Igor Pavlovič, Matej Kostrec

Nové formy počítačovej kriminality

Anotácia: Sociálne inžinierstvo je pirátskou technikou, ktorá je založená na využití dôverčivosti užívateľa informačných systémov a internetu, s cieľom vymámiť od neho citlivé dôverné údaje potrebné na komunikáciu s konkrétnym informačným systémom. Hlavným cieľom piráta je získanie informácií, ktoré mu umožnia právoplatný prístup do informačného systému, do ktorého si želá preniknúť. V tomto článku ponúkame niekoľko odporúčaní, ako sa nestať obeťou sociálneho inžinierstva.

Kľúčové slová: autentizácia – dôvernosť – integrita, doménové mená, elektronické bezpečnostné komunikačné protokoly, internet, sociálne inžinierstvo, šifrovanie.

Sociálne inžinierstvo je praktika používaná na získanie dôvernej informácie manipuláciou a zavádzaním ľudského jedinca. Existuje mnoho definícií pojmu „sociálne inžinierstvo“, ale žiadna nie je dostatočne vyčerpávajúca a jednoznačná pre popis aktivity, ktorú tento pojem predstavuje. Vstupujú pri nej totiž do hry vždy iné ľudské subjekty, ktorých správanie je originálne, a čas i použité metódy sa líšia. Iba cieľ, a to získanie dôverných informácií, je spoločný. Pre lepšiu predstavu si uvedieme príklad použitia sociálneho inžinierstva v praxi.

„Sociálne inžinierstvo bolo hlavnou zbraňou kedysi najhľadanejšieho hackera na svete – Američana Kevina Mitnicka. Ten už v šestnástich rokoch dokonale vycítil, že najlepším kľúčom k zamknutému systému nie je modem alebo počítač, ale obyčajná ľudská ľahkovážnosť. Ešte ako stredoškolák zatelefonoval systémovému manažérovi firmy Digital Equipment, ktorému sa predstavil ako vedúci vývoja nového produktu, a tak z neho vymámil heslo na prístup do siete.

Svoju stratégiu neskôr vypracoval do najmenších detailov. V jednu februárovú noc roku 1994 zatelefonoval systémovému administrátorovi spoločnosti Novell a predstavil sa mu ako zamestnanec firmy Gabe Nault. Tvrdil, že je na dovolenke, ale aj tak potrebuje prístup do siete, aby mohol pracovať na nejakom rozbehnutom projekte. Keďže systémový inžinier G. Naulta nepoznal, chcel si aspoň overiť, či je volajúci skutočne tým, za koho sa vydáva. A tak zatelefonoval na jeho firemný záznamník. Lenže K. Mitnick to predvídal. Skôr ako telefonoval administrátorovi, nabúral sa do hlasovej schránky G. Naulta, vymazal pôvodné privítanie a nahral svoje vlastné. Správcovi systému sa teda zdalo všetko v poriadku, a tak domnelému G. Naultovi zriadil vzdialený prístup do siete. K. Mitnick z firemného servera následne ukradol zdrojový kód najdôležitejšieho produktu firmy, sieťového operačného systému NetWare.“[1]

Ako sa teda popasovať s týmto novým fenoménom počítačovej kriminality a nestať sa jeho obeťou? Pretože nejde výhradne o technické zneužitie počítačových a komunikačných zariadení alebo programového vybavenia, ale hlavnú úlohu tu hrá manipulácia založená na psychológii, najdôležitejším odporúčaním je byť informovaný o tom, že existuje možnosť takejto manipulácie a o jej možných scenároch. Cieľom nášho článku je predstavenie niektorých situácií spojených so sociálnym inžinierstvom, ktorým môžete byť vystavení pri používaní internetu, a najmä pri finančných transakciách realizovaných prostredníctvom elektronickej komunikácie.

