UNIVERZITA PARDUBICE
FAKULTA EKONOMICKO-SPRÁVNÍ
ÚTAV SYSTÉMOVÉHO INŽENÝRSTVÍ A INFORMATIKY

LIDSKÝ FAKTOR V OBLASTI BEZPEČNOSTI INFORMAČNÍCH SYSTÉMŮ

BAKALÁŘSKÁ PRÁCE

AUTOR PRÁCE: Petr Sotona
VEDOUCÍ PRÁCE: Ing. Milan Tomeš

2007

UNIVERSITY OF PARDUBICE
FACULTY OF ECONOMY AND ADMINISTRATION
INSTITUE OF SYSTEM ENGINEERING AND INFORMATICS

THE ROLE OF HUMAN FACTOR IN INFORMATION SYSTEMS SECURITY

BACHELOR WORK

AUTHOR: Petr Sotona
SUPERVISOR: Ing. Milan Tomeš

2007

Univerzita Pardubice
Fakulta ekonomicko-správní
Ústav systémového inženýrství a informatiky
Akademický rok: **2006/2007**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Petr SOTONA**

Studijní program: **B6209 Systémové inženýrství a informatika**

Studijní obor: **Informatika ve veřejné správě**

Název tématu: **Lidský faktor v oblasti bezpečnosti informačních systémů**

Zásady pro vypracování:

1. Možnosti selhaní lidského faktoru
2. Obrana proti selhání lidského faktoru
3. Právní normy vztahující se k ochraně informačního systému
4. Případy zneužití systému vlivem selháni lidkého faktoru
5. Testovaní odolnosti systému proti úniku informací

Rozsah grafických prací:

Rozsah pracovní zprávy:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

[1] MITNICK, K., SIMON, W., Umění klamu, 1.vyd., Gliwice: Helion s.a., 2003, ISBN: 83-7361-210-6

[2] ALLEN, Malcom, Social Engineering: A Means To Violate A Computer System [online], SANS Institute, publikováno červen 2006 [cit. Srpen 2006]. Dostupný z WWW: <http://www.sans.org/reading_room/whitepapers/engineering/529.php>.

[3] DOLAN, Aaron, Social Engineering [online]. SANS Institute, publikováno duben 2004, [cit. Srpen 2006], Dostupný z WWW: <http:/www.sans.org/reading_room/whitepapers/engineering/1365.php>

[4] FITE, Bryan, Corporate Identity Fraud:Life Cycle Managment of Corporate Assets [online], SANS Institute, publikováno březen 2006, [cit. Srpen 2006], Dostupný z WWW: <http://www.sans.org/reading_room/whitepapers/engineering/1650.php>

Vedoucí bakalářské práce: **Ing. Milan Tomeš**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **30. října 2006**

Termín odevzdání bakalářské práce: **21. května 2007**

prof. Ing. Jan Čapek, CSc.
děkan

L.S.

doc. Ing. Pavel Petr, Ph.D.
vedoucí ústavu

V Pardubicích dne 30. ledna 2007

Prohlašuji:

Tuto práci jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně Univerzity Pardubice.

V Pardubicích dne 10. 5. 2007

Petr Sotona

Poděkování:

Rád bych poděkoval vedoucímu své práce Ing. Milanu Tomešovi za trpělivé vedení a cenné rady, které mi poskytl v průběhu zpracovávání celé práce. Také bych rád poděkoval Magistrátu města Děčín, který mi umožnil práci vypracovat po praktické stránce, především tajemníku magistrátu Ing. Jaromíru Zajíčkovi, který svolil k testování odolnosti informačního systému magistrátu, a dále pak vedoucímu odboru provozního a organizačního Ing. Petru Hodboďovi a vedoucímu oddělení informatiky Ing. Tomáši Kejzlarovi, kteří se mnou spolupracovali v průběhu mého testování. Poděkovat bych chtěl také Kláře Vyčítalové za pomoc, kterou mi věnovala při objasňování problematiky pojištění. Poděkování patří rovněž celé mé rodině a přátelům za jejich podporu, kterou mi po celou dobu poskytovali.

Abstrakt

Práce popisuje problematiku lidského faktoru v oblasti bezpečnosti informačních systémů. Jsou popsány metody útoků využívající lidský faktor k narušení bezpečnosti a i způsoby, jak tyto hrozby odvracet. Součástí práce je také testování informačního systému existující organizace z pohledu odolnosti proti metodám sociálního inženýrství.

Obsah

Seznam obrázků

Úvod

Nasazení informačních systémů a technologií se stalo v současnosti nutnou podmínkou úspěšnosti mnoha organizací. Bez nich je dnes práce neefektivní a dokonce i mnohdy nepředstavitelná. Spolu s rozvojem informačních technologií a jejich vzrůstajícímu nasazení ve všech oblastech společnosti výrazně také vzrostly možnosti jejich zneužití. Informační kriminalita se stala běžnou realitou dneška. Konkurenční boj na jakékoliv úrovni podnikání přinesl fakt, že informace jsou zbožím, jejichž cena může mít nemalou hodnotu a jejich cena láká nejen útočníky-profesionály, jako jsou průmysloví špióni či hackeři, ale také vlastní zaměstnance podniku, kteří vidí jedinečnou příležitost jak se rychle a snadno obohatit.

Ukazuje se, že technické zabezpečení systémů je dnes již tak komplikované a účinné, že útočníci se snaží toto zabezpečení alespoň částečně obejít prostřednictvím lidského faktoru. V současnosti roste počet útoků, v nichž figuruje lidský faktor. Lidský faktor v oblasti bezpečnosti informačních systémů je často podceňován, ba dokonce u některých organizací by se dalo přímo říct, že je opomíjen. Přitom paradoxně útoky na informační systém, v nichž figuruje lidský faktor, jsou v současnosti charakteristické vysokou úspěšností.

Tématem bakalářské práce je lidský faktor v oblasti bezpečnosti informačních systémů a jejím cílem je seznámit čtenáře s útoky zneužívající lidský faktor a nastínit opatření, které organizace mohou zavést, aby rizika těchto útoků v co největší míře minimalizovaly.

V první části práce jsou popsány metody, jež útočníci využívají. V druhé části práce uvádím, jaké jsou možnosti obrany proti těmto metodám, a dále ve třetí části je stručně popsána právní úprava problematiky ochrany informací. Následně pak ve čtvrté části jsou uvedeny případy, kdy došlo k úniku informací a kde podstatnou roli hrál lidský faktor. Přibližuji, v kterých oblastech nebyl informační systém dostatečně zabezpečen a jaké konkrétní kroky by měly učinit organizace, aby své systémy proti této formě selhání lidského faktoru zabezpečily. Poslední pátá část je rozsáhlejší a podrobně v ní popisuji průběh svého testování informačního systému Magistrátu města Děčín v oblasti bezpečnosti zpracovávaných osobních údajů, proti němuž jsem se pokusil použít metody sociálního inženýrství. Cílem tohoto testování, bylo zjistit, do jaké míry jsou osobní údaje zabezpečeny a navrhnout pak případná opatření, aby byla jejich bezpečnost dostatečná.

1 Selhání lidského faktoru v oblasti informační bezpečnosti

1.1 Obecný úvod do problematiky

Informační bezpečnost jako obor zabývající se zabezpečením informací v počítačových technologiích je relativně nový pojem. Jeho počátky lze vysledovat v první polovině 80. let. V té době se začaly uplatňovat k řízení chodu organizací a uchovávání informací ve větší míře informační systémy založené na informačních technologiích a vznikla potřeba tyto informační systémy dostatečně také zabezpečovat.

Informační bezpečnost lze chápat jako ochranu informací během jejich vzniku, zpracování, ukládání, přenosu a likvidace prostřednictvím logických, technických, fyzických a organizačních opatření, která musí působit proti ztrátě důvěrnosti[1], integrity[2] a dostupnosti[3] hodnot. Proti úniku informací musí být každý informační systém zabezpečen.[1]

Většina firem se dnes spoléhá zejména jen na technologické zabezpečení svých systémů. Brání svůj intranet před hrozbami zvenku hradbou firewallů, přístup k informacím podmiňují přístupovými právy, šifrují svá data apod. Avšak technologické zabezpečení je pro bezpečný systém podmínkou nutnou a ne postačující. Systém není tvořen jen hardwarovým a softwarovým vybavením. Do systému patří také komplex postupů, služeb a lidí určených ke zpracování a získávání informací. Systém je tak silný, jak je silný jeho nejslabší článek. Dnes je tím neslabším článkem informačních systémů právě lidský faktor. Je přeci mnohem snazší oklamat zaměstnance než probourávat se firewally. Počítače nepřemýšlí, nemají svědomí, nerozhodují se. Dělají přesně to, co se jim naprogramuje, nastaví. Lidé jsou oproti tomu komplikovanější a méně spolehliví. Vnímají věci v širších souvislostech, bojí se, chybují, jsou náladoví, rozčilují se, podléhají emocím.

[1] Důvěrnost – ochrana před prozrazením informace

[2] Integrita – ochrana před neoprávněnou modifikací

[3] Dostupnost – ochrana před neoprávněným odmítnutím služby nebo nemožností službu poskytnout

Formy selhání lidského faktoru v oblasti bezpečnosti informačního systému lze rozdělit do dvou skupin dle toho, kdo je nositelem, resp. původcem ohrožení bezpečnosti.

- **Narušení bezpečnosti vnějším útočníkem** – Téměř všechny tyto formy útoku, lze označit za metody sociálního inženýrství. Útočník se pokouší zmanipulovat obsluhu systému.
- **Narušení bezpečnosti vlastním zaměstnancem** – Msta, vydírání, zneužití informací, narušení z nedbalosti. Zaměstnanec organizace se sám přímo pokouší narušit bezpečnost informačního systému.

1.2 Narušení bezpečnosti vnějším útočníkem – sociální inženýrství

Zkušení útočníci se vždy pokouší napadnout nejslabší článek v zabezpečení systému a využití lidského faktoru k napadení informačního systému je dnes zpravidla nejsnazší cestou. Všechny metody útoku na informační systém, v kterých určitým způsobem figuruje lidský faktor, se označují jako metody sociálního inženýrství. Jsou to metody, kdy se útočník snaží oklamat obsluhu systému, aby provedla aktivitu, která vede k narušení bezpečnosti systému.

Podstatu sociálního inženýrství nejlépe vystihl Kevin Mitnick ve své knize Umění klamu, kde doslova napsal: *„Oblíbené rčení zní, že bezpečný počítač je vypnutý počítač. Vtipné, ale nepravdivé: podvodník prostě přemluví někoho, aby šel do kanceláře a ten počítač zapnul.“* [2]

Dle [3] sociální inženýrství je *„ ...umění využívající slabostí lidského uvažování vedoucí k narušení bezpečnosti informačního systému, přičemž sama oběť nemá podezření, že je jí manipulováno“*. Někdy je často označováno také jako sociotechnika. Pak o útočníkovi, jenž ovládá metody sociálního inženýrství, hovoříme jako o sociotechnikovi.

Je třeba zdůraznit, že se jedná o umění. Ne každý, kdo zná metody sociálního inženýrství, je dokáže správně využít. K tomu musí mít další předpoklady, jako jsou schopnosti improvizace, rychlého uvažování, trpělivosti a potřebné znalosti informačních technologií.

Lze rozlišit dvě skupiny metod. První skupinou jsou metody přímé manipulace. Při těchto metodách útočník přímo komunikuje s obsluhou systému buď prostřednictvím telefonu nebo jednáním tváří v tvář. Jedná se o poměrně náročné metody, které kladou na útočníka

velké požadavky. Na druhou stranu o těchto metodách většina lidí nemá ponětí a tak jsou poměrně hodně úspěšné. Firmy zabývající se bezpečnostními audity udávají, že úspěšnost těchto metod při prvním auditu je velmi vysoká. [2]

Druhou skupinou metod, jsou metody založené na technických prostředcích. Tato skupina metod díky tomu, že je založena na technických prostředcích, umožňuje oslovit velký počet potenciálních obětí ve velice krátkém čase a je tedy charakteristická svou masovostí. Například dle [4] úspěšnost dobře připravených phishingových útoků je velice nízká a to v rozmezí 2-3%. Avšak při představě, že útočník činnosti spojené s oslovení oběti může zautomatizovat napsáním skriptů a s minimální námahou pak může oslovit až několik tisíc uživatelů, je tato představa již poměrně děsivá.

Sociotechnici využívají přirozenou lidskou tendenci důvěřovat lidem a nezamýšlet se nad bezpečností. Vydávají se za jinou osobu jako je nadřízený oběti, její spolupracovník, osoba, jež má blízký vztah k firmě. Snaží se oklamat oběť, že jejich požadavek je zcela normální a přesvědčují ji, že nebude zodpovědná za poskytnutí informací. Jakmile získají důvěru oběti, mají velkou naději, že oběť jim důvěrné informace poskytne. Pro vybudování důvěry zná sociotechnik několik vlastností lidské psychiky, které se projevují u každého zaměstnance, a na těchto vlastnostech staví své útoky.

1.2.1 Slabé stránky lidské psychiky

Silné emoce

Pokud je oběť uvržena do velmi emocionálního stavu, ztrácí přehled o situaci, nedokáže v rozrušení tolik logicky uvažovat a přestane nad svým jednáním přemýšlet. Aby útočník uvedl svou oběť do takového stavu, musí ji překvapit, šokovat nebo naštvat a neustále při tom udržovat v takovém napětí, aby nepřemýšlela nad tím, co vlastně útočník po ní chce.

Zahlcení

Člověk nedokáže vnímat a zpracovávat mnoho informací ve stejný čas. Pokud je oběť zahlcena informacemi, začne se v nich ztrácet, začne zmatkovat a hlavně přestane nad nimi přemýšlet. Stejného výsledku se dá také dosáhnout, pokud je oběť postavena před situaci, kterou může řešit mnoha způsoby. Raději než, aby zdlouhavě přemýšlela jakou metodou situaci řešit, nechá si ochotně poradit od útočníka slabými argumenty.

Vděk

Sociotechnik tuto vlastnost lidské psychiky využívá v dlouhodobé perspektivě. Lidé mají tendenci oplácet pomoc druhému, pokud on jim před tím také pomohl. Později poté, co útočník oběti pomůže, kontaktuje svou oběť s dostatečně velkým časovým odstupem, aby u ní nevzbudil podezření, a požádá ji o pomoc.

Kompromis

Když se dva přou a první po dlouhé hádce ustoupí a sleví ze svého požadavku, druhý bude mít tendenci pak také slevit a oba dva se dohodnou na kompromisu. Útočník zahltí oběť několika požadavky a posléze některý ze svých požadavků, na kterém mu vůbec nezáleží, stáhne. Oběť pak je spokojena, že útočník aspoň částečně uznal její argumenty, a některé z žádostí vyhoví.

Sympatie

Mezi lidmi se společnými zájmy a stejnými problémy vzniká zvláštní druh přátelství. Tito lidé mají větší tendenci si důvěřovat, protože si myslí, že ten druhý jim rozumí a lépe je chápe. Útočník se proto snaží u oběti vyvolat dojem, že je jedním „z nich“ nebo má společné záliby.

