LIDSKÝ FAKTOR V BEZPEČNOSTI IINFORMAČNÍCH SYSTÉMŮ

Milan Tomeš, Petr Sotona
Univerzita Pardubice, Fakulta ekonomicko-správní, Ústav systémového inženýrství a informatiky

Abstract: *Práce je zaměřena na rozbor problematiky lidského faktoru v oblasti bezpečnosti informačních systémů. V práci je popsáno testování konkrétního informačního systému magistrátu města z pohledu odolnosti proti metodám sociálního inženýrství.*

Key words: *Lidský faktor, zabezpečení systému, sociální inženýrství, bezpečnost*

Úvod

Nasazení informačních systémů a technologií se stalo v současnosti nutnou podmínkou úspěšnosti mnoha organizací. Bez nich je dnes práce neefektivní a mnohdy dokonce nepředstavitelná. Spolu s rozvojem informačních technologií a jejich vzrůstajícímu nasazení ve všech oblastech společnosti výrazně také vzrostly možnosti jejich zneužití. Konkurenční boj na jakékoliv úrovni podnikání přinesl fakt, že informace jsou zbožím, jejichž cena může mít nemalou hodnotu, a proto i v této oblasti dochází k rozvoji kriminality.

Je známé, že systém je tak silný, jako jeho nejslabší článek a protože se ukazuje, že technické zabezpečení systémů je dnes již tak komplikované a účinné, snaží se útočníci toto zabezpečení alespoň částečně obejít oklamáním člověka v pozici obsluhy systému, tedy prostřednictvím lidského faktoru. V současnosti roste počet těchto útoků, a proto je třeba se na ně zaměřit a související jevy studovat. Člověk jako součást bezpečnosti informačního systému je bohužel nejen často podceňován, ale dokonce u některých organizací zcela opomíjen. Přitom paradoxně útoky na informační systém, v nichž figuruje lidský faktor, jsou v současnosti charakteristické vysokou úspěšností.

Ústředním tématem této práce je analyzovat bezpečnost systému z pohledu jeho obsluhy, tedy člověka a to na konkrétním příkladu.

Je zde podrobně popsán průběh testování informačního systému Magistrátu vybraného města v oblasti bezpečnosti zpracovávaných osobních údajů, proti němuž byly použity metody sociálního inženýrství. Úkolem tohoto testování, bylo zjistit, do jaké míry jsou osobní údaje zabezpečeny a navrhnout pak případná opatření, aby byla jejich bezpečnost zvýšena.

Cíl testování

Cílem testování bylo zjistit odolnost informačního systému z pohledu lidského faktoru, vedlejším cílem pak získání citlivých informací. V případě, že systém by nebyl dostatečně zabezpečen, pak navrhnout takové změny, aby tomu tak bylo.

K dosažení tohoto cíle byl proveden útok na IS s použitím metod sociálního inženýrství.

Předmětem útoku, jehož bezpečnost byla testována, byly zvoleny osobní údaje (rodné číslo, adresa atd.) jednoho z autorů práce, tedy byl učiněn pokus získat své vlastní osobní údaje neoprávněnou cestou.

Vzhledem k citlivosti informací i celého testování, byl nejdříve požádán o spolupráci a svolení představitel subjektu, jehož informační systém měl být testován, s tím, že získané výsledky budou zpracovány ve formě návrhů ke zvýšení odolnosti jeho informačního systému v tomto směru.

Jako subjekt, jenž byl vybrán pro testování odolnosti informačního systému proti úniku informací, byl zvolen Magistrát města, jehož je autor článku občanem. Tento magistrát souhlasil a pověřil zaměstnance oddělení informatiky, aby testování průběžně konzultovali.

Právní otázky

Při testování odolnosti informačního systému byl samozřejmě brán zřetel na dodržování právních norem České republiky. Nejproblematičtější se jevil Zákon o ochranně osobních údajů č. 101/2000 Sb, ale vzhledem k tomu, že cílem bylo získat své vlastní údaje, tento zákon porušen nebyl. Stejně tak dle Trestního zákona č.140/1961 Sb nebyla naplněna skutková podstata žádného trestného činu, neboť zde není úmysl, že by se kdokoliv chtěl tímto způsobem obohatit nebo někoho poškodit. Právní otázky byly konzultovány s Úřadem pro ochranu osobních údajů, jehož stanovisko bylo takové, že navržené testování neporušuje právní normy České republiky.

Vzhledem k citlivosti veřejnosti v otázce zabezpečení osobních údajů, po konzultaci s vedoucím oddělením informatiky Magistrátu města bylo dohodnuto, že proti magistrátu nebudou učiněny žádné kroky, které by ho mohly jakkoliv poškodit. Z tohoto důvodu není v práci uvedeno konkrétní město, ani žádná skutečná jména osob, které byly útokem dotčeni. Konkrétní město je nahrazeno obecným termínem „město“, rozhovory jsou zde zaznamenány tak, jak se udály, pouze jména osob jsou fiktivní.

