Najviac bolí útok zvnútra

Ak by sme mali charakterizovať súčasný trend v oblasti IT, rozhodne by bolo treba uviesť jeho dva hlavné znaky. Vďaka čoraz intenzívnejšej komputerizácii a rýchlo sa rozvíjajúcim info-komunikačným technológiám vznikajú väčšie a tesnejšie prepojené korporácie, v ktorých sa hranice medzi jednotlivými biznis partnermi čoraz viac stierajú, a ktoré sú viac otvorené tretím subjektom, dodávateľom a zákazníkom. Cena informácie narastá. S rozvojom elektronického obchodovania sa otvorili nové, menej riskantné a zároveň efektívnejšie možnosti organizovaného zločinu, najmä pokiaľ ide o zločiny spojené s odcudzením identity.

Peter Šteruský
Business Development Manager, TEMPEST

peter_sterusky@tempest.sk

Oba tieto trendy spolu s relatívne nízkym rizikom a vysokou efektivitou aktivít majú priamy dopad na zvýšený výskyt tzv. „insider" útoku, t.j. útoku, ktorý je vedený zvnútra organizácie. Zároveň je čoraz viac ľudí s prístupom k informáciám, ktorých je možné čoraz ľahšie skorumpovať, skompromitovať alebo vydierať.

Kto všetko môže vlastne byť potenciálny a obávaný insider? A čo je najčastejšou motiváciou? Tieto dve otázky úzko súvisia. Zatiaľ čo najčastejšou motiváciou je „odplata, strach, ziskuchtivosť", logicky obávaným insiderom bude najčastejšie nespokojný, prepustený, nedocenený alebo vydieraný zamestnanec, resp. člen manažmentu danej organizácie. Pozrieme sa na to detailnejšie.