Spoluzodpovědnost

Útočník přesvědčuje oběť, že také on je zodpovědný za situaci, kterou oběť musí řešit a případná vina padá i na něho. Lidé jsou svolnější k rizikovým k aktivitám, když ví, že nejsou „sami na palubě“.

Morální povinnost

Oběť je oslovena o něco, kdy zamítnutí takové žádosti by bylo v konfliktu s morálkou společnosti nebo firmy. Nejčastější je žádost zaměstnance v nouzi, kdy případné zamítnutí znamená pro zaměstnance propuštění. Další možností je například taková žádost, kdy nevyhovění může poškodit firmu v očích veřejnosti nebo zákazníků.

Strach z autorit

Zaměstnanci raději slepě souhlasí bez jakýchkoliv otázek s kýmkoliv, kdo je v organizaci výše postavený než oni samotní. Zaměstnanec nechce ohrozit svou pozici ve firmě jen kvůli tomu, že odmítne sdělit svému nadřízenému některé informace a tak dokonce ani zpravidla po svých nadřízených nepožaduje, aby prošli základní procedurou verifikace.

Sounáležitost

Spolupracovníci mají tendence si vzájemně pomáhat a to i dokonce, když mezi sebou cítí antipatie. Útočníci toho využívají tím způsobem, že se vydávají za kolegu z práce, který si vzal práci domů a momentálně potřebuje zaslat některá data, bez kterých nemůže dále pracovat.

1.2.2 Sběr informací

Krom znalostí lidské psychiky musí mít útočník co nejvíce informací o struktuře, chodu organizace a jednotlivých pracovnících. Důvod je prostý, čím více informací útočník má k dispozici, tím je přesvědčivější. Zaměstnanci často totiž žijí v mylné představě, že člověk, jenž má přehled o chodu organizace, její organizační struktuře a zná jména zaměstnanců a jejich funkce, je s touto organizací určitým způsobem spojen a považují ho za jednoho ze zaměstnanců, kterému mohou důvěřovat.

Ke spoustě citlivých informací má však útočník často volný přístup. Hierarchie organizace včetně jmen zaměstnanců a jejich telefonních čísel je často zveřejňována na webových stránkách organizace. Také jsou zveřejňovány vnitřní předpisy, dokumenty, telefonní seznamy a významné události v organizaci. Útočníci často také při získávání informací, využívají internetové vyhledávače, k nalezení příspěvků, které do diskuzí vložili zaměstnanci organizace. Tyto příspěvky většinou obsahují pro útočníka zajímavé informace o zaměstnanci a mnohdy i chodu organizace, čehož pak může využít k tomu, aby kdyby se vydával za zaměstnance, mohl být přesvědčivější.[2]

Dalším hodně slibným místem pro sběr informací jsou odpadky. Drtivá většina organizací opomíjí skutečnost, že mnoho cenných informací se dostává ven prostřednictvím

odpadků a útočník prohledáváním odpadků (Dumpster Diving[4]) může získat mnoho cenných informací.[3]

Někdy útočník musí přikročit k přímému dotazování zaměstnanců organizace. Útočník zpravidla provede několik telefonátů a při každém získá určitou informaci. U zaměstnanců krátké telefonáty nevzbuzují podezření a informace, které útočník požaduje, zaměstnanci nepovažují ani většinou za citlivé. V celku ale tyto „bezvýznamné“ informace mohou být pro útočníka velmi cenné.

1.3 Sociotechnické metody

Na základě dostatku znalostí o chodu organizace útočník zvolí metodu, proti které bude informační systém organizace nejméně odolný. Výběr metody závisí na charakteru organizace, jejíž systém se pokouší útočník napadnout, a také na informacích o systému organizace, které má útočník k dispozici.

1.3.1 Útoky prostřednictvím telefonních hovorů

Útočník často využívá telefon, kdy se vydává za osobu, jež je oprávněná dané informace nebo aktivity po zaměstnanci požadovat. Přitom využívá výše popsaných slabin lidské psychiky, kdy například oběť zahltí velkým množstvím informací, vydává se za nadřízeného, předvádí zoufalého člověka, který potřebuje pomoc atd. Velkou výhodu pro útočníka je, že pokud obsluha prohlédne jeho záměry, zůstává neodhalen a nehrozí mu žádné nebezpečí. Útočník si vždy vybírá za svou oběť osobu, která nemá zpravidla ponětí a o hodnotě informace, kterou se snaží útočník získat. Typickým příkladem jsou sekretářky a vrátné.

Poměrně sofistikovanou metodou, která se realizuje prostřednictvím telefonních hovorů, je metoda nazývaná „**reverse engineering**[5]“. Tato metoda spočívá ve vytvoření situace, kdy oběť sama požádá sociotechnika o pomoc. Celá taktika se skládá ze tří částí: představení se, vytvoření problému a poskytnutí pomoci. Sociotechnik nejprve své oběti zavolá a představí se jako osoba, která dokáže ihned vyřešit její budoucí problém. Nejsnazší cestou je vydávání se za osobu z informačního oddělení, za dodavatele softwaru a například

[4] „Dumpster Diving“ – Volně přeloženo jako „Potápění se v popelnicích“.

[5] **„**Reverse Engineering“ - volně přeloženo jako „podraz“

se jen dotázat na to, jestli jsou s dodávaným softwarem spokojeni, jestli se nesetkali zatím s žádným problémem a přitom sdělí oběti kontakt na sebe. Sociotechnik pak vytvoří určitý problém, před který postaví oběť. Problém si může sociotechnik vymyslet, nemusí být skutečný. V našem příkladě třeba kontaktuje zaměstnance, sdělí mu, že je z vedlejší pobočky a právě se jim zničila celá databáze, protože v dodávaném softwaru je bezpečnostní trhlina. Takový zaměstnanec pak zcela jistě bude telefonicky kontaktovat dodavatele softwaru s žádostí o pomoc. Sociotechnik pak ochotně své oběti pomůže. [2]

1.3.2 Vydávání se za zaměstnance organizace

Pokud organizace ukládá zaměstnancům nosit uniformu (ostraha budovy) či vydává zaměstnancům oblečení se svým logem, nápisem, útočník se pokusí toto oblečení získat, protože v něm bude vypadat mnohem věrohodněji a pokusí se v převlečení za zaměstnance organizace vniknout do budovy. Sociotechnik se pak snaží dostat do prostoru kanceláří, které pak jednotlivě prochází a pátrá v nich po zajímavých informací či pozoruje aktivity zaměstnanců (tzv. shoulder surfing[6]).

Útočník se také může vydávat za nového zaměstnance nebo za zaměstnance z jiného oddělení, pobočky a požádá své kolegy o pomoc. Útočník je přesvědčivější o to, že jedná v tváří v tvář. Na druhou stranu se však také vystavuje velkému riziku v případě, kdy zaměstnanci si budou chtít ověřit jeho totožnost.

1.3.3 Vydávání se za obchodního partnera organizace

Pro útočníka nejobtížnější metodou je jednání, kdy se vydává za třetí stranu. Například navštíví budovu organizace v době, kdy nadřízení zaměstnanců již nejsou v budově přítomni nebo jsou na dovolené a představí se jako velmi významný obchodní partner či zástupce společnosti, s níž organizace velice intenzivně spolupracuje, a vyžádá si citlivé informace. Vše může zdůvodňovat tím, že daná organizace s nimi uzavřela dohodu o úzké spolupráci na společném projektu a nevyhovění žádosti může ohrozit pozice obou společností.

6 „Shoulder surfing“ - volně přeloženo jako „nahlížení přes rameno“.

1.3.4 Phishing

Phishing je metoda využívající kombinace sociálního inženýrství a informačních technologií. V podstatě se jedná o souhrn metod, jejichž cílem je „ulovit“ uživatele. Zpravidla se toho dociluje tím, že uživateli je zaslána podvržená zpráva vyzívající ho k určité aktivitě jako např. sdělení citlivých údajů nebo vykonání činnosti na svém počítači, která pak umožní útočníkovi získat nad počítačem kontrolu.

Existují dva názory, jak byl odvozen termín pro tuto metodu. Prvním z nich je, že slovo phishing by se dalo volně rozložit na dvě anglická slova „ personal fishing“. Volně přeloženo se tedy jedná o rybaření, kde jsou na návnadu chytáni lidé. Druhý názor je mnohem prostší. Slovo phishing vzniklo na IRC chatech[7], kde uživatelé často zaměňují hlásku „f“ za „ph“. Výslovnost je totiž téměř totožná.

1.3.5 Klasický phishing

Klasický a nejznámější phishing je forma SPAMu[8] nejčastěji spojována s bankovními podvody, krádežemi osobností (identity theft[9]) a podvody týkajících se kreditních karet.

Slabinou protokolu SMTP[10], který je používán pro přenos emailových zpráv, je že nikterak neověřuje původce zprávy. Tedy jestli jméno odesílatele uvedené v hlavičce zprávy patří skutečnému odesílateli. Proto téměř kdokoliv, kdo má potřebné znalosti, může odeslat email, v němž může uvést u odesílatele jakoukoliv emailovou adresu.

Oběti zpravidla přijde emailová zpráva tvářící se jako sdělení z finančního ústavu. Oběti je oznámeno, že došlo k pádu systému a část dat klientů byla narušena. Oběť je ve zprávě požádána, zda informace uvedené ve zprávě souhlasí se skutečností a aby tyto informace potvrdila nebo případně opravila na níže uvedených stránkách finančního ústavu. Oběť ale není navedena odkazem uvedeným v emailové zprávě na skutečné stránky ústavu, ale na podvržené stránky, kde je dotázána na PIN, číslo účtu a další citlivé údaje. Tyto informace pak nejsou odeslány finanční instituci nýbrž samotnému útočníkovi.

---

[7] IRC – Internet Relay Chat byl jednou z prvních možností komunikace v reálném čase po internetu.

[8] SPAM - Spam je nevyžádané sdělení masově šířené Internetem. Zpravidla se jedná o emailové zprávy.

[9] Identity Theft – Útočník se snaží získat osobní údaje o osobě. Ty pak použije např. k vyřízení půjčky.

[10] SMTP - Simple Mail Transfer Protocol je internetový protokol určený pro přenos zpráv elektronické pošty mezi stanicemi. Protokol zajišťuje doručení pošty pomocí přímého spojení mezi odesílatelem a adresátem.

URL[11] stránek, na které je uživatel odkazován ve zprávě, je velmi dobře maskována, aby oběť neměla podezření. Zpravidla pouze dle URL adresy stránky lze rozeznat, zda se jedná o podvrženou stránku. Například skutečná adresa www.PayPal.com je maskována jako www.PayPa1.com. Písmeno „l“ je v URL adrese těchto stránek nahrazeno „1“, číslicí.

Čím více cílů se Phishing dotkne, tím více lidí tyto informace poskytne a útok je úspěšnější. Počet obětí je totiž přímo úměrný počtu oslovených uživatelů. V současnosti výskyt útoků touto formou má u nás vzestupnou tendenci. Ve vysoce vyspělých zemí jako je USA a Kanada tyto útoky jsou de facto na denním pořádku a vzhledem k tomu, že tamní uživatelé jsou již proti těmto útokům obezřetní, útočníci přesouvají své aktivity jinam a zaměřují se na země, kde většina obyvatel nemá ještě dostatečné povědomí o této formě útoku.

1.3.6 Spear Phishing

Spear Phishing je zvláštní metodou Phishingu. Stejně jako běžný Phishing využívá SPAMu a dále jiných forem šíření zpráv prostřednictvím Internetu (např. ICQ[12] protokol) spolu s kombinací sociálního inženýrství. Tento typ útoku je zaměřen proti anonymní uživatelům Internetu. Není nikterak cílený. V případě emailových zpráv je k samotné zprávě přidružena příloha obsahující spyware, vir či trojského koně. Po otevření přílohy je spuštěn zákeřný kód, kdy zpravidla dojde k infiltraci operačního systému.[4]

V minulosti se také k šíření virů apod. využíval JavaScript[13] či chyb některých emailových klientů jako je MS Outlook. K nejznámějším Spear Phishingovým útokům patřil virus I LOVE YOU, který se šířil prostřednictvím emailů a po otevření se odeslal na všechny adresy, které měla oběť uvedena v kontaktech. Dnes se Spear Phishingové útoky šíří zejména prostřednictvím odkazů v ICQ klientech.

---

[11] URL - Zkratka anglického výrazu Uniform Resource Locator. Je to řetězec znaků s definovanou strukturou a slouží k přesné specifikaci umístění zdrojů informací (ve smyslu dokument nebo služba) na Internetu.

[12] ICQ protokol - Umožňuje uživatelům sledovat, kteří jejich přátelé jsou právě připojeni, a dle potřeby jim posílat zprávy, chatovat, přeposílat soubory mezi uživateli a i jinak komunikovat.

[13] JavaScript - Programovací jazyk pro WWW stránky, vkládaný přímo do HTML kódu stránky. Jsou jím obvykle ovládány různé interaktivní prvky GUI nebo tvořeny animace a efekty obrázků.

1.3.7 WiPhishing

WiPhishing je poměrně novou metodou.Útočník, jenž zjistí, že organizace využívá uvnitř svých budov wifi[14] síť, se pokusí k této budově dostat, co nejblíže a na svém přenosném počítači vytvoří kopii této wifi sítě, kterou pak uvede do provozu. Pracovní počítače zaměstnanců jsou zpravidla nakonfigurovány, tak že se automaticky připojuji k preferovaným wifi sítím. V tom případě, se počítač zaměstnance v místech, kde místo v budově je pokryto jen útočníkovým signálem, sám automaticky připojí na síť útočníka, a tak síťová komunikace zaměstnance bude vystavena hrozbě odposlouchávání nebo počítač bude vystaven hrozbě napadení zkušeným útočníkem.[5]

Většinou ale útočníci tuto metodu používají k odposlechu hesel a citlivých údajů osob, které se náhodně připojují k síti. Útočník vytvoří kopii hot spotu [15], kterou jako službu poskytuje některý mobilní operátor a pak odposlouchává komunikaci přihlášených uživatelů. Ti pokud pak nepoužívají k odesílání citlivých dat šifrovaný způsob komunikace, poskytují útočníkovi cenné informace, jenž pak může zneužít. Předpokladem samozřejmě je, že útočník má zároveň přístup do Internetu, aby zprostředkovával komunikaci a tvářil se tak jako skutečný hot spot.

1.4 Vnitřní útok ze strany zaměstnance

Zaměstnanec je dnes nejrizikovějším článkem v zabezpečení systému. Útok na systém organizace vlastním zaměstnancem způsobuje organizaci největší škody, protože zaměstnanec zná dokonale prostředí organizace, má přístup k citlivým dokumentům a zná procesy uvnitř organizace a vztahy mezi zaměstnanci. Případy, kdy zaměstnanec narušil bezpečnost informačního systémů, jsou nejčastější a to zejména z toho důvodu, že takový útok na systém je nejsnazší, protože zaměstnanec nemusí mít žádné zvláštní schopnosti a vědomosti jako je znalost sociálního inženýrství apod.