[1] http://www.etrend.sk/technologie/it-firmy/bezpecnost-casto-ostava-len-na-papieri/26356.html (6.6.2008)

Opatrnosť v prípade žiadosti o informácie

Nikomu neprezraďte vaše užívateľské meno a heslo. Žiadna seriózna inštitúcia nebude od vás žiadať takýto typ informácie, ani telefonicky. Toto odporúčanie platí aj v prípade, ak sa vám zdá žiadosť vierohodná a obsahuje evidentné identifikačné charakteristiky inštitúcie, od ktorej žiadosť prichádza, napríklad zdrojová elektronická adresa, webová stránka podobajúca sa na oficiálnu stránku inštitúcie. V prípade pochybností neodpovedajte a obráťte sa na príslušnú inštitúciu o potvrdenie serióznosti jej požiadavky.

Preverte si serióznosť dodávateľa

V prípade elektronického nákupu je potrebné obchodovať výhradne so serióznymi dodávateľmi. Zadávajte číslo vašej bankovej karty iba na webové stránky, ktoré používajú bezpečnostný protokol. Túto skutočnosť je možné spoznať prostredníctvom malej visiacej zámky zobrazenej na spodnej lište navigátora alebo prostredníctvom názvu protokolu indikovanom v URL stránky (Uniform Resource Locator), ktorý je HTTPS (HyperText Transfer Protocol Secure) namiesto HTTP.

Pozor: Konštatovanie navigácie na zabezpečené stránky (https) neumožňuje v žiadnom prípade uistenie sa o serióznosti navštívenej webovej stránky. Protokol HTTPS garantuje iba to, že vymieňané informácie nebudú priamo zmenené, ako to môže byť pri používaní protokolu HTTP, ale prítomnosť HTTPS vôbec neumožňuje garantovať:

- serióznosť navštívenej webovej stránky. Táto môže byť pod kontrolou počítačových pirátov. Vaša elektronická objednávka nemusí byť nikdy zrealizovaná a vybavená;
- úroveň bezpečnosti šifrovania vymieňaných informácií. Protokol HTTPS zabezpečuje, že údaje sú šifrované, ale v žiadnom prípade negarantuje silu a pevnosť použitého šifrovania;
- spoľahlivosť žiadosti o zadanie bankových identifikačných údajov. Aj napriek tomu, že spojenie je uskutočnené prostredníctvom protokolu HTTPS, neexistuje žiadna garancia, že požadované bankové údaje nebudú zneužité, ak je spojenie uskutočnené s falošnou webovou stránkou.

Považujeme za potrebné uviesť aj skutočnosť, že aktuálne odhalené nedostatky protokolu HTTPS umožňujú získať spoofingom (získanie užívateľských kont) certifikáty SSL (Secure Socket Layer – šífrovacie kľúče).

Vždy sa odpojte od webových stránok

Odporúča sa, aby ste vždy ukončovali otvorené webové stránky a využívali v menu odkaz na odpojenie sa z webových aplikácií predtým, než sa pripojíte na bankovú webovú stránku na realizáciu elektronických bankových operácií. Ak sa neodpojíte, stopy pripojenia prostredníctvom niektorej webovej stránky môžu zostať prístupné pre počítačového piráta a umožniť mu zneužiť identifikačné údaje na nekalé ciele.

Monitorujte si svoje bankové účty

Môže ubehnúť viacero týždňov medzi získaním a zneužitím identifikačných údajov a zistením škôd užívateľom. Je preto dôležité starostlivo sledovať peňažné pohyby na svojich bankových účtoch, aby ste si overili, že tam nefiguruje žiadna abnormálna operácia a mohli v prípade existencie takejto operácie podať reklamáciu. Nemalo by ubehnúť obdobie dlhšie ako jeden mesiac bez toho, aby ste si overili stav a operácie vykonané na vašom bankovom účte.