Sběr informací

Před samotným útokem bylo třeba získat o chodu instituce dostatek informací. Největším zdrojem byly webové stránky magistrátu. Některé informace pak byly zjišťovány pomocí několika krátkých nenápadných telefonátů. Také bylo využito vyhledávání informací pomocí běžného internetového vyhledávače Google.

Použití internetového vyhledávače Google

Prvním krokem byl pokus vyhledat stránky nebo dokumenty obsahující řetězec “@mmmesto.cz” nebo “@mumesto.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.

Žádná informace nalezená tímto dotazem však nebyla nikterak výrazně cenná. Jediné, co se podařilo zjistit, bylo, že jeden ze zaměstnanců oddělení informatiky úspěšně kandidoval na místo do obecního zastupitelstva své obce (tedy získána informace o místě jeho bydliště) a také byl nalezen inzerát jedné zaměstnankyně správního odboru prodávající své auto.

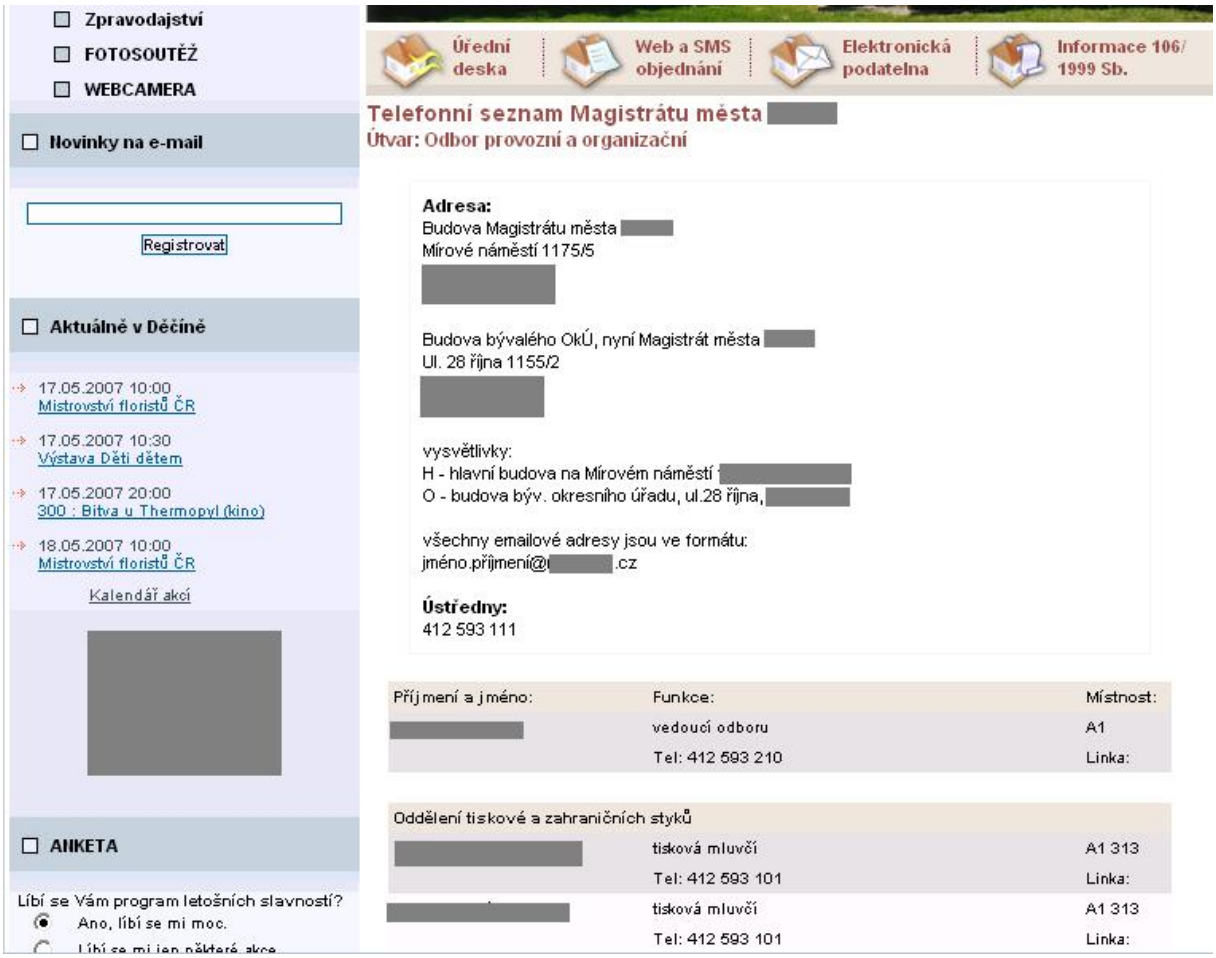
Některé stránky zobrazují statistiky přístupu ke svému obsahu nebo evidují dotaz v diskuzi prostřednictvím zdrojové adresy v doménovém tvaru. Většina síťových administrátorů pojmenovává proxy server, kterým přistupuje organizace k Internetu, ve tvaru „gate.jmeno_organizace.cz“. Ukázalo se, že ne jinak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

Očekáváním bylo, že budou nalezeny příspěvky zaměstnanců v diskuzích, nicméně žádný informačně hodnotný zdroj nebyl nalezen.