Proti této hrozbě se systém velice obtížně zabezpečuje. Aby chod organizace byl plynulý a byly dosahovány co nejlepší výsledky, pracovní prostředí uvnitř organizace musí

[14] WiFi – označení pro bezdrátové sítě, vychází ze standardu IEEE 802.11

15 Hot Spot – Přístupový bod pro bezdrátové připojení poskytovaný zpravidla určitým mobilním operátorem.

být přátelské a neustále prověřování a podezřívání zaměstnanců by bylo velice rušivým elementem.

1.4.1 Nejčastější důvody narušení bezpečnosti zaměstnancem a formy útoku

Snadné finanční obohacení

Nejčastějším motivem je ekonomický profit. Zaměstnanec se může ocitnout ve finanční tísni, kdy je neschopen splácet své dluhy. Má například problémy s hazardem. Pak se může pokusit prodat konkurenci obchodní tajemství, převést finanční prostředky instituce na svůj účet nebo vydírat organizaci s tím, že jinak zveřejní citlivé údaje.

V souvislosti s finančním obohacením je často zmiňován termín „salámový útok“ (Salami Attack, Salami Technique). Termín označuje techniku, kdy se při velkém množství transakcí z téměř každé transakce odčerpá neoprávněně malá nenápadná částka. Tato metoda často využívá chyb programů, nebo číselných zbytků při zaokrouhlování čísel.[6]

Sledování osobních cílů

Zaměstnanec může také sledovat své osobní cíle. Může třeba modifikovat data o členech své rodiny, přátelích. Prohlížet si údaje o svých sousedech atd.

Msta zaměstnance

Silnou a pro organizaci velice nebezpečnou motivací může být msta zaměstnance organizaci, kdy zaměstnanec má například pocit, že jeho práce je nedostatečně ohodnocena. Chce se pomstít svému nadřízenému. Tuší, že bude propuštěn apod. Takovýto zaměstnanec představuje pro organizaci jednu z největších hrozeb, protože činy zaměstnance toužícího po pomstě mají většinou destruktivní charakter.

Aby zaměstnanec zůstal pokud možno v anonymitě, nebyl z takovýchto činů následně podezřelý, používá se tzv. logických bomb. Logickou bombou lze rozumět, část zákeřného programového kódu, který se spustí při určité události. Touto událostí může být uplynutí určité časové doby, nebo specifický vstup do systému. Logické bomby mohou být skryty v systému i několik let po propuštění zaměstnance.

Nedbalost

Neodborné zacházení, chyby administrátorů, neznalost systému apod. lze také zařadit do důvodů, jež vedou k narušení bezpečnosti. Narozdíl ale od všech předchozích, tyto nelze zařadit mezi vědomé útoky a nemůžeme, zde tak mluvit o žádném útočníkovi. Je však je třeba zmínit, aby ani tyto důvody nebyly opomenuty. Typickým příkladem může být odeslání dokumentů na špatnou emailovou adresu nebo zveřejnění citlivých informací na webovém serveru organizace.

2 Ochrana informačního systému organizace

2.1 Bezpečnostní politika organizace

Ochrana informačního systému proti selhání lidského faktoru je velice obtížná. Při budování dostatečně odolného systému je třeba si uvědomit jednu skutečnost: Bezpečnost není produkt, ale proces. Většina organizací žije v přesvědčení, že dostatečnou ochranu lze zajistit pouhým nákupem, tedy pořízením firewallů, antivirů, čipových karet chránících před neoprávněným vstupem do budovy apod. Tato představa je ale naprosto mylná. Spolu s tím, jak se rozvíjí informační technologie, objevují se také nové možnosti zneužití. Na ty musí neustále organizace reagovat přehodnocením své bezpečnostní politiky.[1]

Ochrana informačního systému se realizuje prostřednictvím bezpečnostní politiky. Bezpečnostní politika musí být vypracována na základě předchozí analýzy rizik. Bezpečnostní politika je de facto dokument obsahující tyto položky [6]:

- Popis organizace, jejího poslání
- Stanovení zodpovědností a pravomocí v organizaci
- Klasifikace citlivých informací a určení míry jejich ochrany
- Rámcový plán a harmonogram vybudování bezpečnostní politiky
- Cíle bezpečnostní politiky
- Vypracování bezpečnostní infrastruktury organizace
- Identifikace obecných hrozeb
- Identifikace citlivých dat
- Cíle a strategie havarijních plánů
- Časový plán pravidelných akcí, revizí, oprav
- Návrh koncepce programu školení

Prvním krokem při ustanovení bezpečností politiky je nalezení zranitelných míst. Zranitelným místem zde rozumíme slabinu informačního systému organizace využitelnou ke způsobení škod nebo ztrát způsobených útokem na informační systém. Každý informační systém má několik takovýchto zranitelných míst, které jsou způsobeny zejména selháním v počáteční analýze, návrhu informačního systému nebo chybné implementaci informačního

systému. Krom toho můžou být tato zranitelná místa způsobena vysokou hustotou uložených informací, kdy obsluha systému ztrácí přehled o citlivosti jednotlivých informací, a skrytými kanály pro přenos informace jinou než zamýšlenou cestou.

Dle [6] podstata zranitelného místa může být:

- **fyzická** – umístění informačního systému v místě, které je snadno dostupné sabotáži, vandalismu, výpadku napětí
- **přírodní** – záplavy, požáry, zemětřesení, sesuv půdy, blesk
- **v hardwaru nebo softwaru** – nespolehlivá úložiště dat, nedostatečná kontrola přístupu implementovaná v softwaru
- **v lidském faktoru** – nejčastější a také je nositelem nejtěžších následků. Např. pomsta ze strany zaměstnance, špatná manipulace s daty

Zranitelná místa jsou vlastnostmi informačního systému, jejichž existence způsobuje, že některé vlivy prostředí, ve kterém se informační systém provozuje, představují pro něj hrozby. Pojmem hrozba označujeme možnost využitkovat zranitelné místo informačního systému k útoku na něj.

Charakteristikou hrozby je její zdroj. Ten můžeme dále dělit na vnější (zloděj) a vnitřní (vlastní zaměstnanec). Existence hrozby představuje riziko.

Rizikem rozumíme pravděpodobnost využitkování zranitelného místa informačního systému. Říkáme, že hrozba se uplatní s takovou a takovou pravděpodobností. Krom pravděpodobnosti výskytu lze riziko charakterizovat potenciálně způsobenou škodou.

Nejdůležitější etapou stanovení bezpečnostní politiky je právě analýza těchto rizik, Jejím cílem je identifikace událostí, které mají nežádoucí vliv na aktiva organizace, zjištění jaké škody mohou útokem vzniknout a určení, která opatření rizika hrozeb odstraní nebo alespoň minimalizují a co jednotlivá opatření stojí.

Náplň analýzy rizik lze definovat jako proces porovnávání odhadovaných rizik, jejich pravděpodobností proti ceně možných bezpečnostních opatření. Následně tak můžeme posoudit, zda přijatá opatření by byla přiměřená hodnotě aktiv.

Na základě analýzy rizik se navrhnou opatření, která by rizika minimalizovala na přijatelnou úroveň. Bezpečnostní politiku organizace nelze řešit bez návaznosti na ostatní politiky vymezující chod a poslání organizace. Omezení, která musí být při provozování informačního systému respektována, definuje management organizace a jsou obvykle závislá na prostředí, ve kterém je organizace činná, a řadí mezi ně předpisy, vyhlášky, standardy, zákony a zákonná opatření – jedná se de facto o omezení organizační, finanční, personální, časová, právní, technická, kulturně sociální, omezení životním prostředí atd. Tato všechna omezení významně ovlivňují volbu bezpečnostních opatření.

Bezpečnost systému se pak realizuje kombinací různých bezpečnostních opatření a mechanismů, protože informační systém je vystaven různým formám útoku, které často vyžadují specifický způsob zabezpečení. Z pohledu zabezpečení informačního systému proti hrozbám, útokům zneužívající lidský faktor lze rozeznat bezpečnostní opatření spadající do dvou skupin:

- **Režimová bezpečnost** – Zahrnuje taková opatření, jež jsou realizována formou vnitropodnikových nařízení a směrnic. Nejsou příliš nákladná, ale zajišťování jejich naplňování je celkem obtížné.
- **Personální bezpečnost –** Specifická opatření směřující k ochraně informačního systému proti vlastním zaměstnancům, externím zaměstnancům a bývalým zaměstnancům organizace. Jsou realizovány personálním oddělením nebo zaměstnancem mající na starosti personální politiku organizace.

2.2 Režimová bezpečnost

2.2.1 Obecná charakteristika režimové bezpečnosti

„Režim je administrativní, organizační a věcné uspořádání vztahů mezi lidmi, jejich činnostmi a vlastními procesy v oblasti výkonu i řízení za účelem sladění všech prvků a s cílem dosahování harmonického stavu v dané organizaci.“[2]

Režimem v základním pojetí rozumíme soubor opatření nutných pro určitý účel, řízení nebo vedení vůbec. Jedná se de facto o pokyny, které musí zaměstnanci respektovat a řídit se

jimi při své každodenní činnosti. Režimová opatření z pohledu zabezpečení informačního systému by se měla především týkat:

- Činností pracovníků uvnitř organizace.
- Pohybu a chování osob přicházejících zvenčí.
- Oběhu dokladů a informací uvnitř organizace.
- Výstupu informací, dat, dokumentů vně organizace.

Všechny zásady by měly být zapracovány v patřičných organizačních dokumentech, v interních normách dané organizace, které by měly být naplňovány v každodenním chodu organizace. Správné zavedení režimové bezpečnosti se skládá z několika částí. Nejdříve musí být příslušné směrnice vypracovány, pak jsou implementovány v organizaci zpravidla formou školení zaměstnanců a po implementaci musí docházet k jejich kontrole, jak jsou naplňovány v praxi. S určitým časovým odstupem by se měly přehodnotit a změnit tak, aby se reagovalo na nové hrozby.

2.2.2 Bezpečnostní postupy a pokyny

V každém provozním řádu určitého pracoviště organizace by měla být rozebrána ochrana informačního systému organizace a to v podobě směrnic. Ty by měly být přímo úměrné citlivosti a hustotě uložených nebo zpracovávaných informací v místě pracoviště.

Ve stručnosti by tyto směrnice měly obsahovat:

- **Ověřovací a autorizační procedury** – Jak provést dostatečnou pozitivní identifikaci osoby, která žádá o vykonání určité aktivity nebo sdělení citlivých informací. Jakým způsobem ověřit, že osoba má dostatečné oprávnění k žádosti.
- **Instrukce k distribucím citlivých informací** – Jakým způsobem mohou být předávány citlivé informace. Jaké instrukce musí obsluha systému dodržovat při předávání. Nesmí se zapomínat na to, že nesmí být sdělovány také citlivé informace o spolupracovnících.
- **Instrukce týkající se obsluhy počítače** – Jaké aktivity má zaměstnanec zakázány. Na koho se má obracet s žádostí o pomoc v případě vyskytnutí se problému týkajícího se výpočetní techniky. Komu může umožnit přístup k počítači. Jakým způsobem má volit svá hesla a jak je má chránit.

- **Instrukce týkající se ohlašování incidentů** – Jak mají zaměstnanci postupovat, když dojde k napadení systému. Komu mají hlásit podezřelou aktivitu.
- **Instrukce pro vzdálený přístup do systému** – Jakým způsobem mohou žádat zaměstnanci o vzdálený přístup do systému. Jaké požadavky zabezpečení musí jejich počítače splňovat.

Bylo by velmi vyčerpávající popsat, co vše by měly instrukce obsahovat, a proto níže uvádím, jen některé základní zásady.

Manipulace s informacemi na základě jejich klasifikace

Významnou činností každého podniku, která je většinou podceňována jako zbytečná byrokracie nebo administrativa je klasifikace informací. Ta by měla určovat pravidla, dle kterých by veškeré informace v organizaci měly být rozděleny do několika skupin na základě jejich citlivosti. Každý zaměstnanec by se pak měl řídit určitými pokyny ohledně zpřístupňování informace v závislosti na jejím zařazení. Patřičně klasifikované informace by měly být předávány pouze odpovídajícím kategoriím pracovníků.

Bez této klasifikace by jinak v organizaci jednotliví zaměstnanci rozhodovali pouze na základě svého vlastního subjektivního úsudku a mohlo by dojít k tomu, že citlivá informace by byla sdělena útočníkovi jen proto, že zaměstnanec nevěděl, že tato informace byla citlivá.

Fyzická likvidace dokumentů, úložišť dat

Při ustavování pravidel manipulace s citlivými informacemi se nesmí zapomenout na činnosti spojené s fyzickou likvidací dokumentů. Každá organizace jednou dojde do fáze, kdy bude muset provést tzv. skartační řízení. Při něm dochází k vyřazování dokumentů, které jsou nadále nepotřebné pro současný chod organizace a často k rozhodování, zda dané dokumenty archivovat nebo je zlikvidovat. U obzvlášť důležitých informací je potřeba, aby odpovědný pracovník zůstal přítomen až do poslední fáze fyzické likvidace. Zapomínat se nesmí také na fyzickou likvidaci datových nosičů.

Fyzické zabezpečení systému

Z celého sortimentu dalších dokumentů popisujících či zajišťujících různé způsoby ochrany si zvláštní pozornost zaslouží směrnice strážní služby. Důležité je, aby byla vedena evidence klíčů od pracovních místností, úschovných prostorů, vstupů do objektů. Promyšlené by měly být i směrnice, co se týče úklidu citlivých prostor. Například zda by měl probíhat s dozorem, zda by se měla vést podrobná evidence apod.

Mělo by být zcela jasně stanoveno, jak se má strážní služba zachovat v případě podezřelého chování. Čeho si má všímat. Například v případě, kdy výhled na prostranství je zakryt nějakým objektem, zda má obsluha na tuto skutečnost nějak reagovat. Podobně by měly být stanoveny postupy pro pult centrální ochrany[16]. Strážní služba by měla vést evidenci všech poplachů hlášených pultem centrální ochrany a vždy by je měla prověřit. Musí být také počítáno s tím, jak se má postupovat v případě více poplachů atd.

Organizace by měla mít rozpracován režim pro příchod vlastních zaměstnanců do budovy a pro jejich dočasný, předčasný, definitivní i pozdní odchod z pracoviště. Musí být vypracovány zásady pro pohyb osob uvnitř organizace, a to při rozlišení o jaké kategorie osob se jedná. Tedy jak se má ostraha chovat k vlastním zaměstnancům, externím zaměstnancům, exkurzím, zásobování, služebním návštěvám, soukromým návštěvám, zákazníkům atd.

Vhodné je zvážit, zda by nebylo vhodné zavést povinné nošení identifikátorů zaměstnanci. Pak je ale také podstatné, aby zaměstnanci zastavovali osoby bez těchto identifikátorů a předávali je strážní službě.