Ľudské omyly

Považovať ľudské omyly za hrozby sa môže zdať trochu bezohľadné a netaktné, ale – ako ukazujú štatistiky publikované rôznymi inštitúciami – sú veľmi často príčinou informatických pohrôm. Za ľudský omyl považujeme každé správanie ľudského jedinca, ktoré nerešpektuje správne používanie informatických nástrojov a aplikácií a ktoré môže viesť nedobrovoľným a neželaným spôsobom k rôznym ujmám a škodám. Aktivity zrealizované úmyselne so zlomyseľným cieľom nie sú považované za omyl. Nie je možné zostaviť úplný zoznam ľudských omylov. Rovnako nie je možné ani kvantifikovať všetky možnosti týchto omylov. Jediné, čo vieme urobiť, je určenie niekoľkých rozlišovacích kritérií, pomocou ktorých dokážeme klasifikovať ľudské omyly.

Omyly typu „neznalosť“

Táto kategória zahŕňa všetky omyly, ktorých sa ľudskí jedinci dopustili nevedome. V skutočnosti môže byť veľký počet omylov spôsobený bez toho, aby si užívateľ uvedomil nerešpektovanie správneho používania alebo určitého pravidla, a bez toho, aby sa zamyslel nad dosahom svojho kroku.

Príklady omylov typu „neznalosť“:

- nesprávne používanie informatického nástroja;
- zmazanie údajov;
- sociálne inžinierstvo.

Omyly typu „nedbalosť“

Táto kategória zahŕňa všetky aktivity vedené osobami, ktoré sú informované a znalé, ale ktoré nerešpektujú pravidlá. Mohli by sme teda pridružiť pojem nedbalosť k dobrovoľnej realizácii aktivity. Avšak ani napriek tomu cieľom nedbalosti nie je vo všeobecnosti podvodné konanie.

Príklady omylov typu „nedbalosť“:

- nerešpektovanie procedúr určených na uchovanie údajov;
- nespúšťanie antivírusových programov po zapnutí počítača;
- prezradenie alebo zverenie hesla kolegovi;
- využívanie podnikovej infraštruktúry na súkromné účely;
- inštalovanie „nezakúpeného alebo nenormalizovaného“ programového vybavenia na počítač alebo server.

Ako prichádza k ľudským omylom?

Každý užívateľ informačného systému alebo počítačového a komunikačného zariadenia je potenciálnym subjektom páchania ľudských omylov. Tieto predstavujú neúmyselné hrozby, ktoré vyvolávajú rôzne stupne zraniteľnosti informačných a komunikačných systémov a zariadení.

Prvý stupeň produkujú užívatelia buď svojou lenivosťou, alebo absenciou profesionálneho svedomia. Do tejto kategórie spadajú všetky aktivity spáchané z nedbanlivosti, proti ktorým je veľmi ťažké bojovať. Nápravu je možné dosiahnuť snáď jedine prostredníctvom úrovne prijímania zodpovednosti a sankčných mechanizmov.

Druhý stupeň zraniteľnosti je produkovaný z dôvodu chýbajúceho zaškolenia alebo chýbajúceho zvyšovania povedomia o bezpečnosti. Absencia svedomitosti u ľudského jedinca predstavuje vysoký stupeň zraniteľnosti informačných systémov, ktorého skrytou stránkou je

absencia uvedomenia si spáchania chyby, a teda absencia odhalenia a opravy tejto chyby samotným páchateľom omylu. Chýbajúce zaškolenie a zvyšovanie povedomia o bezpečnosti ľudského jedinca predstavuje riziko, ktoré môže byť zneužité veľmi nebezpečnou hrozbou v podobe sociálneho inžinierstva.

Sociálne inžinierstvo je technika, ktorej cieľom je odcudziť dôverné informácie osôb. Na rozdiel od ostatných útokov si nevyžaduje programové vybavenie. Jedinou silou, ktorú využíva počítačový pirát, je ziskuchtivosť alebo hlúposť jeho obete, od úrovne ktorej závisí aj úspešnosť jeho útoku. Existujú štyri hlavné metódy sociálneho inžinierstva, ktoré počítačoví piráti praktizujú:

