. „Aha, pane Cole, z jaké jste agentury?"

„Jefferson County." Potom Eric kladl nejdůležitější otázky:

„Uveďte, 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 sýšel psaní na klávesnici počítače. O chviličku později říkal něco jako:

„Sakra! Už zas mi to spadlo. Moc se omlouvám, ale celý týden tu 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 několikahodínovém přijímání hovorů a po získání několika desítek kódů institucí se Eric znovu připojil na ústřednu a deaktivoval směrování hovorů.

V tomto příběhu musel Eric spojit své sociotechnické znalosti s technickými znalostmi daného prostředí. Chytrý sociotechnik dokáže využít ale i těch nejmenších detailů.
Telefonní číslo dopravní policie je jako veřejné číslo všem dostupné. Rozebral si telefonní číslo 503-555-5000, které je pro veřejnost. Předvolba pro policii bude mít stejný prefix (503) , 555 je také stejná. Jediný rozdíl byl v posledním čtyřčíslí a tak nebyl problém chtěné číslo získat. Ani při dalším rozhovoru mu nedělalo problémy zjistit telefonní číslo, které potřeboval. Zaměstnanec komunikačního úřadu se neobtěžoval s ověřováním identity. Předal tajné číslo člověku, který si vymyslel jednoduchou historku. Bez správné identifikace a ověření by se takové informace neměly nikdy předávat. Pro přístup do ústředny mu už jen zbývalo získat heslo. Toto heslo samožrejmě nebylo nikterak složité a po pár pokusech byl připojen v telefonní ústředně.[3]

Craiga Cogburnea

Craig Cogburn dostal zakázku, kde mohl konečně využít svůj potenciál. Průmyslovou špionáží si mohl přijít k velkému množství peněz a tak nabídku neodmítl. Jednalo se o konkureční válku a jeho úkolem bylo získat projekty a specifikace nového produktu. Jméno firmy bylo GeminiMed a měla šest poboček v různých městech. Zde se mu naskytla možnost, že lidé z různých poboček se nebudou znát a nebudou se ostýchat si pomoct.

Základem informací byl ústřižek textu z časopisu, který obsahoval název projektu STH- 100. Prvním krokem bylo zjištění jmen lidí, kteří na projektu spolupracují nebo mají k datům alespoň přístup. Zatelefonoval tedy na telefonní ústřednu firmy. *„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."* řekl Craig. *„Máme tu Scotta Archera a Sama Davidsona,"* odpověděla recepční. Požádal o přepojení na Scotta Archera. *„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 jméno šéfa projektu Jerryho Mendela včetně jeho telefonního čísla. Mendel byl na dovolené a zaskakovala za něj sekretářka Michelle na čísle 9137. *„Tady Bili 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 souhlasila. *„A jaké používáte servery?"* zeptal se Craig. *„RM22. A část týmu je také na GM16."*. U další otázky si nebyl příliš jistý, ale proč by to nezkusil, když je Michelle tak ochotná. *„Jerry říkal, že byste mi mohla dát seznam e-mailových adres členů výzkumného týmu,"* řekl. *„Samozřejmě. Rozesílací seznam je ale moc dlouhý na to, abych ho tady četla do telefonu. Mohla bych vám to poslat e-mailem?"* Vědel, že jakmile nebude e-mailová adresa končit „geminimed.com“, vzbudí podežření. *„A mohla byste mi to nafaxovat?"* zeptal se. Neviděla v tom žádný problém. *„Náš fax je nyní v opravě. Musím zjistit číslo druhého. Za chvilku znovu zavolám,"* a položil sluchátko. Zavolal tedy na recepci Geminimed a požádal, zda by mohl přijmout fax na jejich přístroji. Nechal Michelle poslat fax na číslo na recepci. Zavolal znovu do recepce a zeptal se, zda jeho fax dorazil. *„Ano dorazil." „Mám prosbu,"* řekl. *„Musím to poslat našemu konzultantovi. Mohla bys to poslat místo mně?"* Aby se vyhnul osobnímu setkání a možnému riziku prozrazení, nechal si ho poslat do společnosti, kde může fax přijmout a poslat kdokoliv. Zde si fax vyzvedl a získal e- mailové adresy všech zaměstnanců pracujících na projektu. Pro přístup do systému mimo areál firmy mu chybělo telefonní číslo používáné pro vzdálený přístup. Využil tedy ochotu pracovníka informatického oddělení. „*Jsem doma, právě jsem si přinesl nový notebook a potřeboval bych ho nastavit tak, abych se mohl připojovat zvenku.*" řekl Craig. Krok po kroku se nechal vést a informatik mu bez jakýchkoliv problémů číslo sdělil, jako by to byla bežná informace. Připojení fungovalo a tak poděkoval za pomoc a rozhovor ukončil. Po chvíli hledání narazil na počítač, kde byl založen účet „guest“ konfigurovaný tak, že pro přihlášení není nutné heslo. Jednalo se o starší verzi operačního systému UNIX, kde jsou hesla uložena v zašifrovaném tvaru tzn. hash. Stáhl si tento soubor a použil na něj slovníkový útok[11]. Objevil uživatele výzkumného týmu Steve Cramera, který měl konto s heslem „Janice“. Poslední útok naplánoval na víkend, aby si byl jistý, že uživatel nebude v práci.