Důležité jsou i směrnice chování v případě mimořádných událostí jako požárního poplachu v budově, technologických havárií. I v těchto případech se nesmí zapomínat na bezpečnost informací. Jakmile nebezpečí pomine, ostraha musí urychleně prohledat prostory budovy a ujistit se, že v budově nezůstala osoba, která mohla evakuace zneužít k získání citlivých informací.

[16] Pult centrální ochrany - Soubor zařízení a zásad, jejichž správným skloubením je možno vzdáleně sledovat stavy objektů a dálkově či fyzicky na těchto objektech zasahovat a tak docílit jejich ochrany.

2.2.3 Implementace režimové bezpečnosti

Školení

Zaměstnancům musí být vysvětleno, proč je konkrétní postup, doporučení významné, protože jinak ho budou považovat pouze za bezvýznamné plýtvání časem. Pracovníci si musí být vědomi, že vedení vykazuje silnou víru, že bezpečnost informací je pro fungování firmy nezbytná a že otázka bezpečnosti informací je závislá na individuálním postoji každého z nich. V organizaci je pravděpodobně jen málo záležitostí důležitých pro všechny zaměstnance, které mají tak podstatný význam, a zároveň jsou tak nudné, jako jsou otázky bezpečnosti. Proto by školení mělo být podáváno takovou formou, aby dokázalo zaujmout a vzbuzovat u posluchačů pozornost. Jako vhodné je například promítnout zaměstnancům krátký film, jenž by byl na jedné straně poučný a na druhé straně i zábavný. Všichni zaměstnanci, jež projdou školením, by měli podepsat, že tímto školením prošli, byly seznámeny s bezpečnostní politikou organizace a zavazují se jí také řídit.[1]

Ustanovení systému trestů a odměn

Musí být také stanoven systém trestů a odměn za dodržování směrnic. Zaměstnanec, který bude podceňovat bezpečnost a nebude se řídit instrukcemi, musí počítat s tím, že bude určitým způsobem potrestán. Každé potrestání nebo ocenění zaměstnance by pak mělo být široce rozhlášeno ostatním zaměstnancům.

Ustanovení odpovědnosti za ochranu informací

Při implementaci bezpečnostní politiky organizace je zapotřebí ustanovit orgány, jež budou odpovědné za řádné plnění bezpečnostní politiky v organizaci. Alespoň částečnou odpovědnost by měly nést také osoby mající vyšší postavení v organizaci než běžní řádoví zaměstnanci. Na každém pracovišti by měla být jedna takto odpovědná osoba, která musí mít také mít prostředky, jimiž si toto plnění může vymoct na ostatních zaměstnancích. Také by mělo být stanoveno, kdo bude odpovědný za aktuálnost bezpečnostních směrnic.

2.2.4 Bezpečnostní audit

To, že byla vypracována bezpečnostní politika a byla implementována v organizaci, ještě neznamená, že je dostatečná. Pokud je bezpečnostní politika špatně navržena a kontrola plnění bezpečnosti vlastními zaměstnanci neprobíhá na požadované úrovni, pak tyto

nedostatky odhalí pouze kontrola bezpečnosti vnějšími silami. Tedy takovými osobami, které nejsou natolik spjaté se strukturou a chodem organizace, aby upadly do stereotypu každodenní rutinní práce v organizaci, a tak jsou spíše si schopni všimnout nedostatků zabezpečení systému. Důležitější věc je, že díky tomu, že nejsou spjatí s organizací, nebudou brát v kritice ohled na zaměstnance organizace a ani na jejich nadřízené.

Cílem bezpečnostního auditu je odhalit skrytá místa, jež jsou využitelná k útoku na systém a o kterých organizace neví nebo je nedostatečně zajistila. Audit může mít mnoho forem. Zpravidla se uplatňuje audit vnitřní zaměřený pouze na to, zda je vypracovaná bezpečnostní politika organizace správná. Tedy jedná se spíše o formu konzultací a návrhů. Složitější je vnější audit, kdy se auditorská firma pokouší získat citlivé informace ze systému, aniž by před tím dostala od zadavatele o systému jakékoliv informace využitelné pro samotný útok, přičemž zaměstnanci neví, že jejich organizace se rozhodla podstoupit tuto formu auditu.

Závěrem auditu by měl být dokument shrnující jeho průběh, odhalená slabá místa v systému a i návrhy, jak tato slabá místa nejvhodnějším způsobem zabezpečit.

2.3 Personální bezpečnost

Jedná se o ochranu informačních systémů z hlediska úmyslného jednání a chování vlastních zaměstnanců. Personální bezpečnost působí především v oblasti prevence.

Z velké části je personální bezpečnost zajišťována prověrkami zaměstnanců. A to prověrkami budoucích, potencionálních zaměstnanců organizace a prověrkami stávajících zaměstnanců. Zejména by se měly důkladně prověřovat osoby působící v managementu organizace a ve vysokých vedoucích postech. Nemělo by se zapomínat na osoby, jež z organizace již odešly a byly seznámeny s citlivými nebo utajovanými informacemi. Prověrky zaměstnanců by se měly cyklicky opakovat.

O tom, do jaké hloubky by měla prověrka zasahovat, rozhoduje stávající či budoucí funkční postavení prověřované osoby s ohledem na to, s jakými informacemi v organizaci bude přicházet do styku. Nestačí shromáždit pouze informace o osobě ze současného bydliště, ale je nutné také získat informace o osobě z dřívějších bydlišť a pracovišť. Sběr takových informací je ale velmi komplikovaný a často se organizace uspokojují pouze s výpisem z trestního rejstříku. Nicméně pokud má být daná osoba zasvěcena do velmi citlivých událostí,

měly by se sledovat její kontakty, s kým se osoba ve svém volném čase stýká. Tyto skutečnosti jsou zvláště významné. Ve vyspělých státech jdou některé zejména finanční instituce až tak daleko, že posílají své zaměstnance na fyziodetekční vyšetření.[2]

V případě, že zaměstnanec ukončil nebo mu byl ukončen pracovní poměr, personální oddělení musí zajistit, aby bylo odstraněno jeho jméno z telefonního seznamu a všech jiných dokumentů popisující organizační uspořádání organizace. Dále je nutné informovat strážní službu, aby dále nevpouštěla tohoto zaměstnance do neveřejných prostorů organizace. Vhodné se také jeví pravidelně informovat všechny zaměstnance o tom, které osoby již nejsou nadále zaměstnanci organizace a nesmí mít tedy přístup k citlivým informacím. Naprosto nezbytné je upozornit oddělení informatiky, aby okamžitě byla zrušena veškerá přístupová práva do systému organizace.

2.4 Pojištění

Je třeba si uvědomit, že zavedení bezpečnostní politiky v organizaci hrozby neeliminuje, ale pouze rizika spojená s bezpečností systému minimalizuje na přijatelnou úroveň. Proto je třeba si být vědom toho, že i přes dobře navrženou bezpečnostní politiku a i její dobrou implementaci, může dojít k selhání lidského faktoru a následně k úniku informací. Únikem informací nemusí být poškozena jenom samotná organizace, ale i organizace, která je například obchodním partnerem, či fyzická osoba, která organizaci svolila zpracovávat své citlivé údaje. Je velice pravděpodobné, že osoby určitým způsobem postižené únikem informací se budou dožadovat odškodnění. Pro tento případ by měla být organizace pojištěná.

V západních zemích a zejména v USA je pro tento účel nabízeno specifické pojištění informačního systému označované jako „*Cyber Crime Insurance*“ nebo „*Cyber Risk Insurance*“. Jedná se o komplexní pojištění, které má pokrýt veškerá rizika spojená s provozem informačního systému. Toto specifické pojištění vyžaduje po organizaci také specifický přístup. Pro správné plnění pojištění je nutné, aby organizace měla vypracovanou bezpečnostní politiku dle konkrétních norem a kontrolu jejich plnění zajišťovala bezpečnostními audity. Na výsledky těchto bezpečnostních auditů musí organizace reagovat a musí je neustále podstupovat v pravidelných intervalech.

V podmínkách České republiky toto pojištění neposkytuje žádná instituce a dá se předpokládat, že poptávka po tomto specifickém pojištění by u nás byla velice nízká. Obdobnou formu pojištění je možno u nás sjednat pouze individuálně. Nicméně hrozby

plynoucí z lidského faktoru v oblasti zabezpečení systému lze u nás pokrýt pojištěním za škodu z odpovědnosti. Tuto formu pojištění u nás poskytuje většina institucí.

Organizace má dvě možnosti, jak toto pojištění zavést ve své organizaci. Buďto nechá se pojistit jako celek a pojištění se tak bude vztahovat na všechny zaměstnance organizace, nebo nechá pojistit konkrétní zaměstnance, což je vhodné u institucí, které se zpracováváním citlivých informací zabývají pouze okrajově. Je zde také možnost, že zaměstnanec se nechá pojistit sám o sobě, tedy z vlastní iniciativy, což je doporučováno většině zaměstnanců zpracovávající citlivé informace a které organizace odmítá sama pojistit.

Aby mohla být ale požadována po pojišťovně náhrada škody, je třeba pojistným událostem předcházet. Není tedy možné se nechat pojistit a pak složit ruce v klín. Je nutné mít vypracovanou bezpečnostní politiku a neustále ji zdokonalovat.

2.5 Bezpečnostní standardy

Návrhy pro vypracování bezpečnostní politiky jsou obsaženy v mnoha standardech. V podmínkách České republiky za jejich návrh a vypracování odpovídá Český normalizační institut, který zpravidla v této oblasti přejímá normy ze zahraničí a to většinou pouhým překladem. Organizace mající zájem na tom, aby byl její informační systém vnímán jako bezpečný, by měla mít snahu tyto bezpečnostní normy přijmout a implementovat do svého sytému. Níže uvádím několik norem věnující se bezpečnosti informačního systému. Tyto normy jsou si svým obsahem velice blízké a zpravidla popisují metodiku, jakým způsobem má být správně zavedena bezpečnostní politika organizace. [7]

- ČSN ISO/IEC 17799
- ČSN/ISO 27001
- ČSN ISO/IEC TR 13335
- ČSN ISO/IEC 15408

3 Právní úprava v ČR

3.1 Obecná charakteristika právní úpravy v ČR

Bezpečnostní politika organizace je preventivním prostředkem, který umožňuje odvracet hrozby. Naproti tomu právní normy jsou prostředkem represivním. Tedy k jejich uplatnění dochází až potom, kdy byl spáchán delikt. Je třeba si uvědomit, že sama právní úprava sama o sobě nestačí a v oblasti informační bezpečnosti to platí dvojnásob. Škody, které mohou vzniknout narušením bezpečnosti, jsou zpravidla nenapravitelné a poškozují organizaci v očích veřejnosti a svých partnerů. Nízká právní prokazatelnost „informačních deliktů“ a vidina snadného a zároveň velkého obohacení jsou pro útočníky dostatečnou motivací, která je pro ně silnější než strach z případných represivních opatření.

Základním problémem je dnes právní prokazatelnost trestného činu. V “informačních deliktech” se totiž obtížně obstarávají důkazy. Často se také stává, že poškozená instituce se rozhodne nepodat trestní oznámení na pachatele, ačkoliv i zná jeho totožnost. Obává se totiž, že v případě zveřejnění kauzy, by pak v očích svých zákazníků mohla vypadat jako velice nevěrohodný partner. Proto většina případů, kdy došlo k úniku informací, je zamlčována i postiženými organizacemi.[2]

Vzhledem k rozsahu právní úpravy je níže popsána úprava jen velice stručně a jsou popsány jen stěžejní zákony. Hlubší popis by zcela jistě přesahoval rámec bakalářské práce. Některé zákony kromě, případných trestů pro pachatele, stanovují povinnosti pro provozovatele informačního systému zpracovávající státem chráněné informace popřípadě takové informace, na jejichž ochraně má stát zájem.

3.2 Zákon 101/2000 Sb. o ochraně osobních údajů

Nejvýznamnějším přínosem tohoto zákona bylo stanovení povinností provozovatele informačního systému. Provozovatel je dle tohoto zákona povinen zajišťovat ochranu informací i celého systému před neoprávněným a nahodilým přístupem nebo zpracováním. Také mu ukládá jako povinnost činit taková opatření, aby po skončení pracovního nebo obdobného poměru mezi fyzickou či právnickou osobou a provozovatelem, nemohly být informace, s nimiž nakládá příslušný informační systém, touto osobou využity.

Bohužel zákon sice ukládá povinnost provozovateli zajistit dostatečnou bezpečnost systému, není ale přesně definováno, co se dostatečnou povinností myslí. Jakou formu ochrany provozovatel bude realizovat, to už zákon ponechává čistě na něm.

3.3 Obchodní zákoník

Obchodní zákoník právně definuje pojem obchodní tajemství, jenž patří vedle osobních údajů k nejcennějším informacím. Proto, aby údaje mohly být považovány za obchodní tajemství, musí jejich majitel dle své vlastní vůle je utajit. Majitel musí ale tuto vůli opravdu projevit a zajistit jejich ochranu, jinak takové údaje nejsou považovány za obchodní tajemství. Zákoník pak postihuje toho, kdo poruší obchodní tajemství, tím že ho neoprávněně sdělí jiné osobě nebo ho zpřístupní a toto tajemství pak může být využito v hospodářské soutěži.

3.4 Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti

Nejdůležitější kategorii informací z hlediska jejich možného zneužití představují služební a státní tajemství. Tento zákon upravuje ochranu státního tajemství, vymezuje způsob jeho určení a ochrany před vyzrazením a zneužitím proti zájmům republiky. Základní zásady tohoto zákona platí přiměřeně i pro ochranu hospodářského a služebního tajemství.

Oproti Zákonu o ochraně osobních údajů je stanovena povinnost provozovatele mít na základě citlivosti zpracovávaných informací vypracovanou bezpečnostní politiku. Vhodnost a dostatečnost této politiky pak hodnotí Národní bezpečnostní úřad, jenž pak v případě kladného hodnocení provozovateli vydá certifikát na určitou omezenou dobu opravňujícího zpracovávat utajované informace. Zákon dále popisuje podmínky, které musí bezpečnostní politika organizace splňovat.