- **prostredníctvom telefónu.** Počítačový pirát kontaktuje svoju obeť telefonicky. Je to najjednoduchšia technika. Jej cieľom je získať informácie čo najrýchlejšie.
- **prostredníctvom pošty.** Počítačový pirát pošle obeti profesionálny list. Veľmi často používa ako kontakt poštovú schránku fiktívnej spoločnosti.
- **prostredníctvom internetu.** Táto metóda je porovnateľná s metódou používanou pri metóde sociálneho inžinierstva praktizovanej prostredníctvom telefónu. Počítačový pirát sa vydáva za prevádzkovateľa systému, informatika alebo technika zodpovedného za informačný systém.
- **priamym kontaktom.** Táto metóda je najzriedkavejšie používanou metódou, a to z dôvodu zložitosti a potenciálnych rizík pre počítačového piráta. Napriek tomu väčšina spoločností, ktoré poskytujú informatické služby by nepotrebovala veľa námahy, aby zneužívala sociálne inžinierstvo.

Prečo a ako sa chrániť?

Ľudské omyly predstavujú veľkú hrozbu pre všetkých užívateľov informačných a komunikačných systémov a môžu spôsobovať značné finančné ujmy a závažné poškodenia imidžu a straty reputácie.

Existuje mnoho prostriedkov, ako bojovať proti ľudským omylom. Odporúča sa venovať viac energie kontrolným mechanizmom, aby sa obmedzil vplyv ľudských omylov na informačné systémy, a nespoliehať sa na princíp, že budeme počas prevádzky schopní zabrániť vzniku akejkoľvek chyby či omylu.

Uvedieme niekoľko hlavných protiopatrení, ktoré by bolo vhodné prijať na zníženie rizika úspešného použitia sociálneho inžinierstva:

- **zvyšovanie povedomia.** Práve v tejto oblasti môžeme najľahším a najvýraznejším spôsobom znížiť riziko. Väčšina ľudských jedincov má vôľu zvyšovať si svoju informovanosť, a ak ich budeme informovať o dôležitosti ich každodenných úkonov, ako aj o hodnote spracovávaných údajov, zoberú si k srdcu naše odporúčania a budú ich poctivo realizovať.
- **zaškolenie a vzdelávanie.** Najlepším prostriedkom, ako zabrániť zlej manipulácii s dátami a programovým vybavením, je zaškolenie užívateľov na správne používanie softvérových aplikácií a manipuláciu s médiami.
- **sprístupnenie popisu procesov a procedúr a ich kontrola.** Pri zavádzaní softvérových aplikácií do prevádzky je jednou zo zásadných aktivít vypracovanie a sprístupnenie popisov procesov a procedúr, ktoré pokrývajú všetky dôležité bezpečnostné aspekty prihlasovania sa a chodu aplikácie (prístup, ochrana...). Tieto procedúry musia byť kontrolované cyklicky a ich nerešpektovanie by malo byť dôvodom na uloženie sankcií.
- **dvojité overovanie.** Aby sa zabránilo chybám a omylom pri nahrávaní údajov do kritických aplikácií (elektronická platba, elektronický obchod...), je rozumné

zaviesť do aplikácie zopakovanie nahrania údajov alebo dvojité overenie a potvrdenie ich správnosti.

- **riadenie omylov a sledovanie ich riešenia.** Omylom sa nedá úplne zabrániť. Preto je potrebné si z nich zobrať ponaučenie, aby sa zabránilo ich opakovaniu. Iba presná a dôkladná analýza chýb, ktorých sa užívatelia dopustili, a príčin vzniku týchto chýb a omylov umožní zabrániť ich opakovaniu.
- **centrálna správa užívateľov aplikácie.** Aby sa minimalizovali ľudské omyly, odporúča sa striktne obmedziť prístupy k aplikáciám a údajom a udeliť ich výhradne osobám, ktoré ich skutočne potrebujú.

Riziko nakazenia alebo odcudzenia lokálnych doménových mien

DNS (Domaine Name Service) je služba, ktorá umožňuje preložiť symbolické mená počítačov napojených do internetovej siete na IP (Internet Protocol) adresy tak, aby boli rozpoznateľné v sieti. Servery, ktoré vykonávajú túto operáciu na základe požiadaviek užívateľov internetu, sa nazývajú DNS servery. Ich úlohou je konvertovať doménové mená zadané užívateľmi internetu, napr. www.google.com na IP adresu 66.102.9.99, ktorá jediná je platnou lokalizáciou servera Googlu pre všetky počítače napojené na internet.