Webové stránky

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

Tou první je telefonní seznam (Obrázek 10). 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.



Obrázek 10: Zveřejněný telefonní seznam magistrátu

Druhou informaci, kterou se podařilo získat, 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 však stala velice cennou díky rozboru webové stránky tvůrce tohoto informačního systému.

Tam se nachází podrobný popis daného 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 ke konkrétním požadovaným informacím.

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 nimi je uveden také Magistrát města.

Informační systém RADNICE VERA je rozdělen na čtyři základní skupiny podsystémů (finanční, majetkové, správní, organizační). Z pohledu testování byla zajímavá pouze skupina správních podsystémů. V této skupině se nachází 15 podsystémů, z nichž 5 má přístup do registrů obyvatel, tedy i k 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.

Příprava útoku

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 pak odvodit 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 počítat s co největším počtem možných variant, 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.

Návrh útoku

Na základě těchto informací byl navržen pokus o získání 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, druhý dotaz povede na osobní údaje útočníka, konkrétně 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.

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), se dalo předpokládat, že tomu tak bude, ale ne s absolutní jistotou. Proto hned na začátku prvního hovoru bylo třeba toto ověřit 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 pak lze rozhodnout, jakým způsobem měl hovor probíhat, zda se měl vést v přátelském tónu, zda se mělo zaměstnanci tykat nebo vykat apod.

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

Všechny hovory skončily s téměř stejným výsledkem. Osoba, která zvedla telefon, po krátkém zamyšlení sdělila, kde hledanou osobu najít. Pak ihned přepojila na správnou telefonní linku (V tu chvíli byl telefon zavěšen). 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.

Zde je uveden průběh jednoho rozhovoru:

Zaměstnankyně správního odboru: *"Dobrý den, zde paní Jiřina Novotná, oddělení podpory pro nezaměstnané, jak vám mohu pomoci?"*

Útočník: *"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."*

Útočník: *"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 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 bylo 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.

Samotný útok

Na základě výše zjištěných informací a návrhu útoku byl proveden samotný útok, který se skládal ze dvou telefonních hovorů. Zde je uváden jejich průběh:

První hovor:

Zaměstnanec: *„Dobrý den, zde Jitka Nováková agenda ***."*

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. 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.“*

Druhý hovor o 5min později:

Zaměstnanec: *„Jitka Nováková, agenda ***.“*

Útočník (pomalým hlasem)*: „ Dobrý den, tady je operační dispečer Městské policie. 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:

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 ***.“*

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

Útočník: *„Vypadá prý mezi 20-25.“*

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

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

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

Rozbor útoku

Klíčový pro tento útok byl první hovor. Hned na začátku se útočník 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 se útočník vydával. To bylo překvapivé, neboť 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 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 začala útočníkovi tykat a oslovovala ho i křestním jménem osoby, za kterou se vydával.

Důvodů, proč považovala útočníka za osobu, za kterou 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 podařilo získat osobní údaje, i když nastaly určité komplikace, kdy nadřízená nesdělila zaměstnanci, na jehož pracoviště útočník 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.

Slabé stránky bezpečnosti IS

V případě magistrátu bylo odhaleno 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.

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, 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.

Nicméně je zbytečné, aby na webových stránkách magistrátu byl telefonní seznam obsahující jména všech zaměstnanců, např. 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. Obecně by měla být zveřejněna jen ta jména, která jsou pro veřejnost relevatní a souvisí s výkonem státní správy. To má i výhodu v tom, že občan lépe identifikuje vhodného úředníka pro svou potřebu. 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 by z veřejného telefonního seznamu měla být odstraněna 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.

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.

Shrnutí navrhovaných změn

Navrhované změny jsou následující:

- 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. Zaměstnanec, který při testování spolupracoval, 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. 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 zejména ty zaměřené na přímou manipulaci obsluhy, jsou pro případného útočníka použitelné k získání citlivých informací a jsou v oblasti ochrany informací podceňovány.

Závěr

Podceňování problematiky bezpečnosti informačního systému z hlediska lidského faktoru je v současné době nepřijatelné 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 se stát 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 médiích. Také média by mohla častěji upozorňovat na aktuální hrozby v podobě nových rychle se šířících virů apod. Provedené testování 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] SOTONA, Petr. Lidský faktor v oblasti bezpečnosti informačních systémů. Pardubice, 2007. 60 s. , 2, Univerzita Pardubice.

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

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

[4] 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>

[5] 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>

Kontaktní adresa:

Ing. Milan Tomeš
University of Pardubice, Fakulta ekonomicko-správní,
Ústav systémového inženýrství a informatiky
Studentská 84
53210 Pardubice
Email: milan.tomes@upce.cz
tel. č.: +420 466 036 147