3.5 Trestní zákon

Trestní zákon popisuje širokou škálu trestných činů, řada z nich se týká také porušování ochrany informací. Především se jedná o tyto trestné činy:

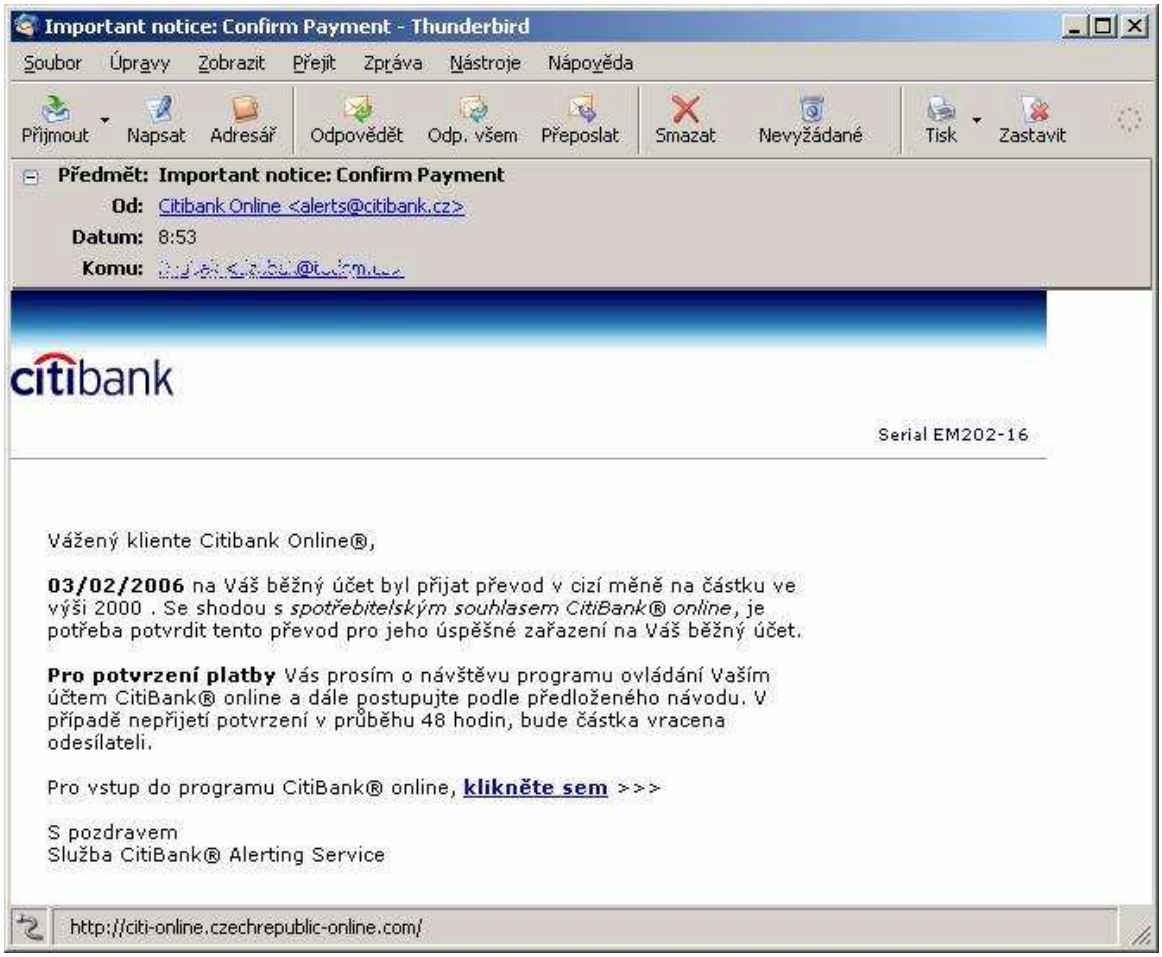
- Vyzvědačství. Vyzrazení státního tajemství cizí mocnosti.
- Ohrožení státního nebo služebního tajemství.

- Ohrožení hospodářského tajemství.
- Zneužívání informací v obchodním styku.
- Poškození a zneužití záznamu na nosiči informací.
- Neoprávněné nakládání s osobními údaji.
- Úmyslné a nedbalostní ohrožení.

4 Případy úniku informací

4.1 Phishingový útok na klienty CitiBank ČR

V březnu 2006 byl proveden phishingový útok na klienty společnosti CitiBank ČR. Do emailových schránek klientů přišla zpráva, že na účet byla připsána platba v hodnotě 2000 liber ze zahraničí. K tomu, aby byla částka skutečně připsána na účet klienta, měla být ze strany klienta-příjemce potvrzena. V textu (obrázek 1) se proto dále nacházel odkaz, pomocí něhož byl klient naveden na falešný přihlašovací formulář společnosti CitiBank, kde po přihlášení měl klient dotyčnou částku potvrdit.[8]



Obrázek 1 Phishing na CitiBank [8]

Jednalo se de facto o historicky první phishingový útok psaný v českém jazyce. Do té doby se útočníci českým institucím zcela vyhýbali. Útočník využil několik triků, kterými chtěl zmást svou oběť. Za prvé slíbil své oběti odměnu za vyplnění přihlašovacích údajů a to

hned v podobě 2000 liber a za druhé vyhradil své oběti omezený čas. Sdělil, že pokud nebude přijetí potvrzeno, celá částka bude vrácena. Na první pohled email vypadal stejně jako emaily rozesílané společností CitiBank. Obsahoval tedy logo společnosti, číslo zprávy a i text byl napsán v typickém strohém stylu společnosti. Proto působil velice důvěryhodně. Odkaz ve zprávě ale odkazoval na adresu *citi-online.czechrepublic-online.com.* CitiBank ČR má své stránky umístěné na adrese *czechrepublic.online.citibank.cz* Odkaz tedy nevedl na stránky společnosti CitiBank ČR, ale na podvržené stránky.

CitiBank ČR na phishingový útok velice rychle reagovala a během několika hodin se jí podařilo vyřadit všechny stránky, na něž bylo odkazováno v textu zprávy. Své klienty také navíc ihned po nahlášení incidentu varovala SMS zprávami a emailem. Dle sdělení společnosti CitiBank nebyly z účtů klientů neoprávněně odčerpány žádné finanční prostředky.

Všechny organizace by měly své zaměstnance varovat, že v emailových zprávách se dá podvrhnout adresa odesílatele. Nelze tedy zaručit, že zpráva pochází skutečně od odesílatele, jenž je uveden ve zprávě.

4.2 Únik osobních udajů z Ministerstva USA pro záležitosti veteránu

3. května 2006 si jeden ze zaměstnanců Ministerstva pro záležitosti veteránů USA přinesl domů svůj pracovní počítač s několika externími disky. Na těchto discích byly uloženy osobní údaje 26,5 miliónu amerických vysloužilců. Zaměstnanec tím tedy hrubě porušil hned několik předpisů, kterými se musel řídit při práci s citlivými osobními údaji.

V noci ze 3. na 4. května byl jeho dům vykraden a externí disky včetně jeho pracovního počítače byly odcizeny. Zloději se tak zmocnili osobních údajů všech osob, které od roku 1975 sloužili v armádě USA, a to včetně čísel sociálního pojištění jejich manželek. O krádeži informoval sám Pentagon a na dopadení zlodějů vypsal odměnu ve výši 50 000 dolarů. Zloději se pak zalekli svého úlovku a počítač i s externími disky zanesli do jednoho ze středisek FBI v Baltimore. Proti nim pak nebyly podniknuty žádné kroky a FBI držela jejich jména v tajnosti.

Nejhorší dopad pro ministerstvo pak byla následná žaloba vojenských veteránů u federálního soudu ve Washingtonu, kteří společně žádali odškodnění ve výši 1000 dolarů pro každého z nich, protože bylo porušeno právo na jejich soukromí.[9]

Vinu za únik informací zde pochopitelně nese zaměstnanec, který porušil vnitřní předpisy organizace tím, že vynesl citlivé údaje vně budovy na místo, které nebylo proti krádeži dostatečně zajištěno. Ačkoliv nebyly organizaci způsobeny žádné škody, musela pak čelit požadavkům na odškodnění a její reputace v očích veřejnosti značně poklesla. Organizace sice měla vypracovanou bezpečnostní politiku, ale ta nebyla důsledně uplatňována v praxi.

4.3 Únik osobních údajů na stránkách Naval Safety Center

Nedlouho poté, co americká armáda čelila žalobě, kterou na ni podali vojenští veteráni, na světlo se vynořil další skandál spojený s únikem osobních údajů. Čtenář webu Naval Safety Center upozornil v červnu 2006 webmastery, že na jejich stránkách se nachází osobní údaje více než 100 000 námořníků. Dle mluvčí centra, která se následně všem postiženým omluvila, k úniku došlo nedbalostí zaměstnanců, kteří mylně vložili osobní údaje do souboru, jež byl následně vystaven na web. Osobní údaje byly na webu zveřejněné již od prosince 2005. Byly tedy dostupné celý půl rok z Internetu.[10]

V tomto případě je vidět, jak důležité je, aby zaměstnanci si byli vědomi citlivosti jimi zpracovávaných informací a vyvarovali se tak špatné manipulaci s nimi. Organizace by neměly podceňovat klasifikaci informací a manipulace s nimi by měla odpovídat citlivosti daných informací.

4.4 Nález osobních údajů klientů Českomoravské spořitelny

V listopadu roku 2006 starosta Jenišova na Karlovarsku nalezl v obecním kontejneru igelitový pytel a dvě krabice obsahující vyplněné formuláře Českomoravské spořitelny. Na formulářích bylo uvedeno jméno, adresa, telefonní číslo a také cílová částka spoření. Jednalo se o klienty z let 2000 až 2004. Případem se ihned začal zajímat úřad pro ochranu osobních údajů a Policie ČR pro podezření z neoprávněného nakládání s osobními údaji.[11]

V tomto případě byla zanedbána skartační činnost spořitelny. V případě, že dokumenty, listiny obsahující osobní údaje klientů nejsou již zapotřebí a spořitelna nemá na jejich dalším uchováním zájem, měla by je důsledně skartovat. Stejně tak by se nemělo zapomínat na uložiště dat. Ta by měla také projít dostatečnou likvidační procedurou a ne pouhým vyhozením do koše.

4.5 Win32 Stration

V říjnu 2006 se začal prostřednictvím Internetu šířit vir Win32 Stration. Ke svému šíření využíval klienta ICQ a emailové klienty nainstalované na počítači. Vir se objevil v několika vlnách a způsobil výrazné škody. [12]

Úspěšnost tohoto viru spočívala v tom, že po infikování operačního systému se sám rozeslal dalším osobám, jenž měl uživatel infikovaného počítače uložené v kontaktech. Osobě, jenž byla uvedena v listě kontaktů, pak přišel ve zprávě odkaz bez jakkéhokoliv dalšího textu. Vzhledem k tomu, že zpráva pocházela od důvěryhodného zdroje, uživatel většinou odkaz otevřel a povolil spuštění souboru, na nějž bylo ve zprávě odkazováno, čímž se na uživatelově počítači spustil vir, který infikoval operační systém. Po určité době se vir na infikovaném operačním systému opět začal rozesílat osobám, jenž měl napadený uživatel uvedené v kontaktech.

Vir se rozšiřoval takovým tempem, až společnost ICQ se rozhodla fitrovat zprávy a odstraňovala z nich veškeré odkazy. Úspěšnost, s jakou se šířil, se dá přisoudit zejména tomu, že tvůrce viru pro jeho šíření využil jednu z metod sociálního inženýrtsví. Spousta uživatelů ICQ si vzájemně posílá odkazy, které bez rozmyšlení otevírají. Odkazy vedou na zajímavé stránky asoubory. Uživateli je tedy slíbena jakási odměna v tom, že se pobaví a na chvíli odreaguje. Většina lidí proto neodolá takové nabídce a odkaz otevře.

Všechny organizace by měly své zaměstnance upozorňovat, aby ihned neotevíraly podezřelé odkazy posílané přes ICQ a emailovou poštu. Nejdříve se musí odesílatele dotázat, kam odkaz míří a zda o odeslané zprávě ví. Vzhledem k tomu, že se po těchto vlnách útoku viru objevují jeho další odnože, jež umožňují útočníkovi i vzdálený přístup do počítače, neměla by se tato skutečnost podceňovat.

4.6 Krádež elektronických adres klientů America Online

V červnu 2004 američtí vyšetřovatelé zadrželi a obvinili zaměstnance společnosti America Online, který získal seznam elektronických adres klientů společnosti a prodával je marketingovým společnostem, které pak na adresy posílaly spam. Zaměstnanec pracoval ve společnosti jako programátor a měl k seznamu emailových adres přístup. Naštěstí pro společnost správně nastavená přístupová práva k uloženým informacím mu zamezila získat i čísla kreditních karet klientů.[13]

Společnost zaměstnance ihned propustila. Nicméně seznam elektronických adres, který ze společnosti unikl, může být dál užíván k šíření spamu.

Organizace by měla umožňovat přístup k citlivým údajům jen těm zaměstnancům, u nichž si je jista jejich loajálností. Ta může být dosažena i nadstandardním platem zaměstnance. Přístupy k citlivým údajům by se měly zaznamenávat a průběžně i vyhodnocovat, zda přístup k nim byl opravdu nutný a z jakého důvodu k nim zaměstnanec přistupoval.

5 Testování odolnosti informačního systému Magistrátu města Děčín

5.1 Cíl testování

Cílem testování bylo zjistit odolnost informačního systému proti použití metod sociálního inženýrství, vedlejším cílem pak získání citlivých informací. V případě, že systém by nebyl dostatečně zabezpečen, jsem měl pak navrhnout takové změny, aby tomu tak bylo.

Vzhledem k citlivosti informací, které jsem se chtěl pokusit získat, jsem nejdříve požádal představitele subjektu, jehož informační systém jsem se rozhodl testovat, o svolení k tomuto testování s tím, že následně mu sdělím výsledky testování a případné návrhy vedoucí ke zvýšení odolnosti jeho informačního systému v tomto směru.

Jako subjekt, jenž byl mnou vybrán pro praktické testování odolnosti informačního systému proti úniku informací, byl zvolen Magistrát města Děčín. Po oslovení magistrátu s testováním tajemník magistrátu souhlasil a pověřil zaměstnance oddělení informatiky, aby se mnou průběžně konzultovali testování. Na tyto zaměstnance jsem se pak obracel a informoval je o svých dalších krocích. Po vzájemné konzultaci s magistrátem jsme se dohodli, že se pokusím získat mé osobní údaje.

5.2 Právní otázky týkající se testování informačního systému

Při testování odolnosti informačního systému jsem se snažil dodržovat právní normy České republiky tak, abych při testování neporušil žádný ze zákonů. Nejproblematičtější v mém případě se jeví Zákon o ochranně osobních údajů[17]. Vzhledem ale k tomu, že získávám své vlastní údaje, tento zákon neporušuji. Stejně tak dle Trestního zákona [18] žádného trestného činu se v případě testování nedopouštím. Není zde úmysl, že bych se chtěl tímto způsobem obohatit nebo někoho poškodit. Nicméně raději jsem se obrátil s dotazem na Úřad pro ochranu osobních údajů (příloha 1), abych měl v této problematice naprostou jistotu. Úřad

[17] Zákon č. 101/2000 Sb.

[18] Zákon č.140/1961 Sb.

pro ochranu osobních údajů mi sdělil (příloha 2), že mnou provedené testování neporušuje žádným způsobem právní normy České republiky.

Vzhledem k citlivosti veřejnosti v otázce zabezpečení osobních údajů, jsem se také po konzultaci s vedoucím oddělením informatiky Magistrátu města Děčín ústně zavázal, že proti magistrátu neučiním žádné kroky, které by ho mohly jakkoliv poškodit. Z tohoto důvodu v níže popsaném průběhu testování neuvádím žádná skutečná jména osob, které jsem se snažil během útoku zmanipulovat. Rozhovory jsou zde ale zaznamenány tak, jak se udály. Pouze jména osob jsou fiktivní.