Z technického hľadiska každý server DNS disponuje databázou, ktorá obsahuje jednoznačnú väzbu medzi doménovými menami a IP adresami príslušných serverov. A ako pracuje DNS server? Jednoducho sa na základe zadania doménového mena pozrie do svojej vlastnej databázy a dá užívateľovi Internetu IP adresu servera, aby sa mohol napojiť svojou požiadavkou na správny server bez toho, aby si musel pamätať príslušný číselný reťazec. A tak sa základnou myšlienkou aktívnych útokov proti DNS serverom stáva nakazenie alebo odcudzenie internej databázy jedného alebo viacerých DNS serverov. Cieľom nakazenia databázy je prinútiť DNS server, aby dával zlú IP adresu počas požiadavky užívateľa internetu na preloženie doménového mena na IP adresu. Väzba doménové meno – IP adresa je v databáze narušená, t. j. presmerovaná.

Po takomto nakazení jedného alebo viacerých DNS serverov stačí počítačovému pirátovi napojiť do internetu záškodnícky server nakonfigurovaný na IP adresu, ktorú vložil počas operácie nakazenia do DNS servera. Následne budú všetci užívatelia internetu, ktorí si zadajú požiadavku na preklad doménového mena do tohto DNS servera, presmerovaní na server napojený pirátom. Navyše, ak pirát na ňom zobrazí identický obraz ukradnutej webovej stránky, nemá užívateľ internetu žiadny prostriedok na to, aby o tomto presmerovaní vedel, a nebude vedieť ani o tom, že ak zadá svoje osobné údaje na túto stránku, tieto budú zozbierané a zneužité počítačovým pirátom. Takýto typ útoku je používaný napríklad pri phishingu.

Ako môže počítačový pirát nakaziť DNS servery?

Túto operáciu môže vykonať dvoma rôznymi spôsobmi:

- **Útoky proti DNS serverom na internete**
  - DNS poisoning alebo DNS pharming
  - Falšovanie odpovede DNS

- **Útoky priamo proti užívateľom internetu**

Útoky proti DNS serverom na internete

1. *DNS poisoning alebo DNS pharming*

Popis

DNS poisoning, nazývaný aj DNS pharming, je pirátska technika, ktorá pozostáva v pomýlení DNS servera tým, že sú mu do databázy odkomunikované chybné väzby medzi doménovým menom a IP adresou.

Útok

Počítačový pirát musí aktívne nakaziť DNS server tým, že zmení jeho internú databázu. Hneď ako tento manéver uskutoční, všetci užívatelia internetu, ktorí požiadajú tento DNS server o preklad doménového mena na IP adresu, dostanú namiesto pôvodnej IP adresy IP adresu zvolenú počítačovým pirátom.

Protiopatrenie

DNS servery disponujú bezpečnostnými mechanizmami, ktoré obmedzujú následky tohto typu útokov. Tieto bezpečnostné kontroly, implementované na DNS servery sieťovými a systémovými administrátormi, sú relatívne účinné a garantujú užívateľom internetu správnosť, neporušenosť a integritu a umožňujú im dôverovať odpovediam poskytnutým DNS servermi. Vzhľadom na implementáciu týchto bezpečnostných mechanizmov je tento typ útoku v súčasnosti už zriedkavý.

2. Falšovanie odpovede DNS

Popis

Princíp tohto typu útoku spočíva v tom, že prvá odpoveď DNS servera získaná počítačom užívateľa internetu je jediná, ktorá je braná do úvahy.