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

11 Slovníkový útok

„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 Steve. „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 být první v pořadí. 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 teď!" naléhal Steve a přemýšlel, komu zatelefonuje, jestli se mu nepodaří toho chlapa přivést k rozumu.

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

„RM22 i GM16. Oba používám."

„Já bych potřeboval uživatelské jméno a heslo."

„Mohl byste mi ještě jednou říci vaše jméno? A pod koho patříte?" „Ramon Perez. Heleďte, když jste byl přijat do práce, dostal jste vyplnit formulář, abychom vám založili konto a musel jste tam napsat nějaké 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."

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."

Sumarizací celého příběhu vidíme hned několik opakování stejné chyby. Michelle ani informatik nepožadovali žádnou autorizaci, že osoba je ta, za kterou se skutečně vydává. Vzhledem k uveřitelnosti žádosti se nezabývali možností, že by mohli předávát informace do špatných rukou. Recepční by měla být proškolená a vědět, jak rozeznávat důvěrná data. Administrátoři serverů by měli vybavit všechny počítače řádnou ochranou a vyvarovat se ponechání uživatelských účtů, které nejsou zabezpečeny heslem. V neposlední řadě pracovník Steve, podlehajíc panice sdělil své heslo po telefonu.[3]

Bankovní podvod

Abych neuváděl příklady jen z minulosti, popíšu jeden současný příběh. Jedná se o elektronické vyloupení banky. Informace byla zveřejněna v roce 2012, takže je vidět, že sociotechnika je úspešná i v současnosti. Základem byl podepsaný kontrakt mezi Catholic Healthcare West a Merced County z Kalifornie. Šlo o výstavbu zdravotního střediska v San Joaquin Valley. Prostředky na tuto výstavbu byli uloženy na escrow účtu, kde bylo pro tyto záležitosti uloženo 7,5 milionu dolarů. Ve stejné chvíli se rozhodli změnit banku, ke které potřebovaly schválení od dozorčí rady. Tato rada změnu schválila, naneštěstí byla umísťena kopie tohoto potvrzení na oficiální stránky Merced County. Obsahovalo veškeré podrobnosti, včetně podpisu CFO a ředitele veřejného zdravotnictví firmy Merced County.

Získal tedy veškeré informace, které jsou potřebné pro jakýkoliv kontrakt. Číslo účtu, jméno banky, kde je účet veden a podpis CFO. Svůj plán začal naplňovat v prosinci 2011. Poslal fax s požadavkem na převod 445.000 dolarů z escrow účtu na jiný v bance v New