5.3 Sběr informací

Před samotným útokem jsem musel získat o chodu instituce dostatek informací. Největším zdrojem pro mě byly stránky magistrátu. Některé informace jsem pak musel zjišťovat pomocí několika krátkých nenápadných telefonátů. Také jsem se pokusil vyhledat některé informace pomocí internetového vyhledávače Google.

5.3.1 Použití internetového vyhledávače Google

Vyhledání stránek obsahující řetězec “@mmdecin.cz” nebo “@mudecin.cz”

Prvním krokem byl pokus vyhledat stránky nebo dokumenty obsahující řetězec “@mmdecin.cz” nebo “@mudecin.cz”, tedy takové stránky, na nichž figuruje některá emailová adresa z řad zaměstnanců magistrátu.

Výsledkem dotazu bylo hned několik set webových stránek. I když se sice zpravidla jednalo o stránky věnující se veřejné správě, některé stránky svědčily o tom, že zaměstnanci emailové schránky magistrátu používají i k ryze soukromým účelům.

Bohužel pro mne žádná informace nalezená tímto dotazem nebyla nikterak výrazně cenná. Jediné, co jsem zjistil bylo, že jeden ze zaměstnanců oddělení informatiky úspěšně kandidoval na místo do obecního zastupitelstva své obce (tedy získal jsem informaci o místě jeho bydliště) a také jsem nalezl inzerát jedné zaměstnankyně správního odboru prodávající své auto.

Vyhledání stránek obsahující řetězec “gate.mmdecin.cz” nebo „gate.mudecin.cz”

Některé stránky zobrazují statistiky přístupu ke svému obsahu nebo evidují dotaz v diskuzi prostřednictvím zdrojové adresy v doménovém tvaru. Většina síťových administrátorů pojmenovává proxy server[19], kterým přistupuje organizace k Internetu, ve tvaru „gate.jmeno_organizace.cz“. Ukázalo se, že ne jinak je tomu i v případě magistrátu. Magistrát svým zaměstnancům umožňuje přístup k Internetu prostřednictví proxy serveru “gate.mmdecin.cz”. Tuto skutečnost, jsem zjistil pouhým dotazem do vyhledávače Google, který mi na dotaz vrátil hned několik stránek, kde byl ve statistikách přístupu uveden tento řetězec. Je tedy patrné, že proxy server tohoto jména existuje.

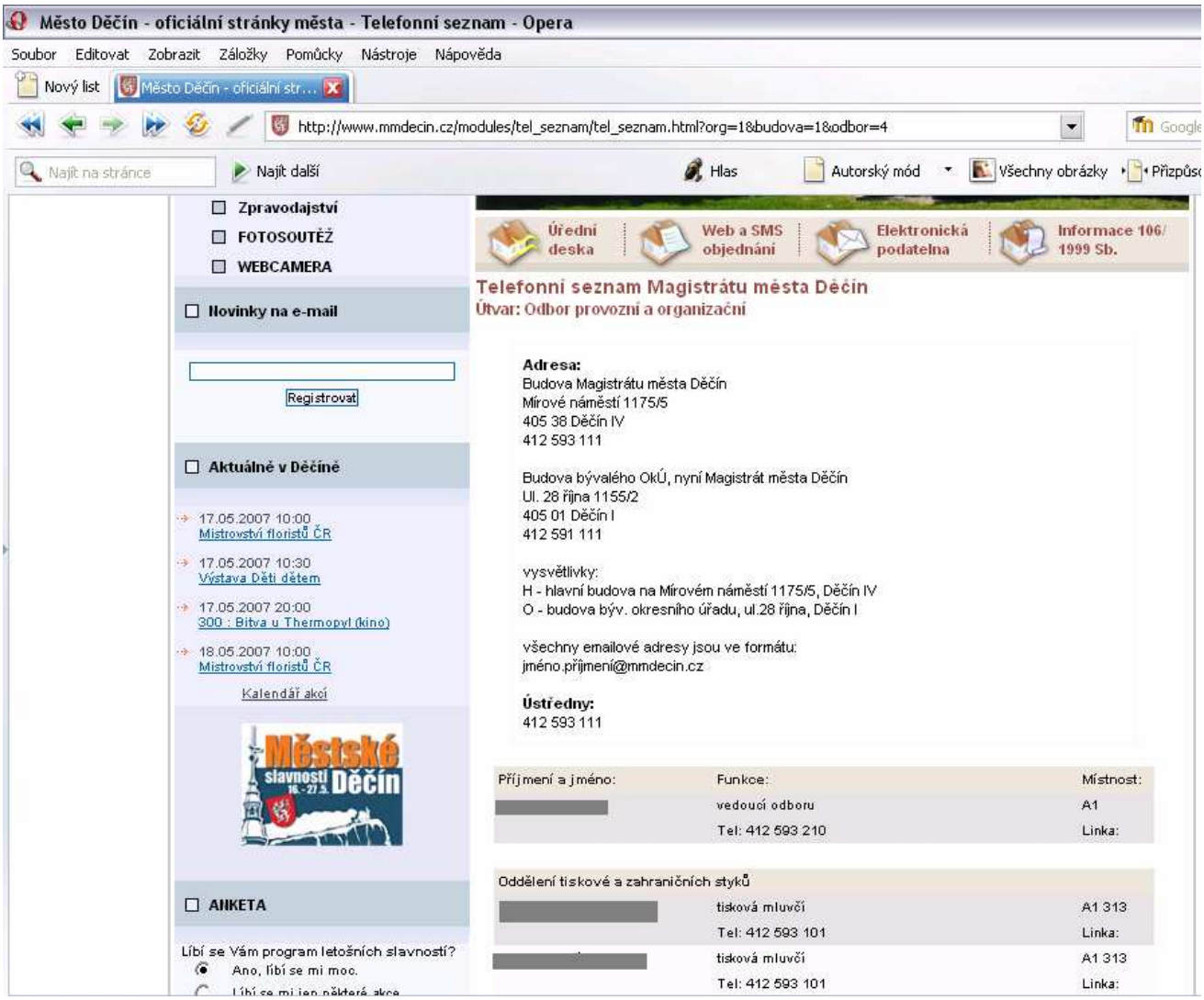
Sliboval jsem si od toho, že naleznu příspěvky zaměstnanců v diskuzích. Jediné co jsem však zjistil a mělo pro mě alespoň určitou hodnotu, bylo to, že jeden ze zaměstnanců se zřejmě ve svém volném pracovním čase věnuje hře Counter-Strike.

5.3.2 Webové stránky instituce

Dalším mým krokem byla analýza webových stránek organizace. Magistrát města Děčína má své webové stránky umístěné na adrese http://www.mmdecin.cz . Tyto stánky jsou bohaté na informace o struktuře magistrátu a také jeho chodu. Na webových stránkách jsem nalezl pro případného útočníka dvě velmi cenné informace.

Tou první je telefonní seznam (obrázek 2). Ten nejenže obsahuje jména a telefonní čísla, ale obsahuje také pracovní zařazení zaměstnance v rámci odborů magistrátu, jeho funkci v rámci odboru a i číslo linky, z níž se dá odvodit, s kým pravděpodobně sdílí kancelář a v jaké se nachází budově.

[19] Proxy server - Funguje jako prostředník mezi klientem a cílovým serverem, překládá klientské požadavky a vůči cílovému serveru vystupuje jako klient. Přijatou odpověď následně odesílá zpět na klienta.



Obrázek 2 Zveřejněný telefonní seznam magistrátu [16]

Druhou informaci, kterou se mi podařilo objevit, je, že magistrát využívá ke svému chodu informační systém RADNICE VERA. Jedná se o poměrně nenápadnou a zdánlivě nezajímavou informaci, která se nachází v jednom odstavci pojednávající o práci odboru tajemníka města. Tato informace se pro mě stala ale velice cennou poté, co jsem navštívil webové stránky tvůrce tohoto informačního systému.

Zde se nachází podrobný popis tohoto systému včetně toho, kdo má jaká práva v tomto systému. Spolu se získaným telefonním seznamem, kde jsou napsány funkce jednotlivých zaměstnanců, lze lehce odvodit, kdo má na magistrátu přístup k mnou požadovaným informacím.

5.3.3 Informační systém RADNICE VERA

Internetové stránky, na kterých tvůrce prezentuje tento informační systém, se nachází na internetové adrese http://www.vera.cz. Popisuje zde zejména technické požadavky nutné k provozu systému a jeho strukturu. Jako reference se zde nachází seznam několika veřejných institucí, které využívají tento systém. Mezi těmito institucemi je uveden také Magistrát města Děčín.

Informační systém RADNICE VERA je rozdělen na čtyři základní skupiny podsystémů (finanční, majetkové, správní, organizační). Z mého pohledu mě zajímala pouze skupina správních podsystémů. V této skupině se nachází 15 podsystémů, z nichž 5 má přístup do registrů obyvatel. Tedy i k mým osobním údajům. Konkrétně se jedná o podsystémy: Matrika, Městská policie, Občanské průkazy a pasy, Ohrožení obyvatelé a Sociální agenda.

Na stránkách je dále popsáno, jaké možnosti poskytují jednotlivé podsystémy a jaká mají přístupová práva ve vztahu k registrům.

5.4 Návrh a příprava útoku

5.4.1 Použité informace

Z popisu informačního systému RADNICE VERA na stránkách jeho tvůrce, lze zjistit, kteří zaměstnanci magistrátu mají přístup do registrů obyvatel. Ve spojení s telefonním seznamem zaměstnanců na webových stránkách magistrátu lze odvodit pak i jejich konkrétní jména, telefonní číslo na jejich pracoviště a na základě čísla vnitřní linky lze také odvodit, s kým pravděpodobně sdílí své pracoviště a v které budově magistrátu se nachází.

Vzhledem k tomu, že většina zaměstnanců majících přístup k registrům obyvatel má pracoviště v jedné budově a jsou zaměstnanci stejného odboru, lze předpokládat, že informace o neúspěšném a odhaleném útoku by si tito zaměstnanci rychle mezi sebou sdělili a při dalším útoku by byli obezřetnější. Proto útok musel být cílenější a musel jsem počítat se všemi možnými variantami, které mohly nastat. Nebylo možné v případě neúspěchu zavěsit telefon a hned se pokusit zmanipulovat jiného zaměstnance. Ten už by totiž byl s největší pravděpodobností o tom, že se někdo pokouší získat citlivé informace tímto způsobem varován.

5.4.2 Samotný návrh útoku

Na základě těchto informací jsem se rozhodl provést pokus o získání mých osobních údajů následujícím způsobem:

Zavolat zaměstnanci majícího na starosti agendu občanských průkazů, jejich výdej, zpracování a představit se jako vedoucí oddělení informatiky. Sdělit mu, že městská policie má problém s připojením k síti, a tak se nemohou dostat do registrů. Před půl hodinou městští strážníci zadrželi dvě podezřelé osoby, které nedokázaly dostatečně prokázat svou totožnost, a bez přístupu do registrů je nemohou ověřit. Než se podaří opět zprovoznit síť, bude to trvat ještě minimálně hodinu. Při tom ho požádat, zda by nemohl pomoci a ověřit jejich totožnost. V případě kladné odpovědi mu sdělit, že mu operační důstojník zavolá během následujících pěti minut.

Po pěti minutách opět zavolat stejnému zaměstnanci a tentokrát se představit jako operační důstojník městské policie. Odvolávat se na předchozí hovor a požádat ho o vyhledání trvalého bydliště dvou osob. První osoba bude smyšlená, tedy o ni nebude žádný záznam v registrech, při druhém dotazu se pak zeptám na své osobní údaje, konkrétně na své trvalé bydliště.

Útok by měl tedy vyznít jako žádost zaměstnance, jenž potřebuje pomoci. Zaměstnanci si mají tendenci pomáhat, protože nikdo neví, zda jednou nebude potřebovat pomoc od svého kolegy a tak každý chce si udržovat na svém pracovišti přátelské vztahy a to zejména mezi lidmi, kteří jsou ve stejném postavení. Proto je velice pravděpodobné, že oslovená osoba žádosti vyhoví.

Aby se oslovená osoba nad otázkami spojené s bezpečností nezamýšlela, musí jí být rychle a jasně sděleno, co se od ní konkrétního očekává. Pak nebude zamýšlet nad konkrétními kroky, které by měla udělat, ale raději přijme to, co ji bude navrženo. Lidé jsou líní přemýšlet nad svými kroky.

V případě, že by se osoba na dlouhou chvíli zamyslela, je nutné ji pak v případné pomlce zahltit velkým množstvím informací. V tomto případě by ji začalo být vysvětlováno, proč policisté si tak nutně potřebují ověřit totožnost pachatele, proč bude tak dlouho trvat, než se obnoví připojení, co vše se musí udělat. Přitom je ale důležité, aby oslovená osoba byla vtažena neustále do rozhovoru, a tak se na tok informací musela soustředit. Proto je třeba rozhovor prokládat větami typu: „Pořád mě někdo někam honí. Znáte to, že?“, „Já vím, že to

je pro vás asi nepříjemné, ale co byste dělala na mém místě vy?“ apod. Oslovená osoba musí být neustále vtažena do rozhovoru a tak nebude mít čas na přemýšlení. Pak se v něm začne ztrácet a raději si nechá sdělit, co by měla udělat.

5.4.3 Kritická místa útoku

Výše navržený postup útoku měl tři kritická místa, v kterých mohl selhat. První byl, zda zaměstnanec bude v době hovoru mít přístup k registrům. Na základě předchozího sběru informací (webové stránky magistrátu, stránky popisující informační systém magistrátu), jsem domníval, že tomu tak bude. Přesto ale jsem nemohl s jistotou říci, že tomu tak bude skutečně. Proto hned na začátku prvního hovoru bylo třeba toto zjistit a v případě negativní odpovědi ukončit hovor s tím, že bylo vytočeno špatné číslo a jméno zaměstnance, když se představoval, bylo přeslechnuto.

Druhým kritickým místem útoku byl druhý hovor. Zaměstnanec nesměl rozpoznat, že mu volá stejná osoba. Proto při druhém hovoru je zapotřebí alespoň částečně změnit styl řeči a hloubku hlasu.

Třetím a zásadním kritickým okamžikem bylo představení se. Zaměstnanec nesměl zjistit, že mu volá jiná osoba než ta, za kterou se volající vydával. Proto bylo třeba zjistit, jaké vztahy mezi zaměstnanci panují na magistrátu. Na základě toho jsem pak mohl rozhodnout, jakým způsobem měl hovor probíhat, zda se měl vést v přátelském tónu, zda se mělo zaměstnanci tykat nebo vykat apod.

5.4.4 Zjištění charakteru zaměstnaneckých vztahů

Cílem následujících telefonních hovorů bylo zjistit, nakolik zaměstnanci odboru správních agend znají zaměstnance oddělení informatiky. Zda mají ponětí o jejich jménech a funkcí.

Celkem jsem provedl tři rozhovory v průběhu jednoho týdne. Pokaždé jsem se představoval jako zaměstnanec některé z děčínských firem a požadoval jsem k telefonu jednoho ze zaměstnanců magistrátu majícího na starosti informační systémy, přičemž jsem se dovolal na odbor správních agend. Pokaždé jsem předstíral, že jsem se dovolal na špatné číslo. Sdělil jsem vždy pouze jméno zaměstnance, žádnou jeho funkci. Dále jsem se zeptal, zda by mi mohl ještě sdělit, kde ho najdu.