Útok

Počítačový pirát atakuje užívateľa internetu, ktorého údaje chce odchytiť, početnými nevyžiadanými odpoveďami DNS s falošnou IP adresou pre vybrané doménové meno. Štatisticky je dokázané, že je to najčastejšie žiadaná adresa obete. Ak chce napríklad počítačový pirát odchytiť identifikačné údaje užívateľa webovej stránky www.Mojabanka.com, nainštaluje na internet server vizuálne podobný serveru Mojabanka a bude bombardovať svoju obeť nevyžiadanými DNS odpoveďami, ktoré prevádzajú doménové meno www.Mojabanka.com na IP adresu svojho falošného servera. Pokiaľ si užívateľ internetu, ktorý je vybraný za obeť, nepozerá stránku www.Mojabanka.com, nevyžiadané odkazy posielané pirátom nebudú brané do úvahy. Ale len čo sa bude chcieť užívateľ internetu pripojiť na stránku www.Mojabanka.com, automaticky a bez toho, aby si to užívateľ uvedomil, bude poslaná ako jediná odpoveď z DNS servera IP adresa, ktorá ho pripojí na pirátsku stránku, a citlivé údaje, ktoré zadá užívateľ, budú odchytené pirátom.

Protiopatrenie

Nainštalované bezpečnostné mechanizmy, ako napríklad kľúče, umožňujú chrániť transparentným spôsobom užívateľov internetu a čeliť takémuto druhu útokov. Kľúč je sekvencia písmen a číslic, niekedy náhodná, poslaná na server DNS s každou požiadavkou zo strany počítača užívateľa internetu na preklad doménového mena. Kľúč poslaný s požiadavkou musí byť prijatý serverom DNS a späť odoslaný spolu s odpoveďou, aby túto odpoveď užívateľov počítač zobral do úvahy. Pokiaľ počítačový pirát neodhalí, nespozná alebo neodchytí kľúče používané pri posielaní žiadostí užívateľov internetu do DNS serverov, používanie týchto kľúčov umožňuje ochranu užívateľov internetu pred takýmto typom útokov.

Útoky priamo proti užívateľom internetu

1. *Nakazenie lokálneho súboru odpovedí servera DNS*

Popis

Tento útok je lokálnym útokom, ktorého cieľom je nakazenie systémového súboru počítača obete. Tento súbor sa používa ako prvý zdroj informácií na prevod doménového mena ešte predtým, než je kontaktovaný sieťový DNS server.

Útok

Počítačový pirát musí zmeniť systémový súbor počítača obete. Tento súbor hrá úlohu lokálnej minidatabázy doménových mien a nachádza sa na každom počítači. Každá operácia, prostredníctvom ktorej sa vykonáva prístup na internet, sa v prvom rade pri zisťovaní doménového mena obracia na tento súbor. Preto sa nakazenie tohto súboru dotýka všetkých požiadaviek na získanie doménového mena, to znamená, že prístup na ktorúkoľvek webovú stránku môže byť presmerovaný na falošnú stránku počítačového piráta. Nakazenie tohto súboru môže mať dva následky:

- Presmeruje užívateľa internetu na falošnú webovú stránku namiesto legitímnej. Útok je podobný útoku vykonávaného formou DNS poisoningu, avšak nenapáda DNS servery zapojené do siete internetu, ale lokálny súbor počítača obete.

- Zabraňuje prístup ku konkrétnemu serveru. Táto forma útoku je často používaná počítačovými pirátmi, ktorí vyvíjajú počítačové vírusy a červy, aby zabránili aktualizácii antivírusových programov na napadnutom počítači a zabránili odhaleniu a eliminácii vírusu alebo červa.

Aby počítačový pirát zabránil odhaleniu existencie vírusu alebo červa implementovaného v počítači, jeho prvou aktivitou je zamedzenie normálneho fungovania antivírusových programov. Aktualizácia antivírusových programov môže byť blokovaná nakazením lokálneho súboru počítača. Pretože aktualizácia antivírusových programov sa vykonáva pripojením sa na webovú stránku tvorcu týchto programov, nakazenie lokálneho súboru počítača spôsobí, že bude sfalšované doménové meno servera tvorcu antivírusových programov a aktualizácia sa nevykoná. Nebude teda možné odhaliť existenciu vírusu alebo červa v počítači obete počítačového piráta.