KRUTÁ REALITA VO VYŠE POLOVICI SPOLOČNOSTÍ

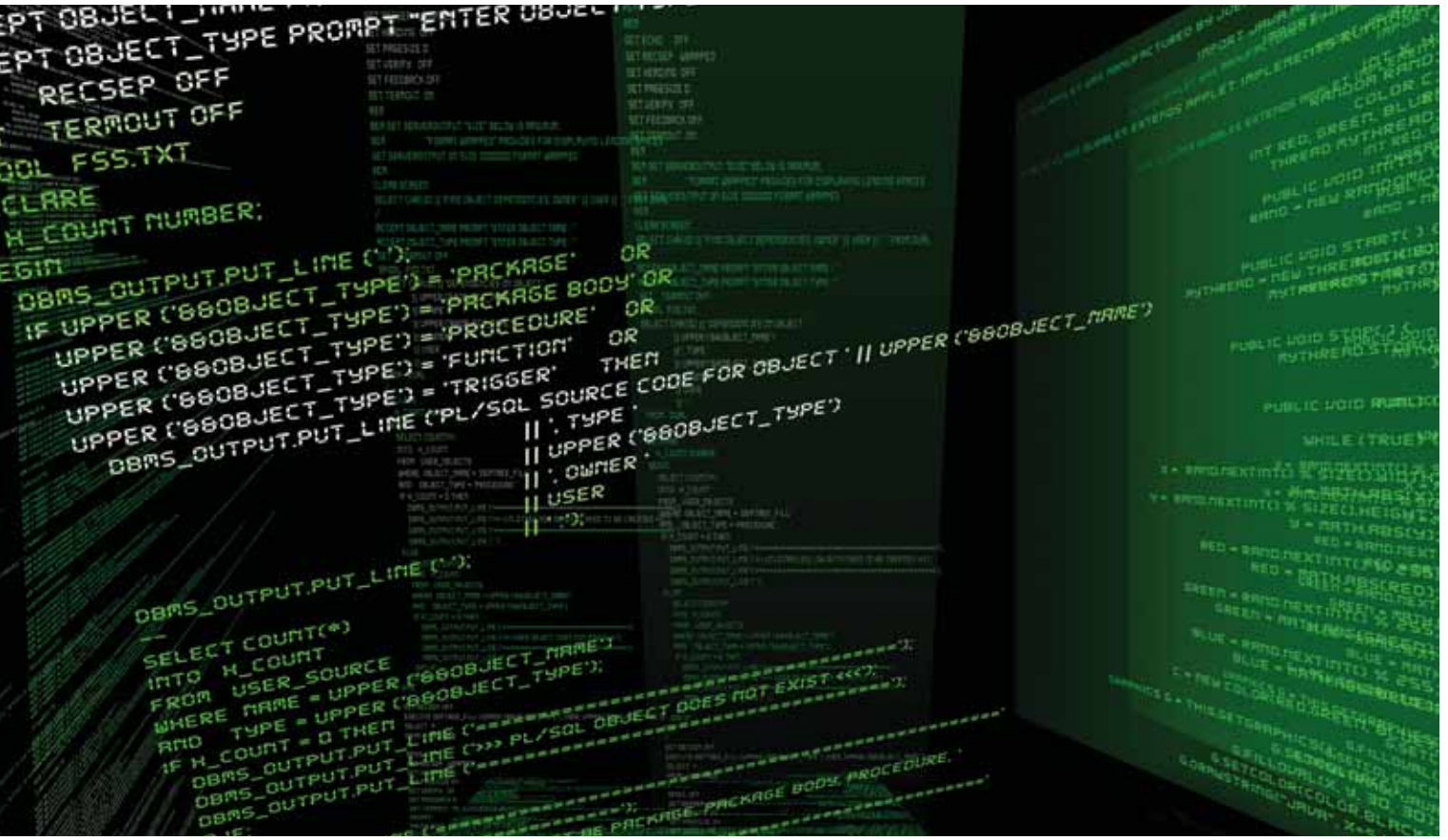
Tradične primárnou starosťou bolo chrániť počítačové systémy pred útokom zvonka. Dnes to už zďaleka nie je pravda. Útok zvnútra je veľkým a stále vážnejším problémom. Podľa prieskumov a štatistík tajnej služby, FBI a ďalších organizácií je postihnutých viac ako 59 % spoločností. Z týchto 59 % spoločností 7 % priznalo, že straty zapríčinené insidermi zodpovedajú až za 80 % ich finančných strát. Najnovšie odhady hovoria o celkových stratách vďaka cyber kriminalite a organizovanému zločinu za pričinenia insiderov v hodnote 1 bilióna USD len za posledný rok. Jednoduchý príklad: Société Générale počas troch dní v januári 2008 stratila v dôsledku insider attacku 4,9 miliardy eur. Ekonomická a finančná kríza prispieva k rastúcemu trendu nemalou mierou. Čoraz viac ľudí pracuje pod hrozbou straty svojho miesta a finančnej neistoty. Príčin, prečo je „insider attack" takou vážnou a rastúcou hrozbou je však okrem toho hneď niekoľko.

V prvom rade útok zvnútra nie je jednoducho rozpoznateľný. Ďalším vážnym dôvodom, prečo sa vyskytuje častejšie, je motivácia. Cyber kriminalita je dnes miliardový biznis a kompromitácia informačných systémov nie je už len koníček, zábava nadaných profesionálov z oblasti IT, ale úmyselná, vedomá aktivita s cieľom získať profit. Tým nechcem povedať, že peniaze bývajú jedinou motiváciu. Niekedy ňou môže byť aj nuda, úsilie niečo „vyviesť", dostať sa k dátam, ktoré mi zamestnávateľ nechce ukázať, alebo dokonca pomsta a odplata za reálne či imaginárne ublíženie zo strany spoločnosti.

„SMRTIACA" KOMBINÁCIA

Treba si uvedomiť dva charakteristické znaky situácie insiderov – útočník je niekto, kto zvyčajne veľmi dobre pozná interný systém, a zároveň niekto, komu bola poskytnutá dôvera a prístup k informačnému systému. Insider je teda obrovské bezpečnostné riziko vďaka dvom atribútom: znalosti a prístupu k systému. Toto je často „smrtiaca" kombinácia. Pre IT security profesionála je často problém chrániť systém pred útokom zvonka. Úspešne ho však ochrániť pred útokom zvnútra sa môže zdať za určitých okolností nemožné. Ak insider dobre pozná systém a vie, ktoré jeho časti sú chránené a ktoré nie, môže sa jednoducho zamerať na najmenej chránené alebo vôbec nechránené systémy. Ak si položíme otázku „kto stráži strážcov", máme na stole znova otvorený problém. Skúsme nezabúdať, že insiderom, ktorý dokáže zničiť firmu je často jej manažér alebo riaditeľ. Priznajme si, že osoby, ktorých úlohou je chrániť informačný systém a udržovať ho v prevádzke sú často najväčšou hrozbou pokiaľ ide o informačnú bezpečnosť. Najnovšie prieskumy CERT a Secret Service uvádzajú, že 86 % prípa-