Všechny hovory skončily s téměř stejným výsledkem. Osoba, která zvedla telefon, mi po krátkém zamyšlení sdělila, kde hledanou osobu najdu. Pak mě ihned přepojila na správnou telefonní linku. V tuto chvíli jsem telefon zavěsil. To vše dělala oslovená osoba rychle a bez rozmýšlení. Bylo tedy patrné, že měla přehled o jednotlivých zaměstnancích oddělení informatiky a věděla, jaké jsou jejich funkce.

Níže uvádím průběh jednoho z rozhovorů. Podotýkám, že níže uvedená jména jsou smýšlená.

> ***Zaměstnankyně správního odboru:*** *"Dobrý den, zde paní Jiřina Novotná, oddělení podpory pro nezaměstnané, jak vám mohu pomoci?"*
>
> ***Já:*** *"Dobrý den zde Jiří Stejskal ze společnosti DC FreeNet, mohl bych mluvit s panem Petrem Svobodou? Nejsem si jistý, zda jsem se dovolal na správné telefonní číslo."*
>
> ***Zaměstnankyně správního odboru:*** *(ihned pohotově odpovídá) "To máte špatné telefonní číslo. Pan Svoboda zde není. Ten je v jiné budově.. Já se vás pokusím přepojit."*
>
> ***Já:*** *"Aha... To by jste byla moc hodná, děkuji." (přepojuje mě a když telefon začne vyzvánět zavěšuji).*

Na základě těchto rozhovorů se dalo tedy usoudit, že zaměstnanci se znají. To mohlo útok usnadnit tím způsobem, že nebude muset být vysvětlováno, jakou funkci má osoba, za kterou se jsem já jako útočník chtěl vydávat. Úzké přátelské vztahy mohou také způsobit, že oslovený zaměstnanec mohl brát požadavek o spolupráci jako přátelskou prosbu, a tím spíše by žádosti vyhověl. Na druhou stranu vzhledem k tomu, že zaměstnanci přichází spolu zřejmě do styku, mohl oslovený zaměstnanec rozpoznat, že hlas v telefonu nepatří osobě, za kterou se útočník bude vydávat. Jednou z možností, jak tento problém překonat, je že útočník bude předstírat, že je nastydlý.

Co se týče způsobu vyjadřování a stylu řeči vzhledem k tomu, že se zaměstnanci znají a zřejmě spolu běžně hovoří, útok by měl vypadat jako rutinní hovor. Tedy se musí říct jasně a rychle, co po zaměstnanci se žádá a to bez zbytečného vysvětlování. Velkým otazníkem ale je, zda si zaměstnanci tykají, vykají apod. Proto je vhodnější volit takové věty, z kterých není

patrné, zda se oslovené osobě vyká nebo tyká a pak teprve následně přizpůsobit způsob vyjadřování na základě několika odpovědí oslovené osoby.

5.5 Samotný útok

Na základě výše zjištěných informací a návrhu útoku jsem provedl samotný útok, který se skládal ze dvou telefonních hovorů. Níže uvádím jejich průběh. Neuvádím v nich ale skutečná jména osob, kterých se hovor týkal a ani správnou skutečnou funkci zaměstnanců, jež jsem oslovil.

5.5.1 První hovor

Zaměstnanec: *„Dobrý den, zde Jitka Nováková agenda ****[20].“

Útočník (nastydlým hlasem a rychlou mluvou)*: „ Dobrej, tady Libor Holý. Jdou vám registry?“*

Zaměstnanec: *„ No.. Já..“*

Útočník*: „ Můžete se k nim připojit?“*

Zaměstnanec: *„Já se podívám... Tak už to nabíhá. Připojuji se. Jo, ano jdou.“*

Útočník (zakašle před tím do telefonu): *„Víte, my tu máme s tím problém. Městské policii nejde net a nemohou se tak připojit do registru a chtěl bych se zeptat..“*

Zaměstnanec*: „Počkejte, to já řešit nemůžu tohle. Já vám někoho tady předám.“*

Nadřízená: *„Ano?“*

Útočník (opět zakašle): *„Dobrej, tady Libor Holý. Tu máme problém s registry. Městská policie se k nim nemůže připojit a než to tu vyřešíme tak to nějakou hodinu potrvá. Díky tomu si nemůžou ověřit totožnost pachatel a tak. Takže se chci zeptat, zda bych jim mohl říct ať vám zavolají a že by jste se podívali do registrů a řekli jim, co potřebují. Bude asi stačit jen adresa, věk.*

20 Jméno agendy z výše popsaných důvodů neuvádím.

Oni právě teď zadrželi nějaké dvě osoby, ale nemůžou si je ověřit. Bylo by to možné?“

Nadřízená: *„Jo… V tom nevidím problém Libore. To by šlo.“*

Útočník: *„Tak to je skvělé. Takže já jim to řeknu a oni vám tak za pět minut zavolají.“*

Nadřízená: *„ Dobře.“*

Útočník: *„Tak zatím.“*

5.5.2 Druhý hovor o 5min později

Zaměstnanec: *„Jitka Nováková, agenda ****[21].“*

Útočník (pomalým hlasem)*: „ Dobrý den, tady je operační dispečer Městské policie Děčín. Nám řekli, že vám máme zavolat kvůli těm registrům.“*

Zaměstnanec: *„ Co? Prosím? Já o ničem nevím... Kdo vám to řekl? “*

Útočník*: „ Máme tu problém s registry. Nemůžeme se k nim připojit, tak jsem volal panu Liboru Holému, že potřebujeme nutně si ověřit totožnost dvou osob a on mi před chvílí zavolal zpět, že mám zavolat na tohle číslo, že mi pomůžete, že to u vás domluvil.“*

Zaměstnanec: *„Co prosím? Kdo je Libor Holý?“*

Útočník: *„ Libor Holý je vedoucí oddělení informatiky na magistrátu. Říkal mi, že s vámi hovořil asi před 5 minutami.“*

Na pozadí je slyšet do telefonu tento rozhovor:

Nadřízená: *„ Nejsou to policajti?“*

Zaměstnanec: *„Jo jsou. Ale vůbec nevím, co po mě chtějí.“*

Nadřízená: *„ Počkej já si to vemu.“*

Telefon si přebírá opět nadřízená:

---

21 Jméno agendy z výše popsaných důvodů neuvádím.

***Útočník**: „Dobrý den, zde dispečer městské policie. Vám volám ohledně toho, že nám nejdou registry a potřebujeme si ověřit totožnost dvou osob. Řekli mi, že vám mám zavolat na tohle číslo, že mi pomůžete.“*

***Nadřízená:** „Ano, vím. Můžete mi říct rodné číslo?“*

***Útočník**: „Bohužel mohu vám říct jen jméno. Ukázal nám jen nějakou kartičku, kde je fotka a jeho jméno. Rodné číslo nevím. Měl by se jmenovat Petr Sotona a bydliště by měl mít v Děčíně.“*

***Nadřízená:** „Dobře. A věk? Je mu kolem čtyřiceti?“*

***Útočník**: „Vypadá prý mezi 20-25.“*

***Nadřízená:** „ Jo mám ho. To asi bude on. Podmokly 28, Děčín 3.“*

***Útočník**: „Počkejte. Já si to musím napsat. Můžete to zopakovat?“*

***Nadřízená:** „ Jo, jo. Podmokly 28, Děčín 3.“*

***Útočník**: „ Děkuju. Mám to. Moc jste nám pomohla.“*

***Nadřízená:** „ A na tu druhou osobu se nebudete ptát?“*

***Útočník**: „ Ehhm... Ne, to už nepotřebujeme. Potřebujeme si ověřit jen tohodle. Ještě jednou děkuji a na shledanou.“*
***Nadřízená:** „Na shledanou.“*

5.5.3 Rozbor útoku

Klíčový pro tento útok byl první hovor. Hned na začátku jsem se nepřímo zeptal, zda oslovený zaměstnanec má přístup k registrům. Jak je vidět z rozhovoru, tato otázka vyvedla zaměstnance z míry a začal mít obavy, že se něco komplikuje. Jakmile ještě uslyšel slovo „problém“ a v hovoru náznak toho, že bude následovat žádost o pomoc, předal telefon své nadřízené, aby se vyhnul nutnosti případnou žádost řešit.

Překvapivé je, že během druhého hovoru tento zaměstnanec, jak se pak ukázalo, nevěděl, jakou funkci má osoba v rámci magistrátu, za kterou jsem se vydával. To bylo pro mě překvapením, protože předchozí hovory prokázaly, že zaměstnanci mají povědomí o osobách na oddělení magistrátu. Kupodivu přesto všechno považoval volajícího za někoho, kdo má co do činění s informačním oddělením a byl ochoten odpovídat na pokládané otázky i

když si nebyl zcela jistý, s kým vlastně hovoří. Výraznou roli, zde hrál ten fakt, že zaměstnanec byl zaskočen tím, jak rychle byla otázka položena a i to, že osoba na druhém konci telefonu mluvila sebevědomě a věděla, že zaměstnanec má na svém pracovišti přístup k registrům.

Nadřízená osoba, jež pak převzala telefon si samozřejmě uvědomovala, že mé osobní údaje jsou důvěrné a neměly by být sdělovány žádné třetí osobě. Za normálních okolností by si nedovolila do telefonu prozradit někomu takové údaje. Ale volajícího v prvním hovoru považovala za svého kolegu, který ji požádal o laskavost a kterého osobně zná, a protože zaměstnanci, jež mají stejné postavení v organizaci, si mají tendenci pomáhat, s prosbou souhlasila.

Jak je patrno z prvního rozhovoru v jednu chvíli nadřízená mi začala tykat a oslovovala mě i křestním jménem osoby, za kterou jsem se vydával.

Důvodů, proč mě považovala za osobu, za kterou jsem se vydával, může být několik:

- Pravděpodobnost útoku touto formou považovala za velice nízkou.
- Osoba na druhém konci telefonu, znala organizační strukturu magistrátu a věděla na koho se obrátit, tedy to nejspíš musela být osoba pracující na magistrátu.
- Osoba používala hovorovou češtinu, která je běžná při komunikaci mezi zaměstnanci při neformálních hovorech.
- Osoba jasně, pohotově a bez jakéhokoliv rozmýšlení sdělovala, co chce. Oslovená osoba tak neměla čas dlouze uvažovat o pochybnostech.
- Osoba byla nachlazená, a tak nemohla rozpoznat, zda hovoří s jinou osobou.

Během druhého hovoru se mi podařilo získat mé osobní údaje, i když nastaly určité komplikace, kdy nadřízená nesdělila zaměstnanci, na jehož pracoviště jsem volal, že se zavázala pomoct s identifikací pachatele na základě vyhledání jeho osobních údajů v registrech. Nadřízená ale tento hovor očekávala a tak se hovoru ujala. Pak už bylo jisté, že operačnímu důstojníkovi pomůže s identifikací pachatele, protože by jinak vypadala nedůvěryhodně v očích svého kolegy, vedoucího oddělení informatiky, kterému se zavázala pomoci s vyřešením problému, což by mělo zcela jistě vliv na přátelské vztahy mezi nimi.

5.6 Návrh vedoucí ke zvýšení odolnosti informačního systému

5.6.1 Zjištěné nedostatky

V případě magistrátu jsem odhalil několik faktorů usnadňující útok sociotechnickou metodou:

- ➔ Informace o tom, kde se jednotliví zaměstnanci nacházejí, jsou volně dostupné komukoliv prostřednictvím Internetu.
- ➔ Organizační struktura magistrátu je zveřejněna na Internetových stránkách.
- ➔ Telefonní čísla na zaměstnance informatiky a ostatních zaměstnanců, u nichž není zapotřebí, aby je veřejnost znala, jsou dostupné komukoliv.
- ➔ Nejsou uplatňovány bezpečnostní procedury při sdělování citlivých informací.
- ➔ Prostřednictvím stránek tvůrce informačního systému Radnice Vera a telefonního seznamu, lze odvodit, kdo má jaká práva v informačním systému magistrátu.

5.6.2 Zveřejňování informací o organizační struktuře

První dva faktory vyplývají z charakteru testovaného subjektu. Vzhledem k tomu, že se jedná o veřejnou instituci, jejíž činnost je zajišťována z veřejných prostředků a podílí se na výkonu veřejné správy, měla by být kontrolovatelná veřejností. V současnosti je snahou chod veřejných institucí zprůhlednit. Dnes občané mají právo vědět, kdo rozhoduje v otázce, která se jich týká, a na koho konkrétně se mají obracet s určitou žádostí. Proto i Magistrát města Děčín, stejně tak jako ostatní veřejné instituce vykonávající veřejnou správu, má dnes na svých webových stránkách zveřejněn telefonní seznam zaměstnanců, jež se podílí určitým způsobem na výkonu správy. Krom toho je zveřejněna i organizační struktura instituce.

Toto je sice vhodné pro dobrou kontrolu chodu veřejné instituce, ale už to není nejlepší řešení z pohledu bezpečnosti informací, kdy útočník může snadno získat přehled o jménech jednotlivých zaměstnancích, jejich funkcích a jejich postavení v hierarchii organizace. Toto je typický příklad, kdy dochází k rozporu mezi různými požadavky v rámci organizace, tedy požadavkem na zajištění bezpečnosti informačního systému a požadavkem na otevřenost instituce směrem k veřejnosti. Pokud se rozhodne organizace, že telefonní seznam a organizační struktura musí být zveřejněna, je pak třeba počítat s tím, že případní

útočníci budou mít tyto informace k dispozici a tomu by měla odpovídat bezpečnostní opatření magistrátu.

Nicméně je zbytečné, aby na webových stránkách magistrátu byl telefonní seznam obsahující jména zaměstnanců oddělení informatiky. Zaměstnanci informatiky nemají žádný vztah k výkonu veřejné správy. Jejich náplní je pouze zajišťovat bezproblémový provoz informačních systémů. Není tedy důvod k tomu, aby veřejnost znala jejich jména. Zbytečné také je, aby v telefonním seznamu bylo uvedeno i číslo vnitřní linky. Dle čísla vnitřní linky se dá lehce odhadnout, s kým daný zaměstnanec sdílí své pracoviště a kteří zaměstnanci se důvěrně znají.

Proto z výše popsaných důvodů by bylo vhodné ze zveřejněného telefonního seznamu odstranit jména zaměstnanců oddělení informatiky a místo toho, by v seznamu bylo uvedeno pouze jedno telefonní číslo, které by zastupovalo celé oddělení informatiky. Na tomto telefonním čísle by byl zaměstnanec odpovědný za vyřizování hovorů zvenčí. Zároveň bych z veřejného telefonního seznamu odstranil čísla vnitřních linek.