Protiopatrenie

Pretože nakazenie lokálneho súboru doménových mien je často spôsobované vírusom, červom alebo malwarom (škodlivý softvér – napr. trójsky kôň), je veľmi dôležité:

- aktualizovať programové vybavenie počítača o patche (softvérové záplaty) dodávané výrobcami operačných systémov a autorizovaného softvéru,
- používať antivírusové programy,
- aktualizovať antivírusové programy.

2. *Nakazenie lokálneho súboru odpovedí servera DNS používaného pri internej domácej sieti počítačov*

Popis

Tento útok je rovnakým typom útoku ako pri nakazení lokálneho súboru odpovedí servera DNS, avšak jeho následky sú širšieho charakteru, pretože je eliminovaný prístup na internetové stránky zo všetkých počítačov napojených na domácu, resp. lokálnu počítačovú sieť. Má teda väčšiu pôsobnosť a zasahuje väčší počet obetí jednej rodiny, inštitúcie alebo podniku. Navyše aj pre komunikáciu medzi počítačmi tejto lokálnej siete sa využívajú lokálne doménové mená namiesto IP adries, a tak je možné touto formou útoku presmerovať aj interné údaje do počítača počítačového piráta.

Útok a protiopatrenie

Útok prebieha podľa rovnakého scenára ako v predchádzajúcom prípade. Protiopatrenia, ktoré je potrebné prijať, sú tiež rovnakého charakteru. Rozdiel je len v tom, že je potrebné aplikovať ich na viacero počítačov súčasne.

A aké sú všeobecné bezpečnostné odporúčania v boji proti sociálnemu inžinierstvu?

Vo všeobecnosti môže iba používanie elektronických certifikátov (SSL pre pripojenia HTTPS) slúžiť ako záruka bezpečnosti pre používateľov internetu. Pripojenia na internet zabezpečené certifikátom SSL prinášajú vysokú úroveň bezpečnosti, ktorá spočíva v troch zásadných princípoch:

- **autentizácia** servera – máte určite záruku, že server, s ktorým komunikujete, je skutočne ten, ku ktorému by ste mali byť pripojení, certifikát vás chráni pred útokmi na doménové mená,
- **dôvernosť** komunikácií vedených prostredníctvom internetu,
- **integrita** komunikácií vedených prostredníctvom internetu.

Je veľmi dôležité si vždy preveriť, či je SSL certifikát, ktorý je používaný pri komunikácii, platný a či bol vydaný dôveryhodnou inštitúciou, ktorá garantuje všetky tri princípy bezpečnosti.

Záver

Neexistujú zaručené odporúčania, ktoré dokážu užívateľa internetu ochrániť pred praktikami sociálneho inžinierstva. Cieľom väčšiny odporúčaní je zvýšenie informovanosti užívateľov o krokoch, ktoré sú počítačovými pirátmi používané. Rýchlosť vývoja nových praktík sociálneho inžinierstva si však vyžaduje aj zvýšenie informovanosti a povedomia všetkých užívateľov elektronických komunikácií, a tým aj prezentovania čoraz väčšieho počtu odborných publikácií dostupných pre širšiu verejnosť.

Literatúra

http://www.cases.public.lu (21. 5. 2008)
http://www.etrend.sk/technologie/it-firmy/bezpecnost-casto-ostava-len-na-papieri/26356.html (6.6.2008)

Key words: authenticity – confidentiality – integrity, domain names, electronically communication security protocols, encryption, Internet, social engineering.

Summary

Social engineering is a pirate practice/technique which is based on use of gullibility/acceptingness of the information system and internet user and its aim is to wangle sensitive confidential data/information needed for communication with the particular information system. The main aim of the piracy is to obtain information that will allow valid access to the information system he wishes to get into. In this article we offer some recommendation how not to become a victim of social engineering.

pplk. Ing. Igor Pavlovič
Akadémia Policajného zboru v Bratislave
e-mail: igor.pavlovic1@minv.sk

Mgr. Matej Kostrec
Akadémia Policajného zboru v Bratislave
Katedra manažmentu a informatiky
e-mail: mato.kostrec@stonline.sk

Recenzent: Ing. Ivan Fořt