Kto všetko môže vlastne byť potenciálny a obávaný insider? Logicky obávaným insiderom bude najčastejšie nespokojný, prepustený, nedocenený alebo vydieraný zamestnanec, resp. člen manažmentu danej organizácie.



dov sabotáže v interných sieťach majú na svedomí technickí pracovníci. Insider nemusí byť len váš zamestnanec alebo IT administrátor, ale ktokoľvek nejako prepojený s vašou organizáciu alebo poverený vykonávať pre ňu určité aktivity, t.j. môžeme rady insiderov rozšíriť o obchodných partnerov, dodávateľov, subkontraktorov a v neposlednom rade o špeciálnu skupinu tzv. bývalých insiderov, kde sa ľahko mohlo stať, že ich prístup k systémom nebol zrušený alebo ktorí používajú na prístup údaje, ktoré si tajne vytvorili v čase, keď ešte insidermi boli.

> Tri typy útoku: zneužitie prístupu, obídenie bezpečnostných prekážok a zlyhanie kontroly prístupu. Posledný typ útoku je zároveň aj jediným typom insider útoku, kde sa dá hovoriť o naozaj účinnej obrane.

TRI HLAVNÉ TYPY ÚTOKU

Profesionáli, ktorí sa zoberajú touto problematikou, definujú v podstate tri hlavné typy útoku: zneužitie prístupu (keď sa príslušné poskytnuté oprávnenia a prístupové práva zneužijú na nesprávne ciele), obídenie bezpečnostných prekážok (čo je pre insiderov, ktorí sa už de facto nachádzajú v sieti omnoho ľahšie ako pre útočníka, ktorý musí prekonať v prvom rade obranu perimetra) a zlyhanie kontroly prístupu (typicky ide o technologický problém, ak napr. systém je zle nakonfigurovaný a má bezpečnostné diery). Posledný typ útoku je zároveň aj jediným typom insider útoku, kde sa dá hovoriť o naozaj účinnej obrane. V prvých dvoch prípadoch ide v prevažnom množstve prípadov skôr o detekciu po útoku alebo maximálne počas útoku.

Ak aj útok zvnútra nebudeme pokladať za najbežnejší bezpečnostný problém informačných systémov, rozhodne patrí pokiaľ ide o svoje dôsledky k najvážnejším. Tak sa k nemu stavajú predovšetkým vládne organizácie a veľké korporácie.

Útok insidera je veľmi ťažké detekovať či už technologickými alebo „ľudskými" prostriedkami. V mnohých prípadoch došlo k odhaleniu náhodou, napr. tak, že sa insider preriekol pred kolegami.

Technologické prostriedky typu IDS, obsahových filtrov či šifrovanie dát cez celú IT platformu majú svoju nezanedbateľnú hodnotu, ale… je zrejmé že aktivita insidera bude väčšinu času úplne v poriadku a nebude sa diať nič anomálne, čo by mohol IDS-IPS systém zaznamenať a vyhodnotiť ako potenciálny útok. Ak chceme monitorovať všetko v sieti, kladieme obrovský nápor na IDS/IPS systém. V prípade, že dochádza k útoku rozloženom per partes vo veľkom časovom intervale, IPS systém musí poskladať tieto kúsky a príslušne ich korelovať cez veľký časový interval, čo je časovo značne náročne.

Dnes je ťažko povedať nakoľko sú tieto technologické prostriedky úspešné v boji proti insiderským útokom. Nie sú k dispozícii dostatočné štatistiky a tiež prevláda názor, že insider, ktorý vie o monitorovaní, je skôr odradený, než prichytený touto technológiou. Keďže tieto technológie musia sledovať obrovské množstvo dát v relatívne veľmi dlhom časovom intervale a navyše ešte rozoznať zlomyseľné aktivity od neškodných, môžeme konštatovať že tieto požiadavky často presahujú možnosti dnešných IDS, IPS a iných technológií. Technológia má však prioritnú úlohu napríklad v momente prepustenia zamestnanca, keď potrebujete okamžite revokovať jeho privilégia. Toto a iné aspekty musia byť rigorózne definované v bezpečnostnej politike organizácie a bezpečnostných direktívach opierajúcich sa o technické prostriedky a procedurálne kontroly.