Zvážit by se mělo, zda zmínka o tom, že magistrát využívá při své činnosti informační systém Radnice Vera je natolik podstatná pro veřejnost, že musí být zveřejněna na webových stránkách magistrátu. Nicméně odstraněním této informace se nic de facto neřeší, protože tato informace se nachází také na stránkách tvůrce tohoto systému, kde jsou jako reference uvedeny veřejné instituce využívající informační systém Radnice Vera. Proto by v případě rozhodnutí, že tato informace musí být odstraněna z webových stránek úřadu, musel být kontaktován i tvůrce systému s žádostí, aby ani on tuto informaci nezveřejňoval.

5.6.3 Zavedení bezpečnostních procedur

To, že telefonní seznam organizace je volně přístupen komukoliv, neznamená automaticky, že nejsou dodržovány zásady bezpečnosti. V bezpečnostní politice magistrátu se na tuto skutečnost musí ale pamatovat a nesmí se podceňovat, že de facto každý útočník bude znát jména zaměstnanců, organizační strukturu a telefonní čísla. Proto tedy, když někdo bude tyto informace znát, neznamená to automaticky, že je zaměstnancem magistrátu a zaměstnanci pracující s citlivými údaji si musí být toho vědomi.

O to více musí být zavedeny bezpečnostní procedury provázející manipulaci s citlivými informacemi. Musí být sestaven postup, jakým způsobem si budou zaměstnanci

ověřovat totožnost volajícího a také to jakým způsobem si budou ověřovat, zda volající má vůbec právo tuto informaci požadovat. Tyto postupy by pak měly být zařazeny mezi směrnice pro příslušná pracoviště, kde dochází ke zpracování citlivých informací. A jejich naplňování by se mělo periodicky neustále kontrolovat. Také by měla být ustanovena zodpovědnost na jednotlivých odborech a v organizaci jako celku, kdo bude ručit za to, že jsou tyto bezpečnostní procedury naplňovány při každodenní činnosti organizace. Na takto pověřenou osobu by zaměstnanci směřovali případné dotazy, kdyby si nebyli jisti správností svého postupu.

5.6.4 Shrnutí navrhovaných změn

Mnou navrhované změny ve stručnosti tedy jsou:

- ➔ Odstranění telefonních čísel na zaměstnance informatiky z veřejně dostupného telefonního seznamu.
- ➔ Odstranění čísel vnitřních linek z telefonního seznamu.
- ➔ Vypracování bezpečnostních procedur pro sdělování citlivých informací.
- ➔ Neustále kontrolovat, zda jsou bezpečnostní procedury uplatňovány.
- ➔ Ustanovení odpovědnosti konkrétním zaměstnancům, kteří budou ručit za uplatňování těchto procedur.

Všechny tyto návrhy byly předány spolu s popisem průběhu testování Magistrátu města Děčín. Zaměstnanec, s kterým, jsem při testování spolupracoval, mi sdělil, že testování prokázalo, že jejich informační systém nebyl dostatečně v tomto směru zabezpečen.

Každý zaměstnanec, který vykonává na magistrátu činnost spojenou se zpracováním osobních údajů, je seznámen s tím, že nesmí sdělovat citlivé údaje třetí osobě. Tato povinnost také vyplývá ze Zákona o ochraně osobních údajů. Nicméně bezpečnostní politika na magistrátu není vypracována do takové míry, aby v případě útoku takovéhoto typu, byl systém zabezpečen. Napadení systému touto formou útoku bylo na magistrátu považováno jako velice nepravděpodobné a v ochraně systému proti této formě útoku se spoléhalo na fakt, že všichni zaměstnanci na magistrátu zpracovávající citlivé údaje se znají a tak dokáží rozeznat, kdo jim volá. Mnou provedené testování ale prokázalo, že spoléhat se pouze na tento fakt je mylné. Magistrátem zveřejněné informace jsou dostatečné k tomu, aby

umožnily případnému útočníkovi oklamat obsluhu systému. Testování krom tohoto zjištění ověřilo také to, že metody sociálního inženýrství zejm. ty zaměřené na přímou manipulaci obsluhy, jsou pro případného útočníka použitelné k získání citlivých informací a jsou v oblasti ochrany informací podceňovány.

Závěr

Téma lidský faktor v oblasti bezpečnosti informačních systémů je poměrně rozsáhlé a tomu také odpovídá rozsah této práce. Cílem bakalářské práce bylo popsat základní hrozby, kterým informační systém organizace musí čelit a které vyplývají z lidského faktoru, a základní možnosti, jak rizika těchto hrozeb minimalizovat na přijatelnou úroveň.

Tento cíl byl splněn, i když vzhledem k omezenému rozsahu práce nebylo možné popsat všechny aspekty bezpečnosti informačního systému a i všechny možnosti, jak systém dostatečně zabezpečit.

Krom toho, bylo popsáno několik případů, kdy došlo vlivem lidského faktoru k narušení bezpečnosti informačního systému, a byl testován informační systém Magistrátu města Děčín z pohledu odolnosti proti metodám sociálního inženýrství. Jak jednotlivě popsané příklady úniku informací, tak i samotné testování magistrátu prokázalo tvrzení, že v současné době je bezpečnost informačního systému z hlediska lidského faktoru podceňována a nevěnuje se ji dostatečná pozornost.

Podceňování této problematiky je ale přitom v současné době nepřijatelné a vzhledem k rostoucím tendencím útočníků využívat lidský faktor jako nejslabší článek zabezpečení informačního systému se očekává, že takových útoků bude přibývat a zejména organizace zpracovávající citlivé informace by měly být na tyto formy útoku připraveny. Vzhledem k tomu, že většina organizací zpracovávající citlivé informace jsou veřejné instituce, stálo by za zvážení, zda by stát se neměl v této problematice více angažovat a provést takovou systémovou změnu, která by tyto instituce výrazněji přinutila přijmout odpovídající bezpečnostní opatření.

Ani v případě samotných fyzických osob není povědomí o hrozbách dostatečné. Tento fakt umožňuje snadné šíření virů a další negativní jevy jako rostoucí nedůvěra k bezpečnosti na Internetu. Mnoho kurzů či knih věnujících se základům práce s počítačem naprosto opomíjí zmínit pravidla, kterými by se měl internetový uživatel řídit, aby tak neohrozil své citlivé údaje či finanční prostředky spravované prostřednictvím internetového bankovnictví. I zde by stálo za zvážení, zda by neměla být spuštěna kampaň upozorňující na tuto problematiku ve veřejnoprávních médií. Také média by mohla častěji upozorňovat na aktuální hrozby v podobě nových rychle se šířících virů apod. Mnou provedené testování magistrátu

odhalilo, že systém magistrátu byl nedostatečně zabezpečen a nebyl odolný proti útokům využívajících metod sociálního inženýrství. Toto zjištění, přinutilo magistrát k přehodnocení své bezpečnostní politiky a nápravě nedostatků a to zejména v oblasti sdělování citlivých informací.

Použitá literatura

[1] BRABEC, František, et al. Bezpečnost pro firmu, úřad, občana. 2001. vyd. Praha : Public History, 2001. 400 s. ISBN 80-86445-04-06.

[2] MITNICK, Kevin, SIMON, William. Umění klamu. Gliwice, POLSKO : Helion S.A., 2003. 348 s. ISBN 83-7361-210-6.

[3] ALLEN, Malcom. Social Engineering : A means to violate a computer system. [s.l.], 2006. 13 s. Sans Institute. Certifikační práce. Dostupný z WWW: <www.sans.org/reading_room/whitepapers/engineering/529.php>

[4] BERG, Al. Spear phishing : Don't be a target. SearchSecurity.com [online]. 2004 [cit. 2006-10-20]. Dostupný z WWW: <http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci1171131,00.html>.

[5] Cyber Criminals Haven't Retired - They've Just Gone Phishing!. Laptopical [online]. 2007 [cit. 2007-05-20]. Dostupný z WWW: <http://www.laptopical.com/wi-phishing.html>.

[6] DOBDA, Luboš. Ochrana dat v informačních systémech. 1. vyd. Praha : Grada Publishing, 1998. 288 s. ISBN 80-7169-479-7.

[7] Český normalizační institut [online]. 2007 [cit. 2007-02-20]. Dostupný z WWW: <www.cni.cz>.

[8] Phishing zasáhl CitiBank. Antivirové centrum [online]. 2006 [cit. 2006-11-10]. Dostupný z WWW: <http://www.antivirovecentrum.cz/clanky/phishing-zasahl-citibank.aspx>.

[9] Američané přišli o notebook s daty o 2,2 miliónu aktivních vojáků. Novinky.cz [online]. 2006, roč. 2006 [cit. 2006-08-07]. Dostupný z WWW: <http://www.novinky.cz/internet/americane-prisli-o-notebook-s-daty-o-2-2-milionu-aktivnich-vojaku_87499_d2ukb.html>.

[10] Američanům opět unikla data, postiženo 100 000 námořníků. Novinky.cz [online]. 2006 [cit. 2006-07-11]. Dostupný z WWW: <www.novinky.cz/internet/americanum-opet-unikla-data--postizeno-100-000-namorniku_90115_sa6b7.html>.

[11] Osobní údaje klientů spořitelny byly v kontejneru. Novinky.cz [online]. 2006 [cit. 2006-11-20]. Dostupný z WWW: <http://www.novinky.cz/krimi/Novinky_Osobní_údaje_klientů_spořitelny_byly_v_kontejneru.html>

[12] Jak se zbavit viru Win32/Stration, Win32/Warezov. Antivirové centrum [online]. 2007 [cit. 2007-03-10]. Dostupný z WWW: <http://www.antivirovecentrum.cz/potrebuji-poradit/jak-se-zbavit-win32-stration-win32-warezov.aspx>.

[13] AOL engineer sold 92 million screen names to spammer. Security Crawler [online]. 2004 [cit. 2006-08-10]. Dostupný z WWW: <http://www.securitycrawler.com/2004/06>.

[14] DOLAN,Aaron. Social Engineering.[s.l.], 2006. 16 s. Sans Institute. Certifikační práce. Dostupný z WWW: <http:/www.sans.org/reading_room/whitepapers/engineering/1365.php>

[15] FITE, Bryan. Corporate Identity Fraud: Life Cycle Managment of Corporate Assets. [s.l.], 2006. 21 s.Sans Institute. Certifikační práce. Dostupný z WWW: <http://www.sans.org/reading_room/whitepapers/engineering/1650.php>

[16] Magistrát města Děčín [online]. 2007 [cit. 2006-11-20]. Dostupný z WWW: <www.mmdecin.cz>.

Seznam příloh

Příloha č. 1 – Dotaz na Úřad pro ochranu osobních údajů ohledně legality testování

Dobrý den,

chtěl bych se vás dotázat, zda je možné testovat instituci na odolnost proti úniku informací. V rámci bakalářské práce bych se chtěl pokusit zneužít osoby v instituci, aby mi vyzradily citlivé informace, konkrétně osobni údaje. Problém je, že v případě osobních údajů je to nezákonné. Proto bych se chtěl zeptat, zda informace týkající se mé osoby nebo osoby, která mi dala souhlas, abych měl přístup k jejím osobním údajům, mohu vylákat po zaměstnancích instituce a nepřekročím zákon.

Dle Trestního zákonu je trestné získání informací tím způsobem, že je vylákám, získám od někoho bez jeho souhlasu pouze jen tehdy, když jsem subjektu způsobil určitou újmu nebo když jsem je získal v zlém úmyslu. Pokud tedy získám informace čistě jen proto, abych zjistil, zda je subjekt, instituce odolná proti úniku informací a následně takto získané informace nezneužiji, nebudu je dále šířit apod. tak se protizákonného jednání nedopustím

Jde pouze o zjištění, zda je systém instituce odolný proti úniku informací. Po přečtení Zákonu o ochraně osobních údajů a Trestního zákonu jsem nabyl dojmu, že získání informací tímto způsobem je legální. Nejsem si ale naprosto jistý a tak se obracím na vás s prosbou o bližší objasnění problematiky.

S pozdravem
Petr Sotona, student Univerzity Pardubice

Příloha č. 2 – Stanovisko Úřadu pro ochranu osobních údajů k legalitě testování

Vážený pane,

k Vašemu dotazu Vám sdělujeme, že pokud budete mít k získání osobních údajů uvedeným způsobem předem udělený prokazatelný souhlas všech subjektů údajů, jejichž údaje tímto způsobem shromáždíte, zákon č.101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „zákon o ochraně osobních údajů“) neporušíte. Povinnost podle § 5 odst. 1 písm. g) zákona o ochraně osobních údajů, „shromažďovat osobní údaje pouze otevřeně, je vyloučeno shromažďovat údaje pod záminkou jiného účelu nebo jiné činnosti“, je povinností správce ve vztahu k subjektu údajů. Jestliže tedy subjekt údajů dá předem informovaný souhlas, ve smyslu § 5 odst. 4, k Vámi stanovenému účelu shromažďování, ani tato povinnost nebude porušena.

V uvedeném případě však z Vaší strany půjde o zpracování osobních údajů podléhající režimu zákona o ochraně osobních údajů s povinnostmi stanovenými tímto zákonem, protože nejde ve smyslu § 3 odst. 3 o zpracování pro osobní potřebu, ale pro potřeby školní seminární práce. Správcem, který za zpracování odpovídá, je v tomto případě ten, kdo stanovil účel zpracování, tedy buď Vy sám nebo škola. Plnit je třeba povinnosti stanovené ve vztahu k účelu zpracování podle § 5 odst. 1, povinnost podle § 5 odst. 2 (souhlas subjektu údajů), povinnosti při zabezpečení údajů podle § 13 – § 15 a splnit je třeba oznamovací povinnost podle § 16, protože v uvedeném případě nelze aplikovat žádnou z výjimek podle § 18. Informační povinnost podle § 11 odst. 1 není třeba plnit ve smyslu výjimky podle § 11 odst. 3 písm. d), protože jde o údaje, které nejsou získány od subjektu údajů, avšak se souhlasem subjektu údajů.

Získání osobních údajů za tímto účelem s předem uděleným souhlasem subjektů údajů by zřejmě nebylo možné posoudit ani jako trestný čin neoprávněného přisvojení si osobních údajů o jiném shromážděných v souvislosti s výkonem veřejné správy, podle § 178 trestního řádu. K posuzování skutečnosti, zda byl spáchán trestný čin, jsou však příslušné orgány činné v trestním řízení.

S pozdravem

JUDr. Zdeněk Koudelka v.r., ředitel odboru stížností a konzultací

ÚDAJE PRO KNIHOVNICKOU DATABÁZI

Název práce	Lidský faktor v oblasti bezpečnosti informačních systémů
Autor práce	Petr Sotona
Obor	Informatika ve veřejné správě
Rok obhajoby	2007
Vedoucí práce	Ing. Milan Tomeš
Anotace	Práce popisuje problematiku lidského faktoru v oblasti zabezpečení informačního systému. Jsou zde popsány metody útoků využívající lidský faktor k narušení bezpečnosti a i způsoby, jak tyto hrozby odvracet. Součástí práce je také testování informačního systému Magistrátu města Děčín z pohledu odolnosti proti metodám sociálního inženýrství.
Klíčová slova	Lidský faktor, zabezpečení systému, sociální inženýrství, phishing, režimová bezpečnost