Yorku. Podepsán byl podle podpisového vzoru, ale číslo účtu bylo neexistující a tak transakce neproběhla. Manažer escrow účtu začal zjišťovat, proč nebyla transakce provedena. Poslal fax na číslo uvedené na faxu a zažádal o podrobnosti. Číslo bylo však vedeno na podvodníka, který posléze zavolal a sdělil, že zadaná operace byla chybná a aby ji ignoroval. Další útok naplánoval o týden později. Požadavek na stejnou částku, jen změnil jméno banky a číslo účtu na banku v Hong Kongu. Opět nebyl převod úspešný, neboť účet opět neexistoval. Následující týden už byl ale úspěšný. Požádal o převod 989.000 dolarů na skutečný účet vedený v Hong Kongu. Transakce byla uskutečněna a na účet bylo připsáno skoro milion dolarů. Vidina úspěšného útoku ho neodradila a tak pokračoval dál. Čtvrtý útok byl neúspěšný. Vyšší částka vyžadovala zvýšená bezpečnostní opatření, ale útočník nevědel, která. Další úspěšný útok přišel zanedlouho. Požádál o převod 1,1 milionu dolarů a transakce byla schválena. Získal již tedy 2,1 milionu dolarů a to jen za pomoci posílání faxů. Šestý a poslední útok byl vystaven na částku 2,2 milionu dolarů. Manažer escrow účtu si nebyl jistý legitimností tohoto požadavku. Zavolal na pobočku Catholic Healthcare, kde však o tomto ani o předchozích převodech nebyl žádný záznam z jejich strany.

Manažer jejich escrow účtu rozhodně pochybil při kontrole, zda je zadaný požadavek autorizovaný. Podcenil i dva falešné požadavky na převod tak velké částky na neexistující účty. Jakmile by si dal práci a volal na číslo uvedené ve smlouvě, rozhodně by předešel dalším útokům a následnému zjišťování jak se mohly originální podpisové vzory dostat do cizích rukou. Při identifikaci člověka, kterému volal, a ověření, zda skutečně existuje, by jistě také objevil určité nejasnosti. Největší chybou však bylo zveřejnění podpisových vzorů na veřejně přístupných internetových stránkách. Tato chyba by se dala přirovnat k psaní PIN kódu na kreditní karty. Možná přesnější bude situace, kdy necháme svojí peneženku na lavičče při čekání na metro a odběhneme si na toaletu. Nikdo se asi nebude divit, že při návratu tu peněženka nebude. Jakkoliv se zdá, že první dva kroky byly neúspěchy pro útočníka, opak je pravdou.

První pokus byl odrazovým můstkem, zda je šance na úspěch či nikoliv. Ve chvíli, kdy neexistovalo konto v Americe, byl dotázán právě on a to byl jeho základ úspěchu. Druhým pokusem změnil banku do Hong Kongu, ale manažer tomu nevěnoval pozornost. Vzhledem k předchozímu laxnímu přístupu se nedalo očekávat, že by nastal problém. Peníze byly tedy při dalším útoku úspěšně převedeny. Další pokusy nezaručovaly úspěch, neboť již část peněz byla převedena a někdo si mohl všimnout chybějících prostředků. Nestalo se a tak přisli o další peníze. Útočník byl dobře připraven. Žádosti o převod peněz byly s určitým rozestupem, aby nevzbuzovaly podezření. Celý tento útok trval přibližně šest týdnů, ale až po posledním útoku se na něj přišlo.[6]

Test na zabezpečení

CIO jedné nejmenované firmy chtěl vyzkoušet, jak jsou odolné jeho prodejny. Tim Layton jako odborník na internetovou kriminalitu se neváhal tohoto úkolu zhostit. Vypracoval si 30-ti denní plán na získaní informací z jeho prodejen v různých místech. Kontaktoval centrální kancelář a chtěl mluvit s vedoucím administrátorem, který má na starost databáze, jmenoval se John Davis. Představil se jako zástupce Oracle[12]. Informoval o důležitosti obnovy smlouvy, neboť stávající smlouva brzy vyprší. John upozornil, že informace musí být mylná, neboť na všech svých pracovištích využívají systém Informix. Tim tuto informaci věděl. Chtěl si být jen jistý, že ho využívají na všech prodejních místech. Ne všechny ze všech 100 prodejen májí svoje IT oddělení, menší prodejny mají pouze manažery. Právě na těchto manažerech stojí odpovědnost za chod počítačového systému. Vybral si jednu z těchto menších prodejen bez IT oddělení a zavolal. Představil se jako John Davis, vedoucí administrátor z centrály. Informoval o zavirování systému, ale že by vše měli mít plně pod kontrolou a kontroluje každé pracoviště. Příznakem napadení systému virem je výrazné zpomalení chodu počítače nebo zasekávání se při velkém vytížení. Řekl, ať to zjistí a že se znovu ozve. Po pár dnech se znovu ozval a manažer pobočky přiznal, že mají skutečně tento problém a jak to spolu mohou vyřešit.