TECHNOLÓGIA NESTAČÍ

Technológia nestačí. Jednoznačne musí nastúpiť ďalší aspekt – sociálne vedy. Základnou zložkou útoku insidera je koniec koncov človek. Osoba, ktorá zneužila zverenú dôveru a získané poznatky o systéme. Tu už nastupuje psychológia a úvahy o tom, aký typ ľudí predstavuje hrozbu pre bezpečnosť IS a aký typ ľudí pravdepodobne zneužije svoje postavenie a vedomosti.

A začať treba hneď na začiatku skríningom insiderov. Medzi najlogickejšie preventívne odporúčania patrí preverenie si perspektívnych a nových zamestnancov. Druhým dôležitým odporúčaním je sústrediť sa na obdobie medzi ukončením pracovného pomeru zamestnanca a momentom, v ktorom sú zrušené jeho doterajšie prístupové práva k systémom – teda na obdobie, keď sa udeje najväčší počet útokov insiderov, resp. bývalých insiderov. Poznajte svojich zamestnancov. Ich problémy môžu mať dopad na to, čo robia v zamestnaní a môžu znamenať zvýšene riziko. Rizikovým faktorom môžu byť napr. finančné problémy insidera v dôsledku jeho rozvodu alebo choroby. Nespokojní a nešťastní zamestnanci predstavujú pre firmu isté riziko.

NENAJÍMAJTE SI BÝVALÝCH HACKEROV

Nenajímajte si ako správcov IS a CSO bývalých hackerov. Možno sú to špičkoví profesionáli, ale rovnako by ste predsa na svojom účtovnom oddelení nezamestnali ako daňového poradcu niekoho, kto sedel za daňové podvody. Veľa sa v poslednom čase hovorí o typickom psychologickom profile insidera. Hľadajú sa charakteristiky ako mentálne poruchy, antisociálne alebo nevhodné správanie na pracovisku v minulosti, ale jednoznačný profil, podobne ako pri kriminálnych profiloch, neexistuje. Rozhodne sa však oplatí poznať svojich zamestnancov a ich problémy či starosti. Ak budete mať zamestnanca banky, ktorý zúfalo potrebuje peniaze aby mohol zaplatiť hypotéku a neprišiel o svoj dom alebo byt, a vy mu zamietnete zvýšenie platu, je tu potenciálne riziko, že dotyčný zamestnanec sa pokúsi predať napr. čísla kreditných kariet. Poznajte svoju firmu, svojich ľudí, svoje biznis procesy a všímajte si všetko, čo je anomálne. Insiderov, ich správanie, ich prácu. Vaši zamestnanci môžu byť tiež vystavení nátlaku zvonku a vydieraniu, či už kriminálnikmi, lobistickými skupinami alebo konkurenciou. Ak spozorujete čokoľvek anomálne z hľadiska bezpečnosti vašej spoločnosti, určite to stojí za preverenie. Nie je totiž vôbec jednoduché definovať, čo ešte je normálne a čo už nie. Anomálne správanie nemusí byť vždy škodlivé pre spoločnosť. V dnešnom dynamickom svete napr. investičného bankovníctva musíte ponechať priestor aj na netypické správanie, nová situácia môže zrazu vyžadovať prístup k novým informáciám, ktoré doteraz pracovník nikdy nepotreboval. Je to anomália, ale nie insider útok.

Manažéri musia byť aj psychológmi a sociológmi. Technológia samotná nestačí. Nastupuje integrácia technických riešení a sociálnych vied.

Napriek všetkému povedanému problém insiderov nezmizne, ani ho žiadnym zázrakom nevyriešime. Aspoň kým bude platiť doteraz nedoriešená otázka, ktorú vzniesol už Platón vo svojom diele Republica „Quis custodiet ipsos custodes?" (Kto stráži strážcov?).