12 Firma Oracle je jeden z největších distributorů databazových systémů.

Domluvili se, že pošle interního zaměstnance na vyřešení tohoto problému, ale až v pozdních hodinách neboť je velice vytížený. V předchozích dnech byl Tim navštívit pár jiných prodejen, aby zjistil, jaký mají dress-code[13]. Všichni členové týmu nosí služební tričko. Využil logo z firemních stránek a takové tričko si nechal vyrobit. V převlečení vstoupil do prodejny a požádal o manažera pobočky. Představil se jako spolupracovník Johna Davise a že je zde na opravdu zavirovaného systému. Manažer ho bez jakéhokoliv ověření totožnosti doprovodil k počítači. Poprosil ještě manažera prodejny o papír s přístupy k serveru, který rozesílaly na všechny pobočky. Manažer o žádném takovém papíru nevěděl a tak mu předal svůj vlastní s přístupovým jménem a heslem. V tento okamžik měl plný přístup k systému. Jako upozornění na úspěšné napadení prodejny, umístil do základního adresáře skript[14]. Skript odeslal CIO e-mail o úspěšné infiltraci a že právě tato prodejna byla úspěšně zkompromitována. Stejným způsobem se dostat i do dalších prodejen, kde umístil tento skript.

Na konci 30-ti denního plánu si sjednal schůzku s CIO. Tim během setkání zavolal prvnímu z manažerů. Poprosil, že potřebuje zjistit, jestli je stále funkční jeho úprava, kterou nainstaloval před 14 dny. S manažerem prohodili pár přátelských vět a manažer ho ujistil, že vše nyní funguje, jak má. Tim ho nyní poprosil, aby si sedl k počítači a přihlásil se do systému a do příkazové řádky[15] napsal „update“. Dále ho upozornil, aby při každém zpomalení počítače provedl tento příkaz. Tim poděkoval za jeho čas a rozhovor ukončil. Tim nyní řekl CIO, aby si zkontroloval svůj e-mail. CIO přišel e-mail od manažera s textem „*you have been hacked*“. Společnými kroky se poté dali do vypracování kampaně, která by přinesla do povědomí zaměstnanců, jaká rizika může sociotechnika přinést a jakým způsobem se bránit. [7]

13 Dress code jsou pravidla pro oblékání. Většinou využito u pracovníků, kteří přicházeji do styku se zákazníky.

14 Skript je souvislý způsob přikazů vykonávající určité úkoly. Typickým přikladem může být makro, které využívá prostředí Microsoft Office.

15 Příkazový řádek znamená uživatelské rozhraní, ve kterém uživatel komunikuje pomocí přikazů s programy nebo s operačním systémem.

Příloha II : Phishingovy mail pod jménem České Spořitelny

Bezpeиn Opatшenн ode Ceskб Sporitelna Internet Bankovnн

Cesk? Sporitelna [bmkybr@yahoo.com]

This message was sent with High importance.

To: undisclosed-recipients:

ČESKÁ SPOŘITELNA

Vбћenэ Ceskб Sporitelna vyъitovat drћitel,

Vzhledem k nмkolik selhalo pшihlбsit pokusy aby vy online vyъitovat, tvoji Ceskб Sporitelna vyъitovat vlastnosti mнt bэt zakбzanэ za od ten иas od tomu oznбmenн. Na dalљн vyъitovat znalosti, aby restaurovat vбљ vyъitovat vlastnosti i vytvбшet nмjakэ online platba, musнte kontakt nбs u **http://www.csas.cz**.

Tomu poselstvн je na znalosti ъiely jenom.

Potmљit chбpat ta my neumн reagovat aby jednotlivэ zprбvy skrze tomu emailovэ oslovit. Ono nenн zajistit i mml by ne bэvat zvyklэ na kreditnн karta souvisejnсn otбzky.

Aby rekonstruovat vбљ Ceskб Sporitelna Online Bankovnн vlastnosti, potmљit vyplэvat ty schody:

1. Kontaktujte nбs ve
http://www.csas.cz/banka/appmanager/portal/pageLabel=Login
2. Pшihlбsit na do tvou online bankovnн konto i proљetшit tvou Vyъitovat Vlastnosti

Po tм co vy pшedloћenэ tvoji poselstvн, ovmшit na za reakce uvnitш 24 hodiny.

Dostupný z : http://www.pooh.cz/a.asp?a=2014601