



LEÉPÍTETT VESZÉLY!

Évek óta hangoztatják a biztonsági szakértők, hogy a belső dolgozók nagyobb veszélyt jelentenek a vállalatokra, mint a külső támadók. A válság elmélyülésével eljött a cselekvés órája, ha a vállalatok nem akarnak komolyabb veszteségeket elkönyvelni.

2008. október 24. 04.00 p.m. Rajendrasinh Babubha Makwana, 35 éves Unix adminisztrátor leütötte az utolsó Entert a rövid programban, amely minden reggel lefutott rendszerkarbantartó modulként. Egy órával később leadta a belépő kártyáját, aláírta a kilépő papírjait a Fannie Mae pénzügyintézetnél.

2009. január 31. 09.15 a.m. A Fannie Mae vállalat egyik kulcsfontosságú Unix szerverével megszakadt a rendszerfelügyelet kapcsolata. Majd sorban többiekkel is. A kritikus gépekre nem lehetett belépni, mintha minden hozzáférési jogosultság megszűnt volna.

A későbbi vizsgálatok megállapították, hogy mind a 4000 számítógépet módszeresen letörölték, aznap reggel 9.00 órától kezdődően. A kár több millió dollár, a Fannie Mae szolgáltatások 1 hétig elérhetetlenek voltak.

Nem, ez nem a legújabb high-tech krimi bevezetője, és Makwana nem egy versenytárs által felbérelt szuper-szabotőr, csak egy egyszerű szerződéses munkavállaló. A fent vázoltak szerencsére csak részben történtek meg, köszönhetően annak, hogy 2008. október 29-én egy rutin karbantartás során véletlenül felfedezték a Makwana által elrejtett logikai bombát, amely 2009. január 31-én aktiválódott volna.

Nem minden vállalat volt ilyen szerencsés az elmúlt időszakban:

- A Progressive Hydraulics másfél millió dollár árbevételű újjeländi mérnöki társaságnak 5 évre visszamenőleg semmisültek meg hasonló módon adatai, és csak 40%-át sikerült visszaállítani.
- A kaliforniai áramtözsdét működtető társaság egy hétfői napon kénytelen volt zárva tartani, mivel a pénteken elbocsátott munkatárs vasárnap este visszatért a nála hagyott belépőkártyával, és áramtalanította a teljes informatikai rendszert.

Az elkövetők minden esetben belső információval rendelkező munkatársak voltak, a motiváció pedig a düh, a csalódottság, a bosszúvágy.

A gazdasági válság miatt állásuk és akár az otthonuk elvesztésével szembesülő dolgozókból a recesszió „abnormális” reakciókat válthat ki. Az informatikai rendszerek megrongálásán túl a távozók előszeretettel visznek magukkal információkat, adatokat és fizikai tárgyakat. Egy kutatásban a résztvevő elbocsátottak 59%-a ismerte el, hogy bizalmas vállalati információkkal távozott. Általános munkavállalói gyakorlat az üzleti adatok CD-re, DVD-re, USB eszközre mentése, vagy egyszerűen a saját magán e-mail címre küldése.





A beépített veszély

Azokban az iparágakban, ahol (és hol nem...) csökken a teljes piac mérete, a túlélésért folytatott harcban bevetnek olyan módszereket, amelyeket egy-két évvel ezelőtt még a vállalatok nagy többsége elutasított. A legális ipari hírszerzésen túl fel kell készülni a törvényi kereteket súroló vagy átlépő információszerző támadások kivédésére.

A cyber veszély

A bankok szigorították a hitelezési gyakorlatukon, ma már nehezebben lehet lopott személyes információkkal bankszámlát nyitni, hitelkártyát igényelni. A cyber alvilág válasza kézenfekvő: mivel a személyes adatok leértékelődtek, többet fizetnek az online bankszámla és aktív hitelkártya információkért.

■ A PWC és biztonsági szoftvergyártó Finjan kutatása szerint a feleslegessé vált IT munkavállalók gyakran „tesznek egy próbát”, és megpróbálják értékesíteni megszerzett gyakorlatukat, illetve a korábbi munkaadóktól gyűjtött adatokat.

■ A gazdasági helyzet rákényszeríti a cyber alvilág szereplőit, hogy diverzifikálják a támadási formákat, és a spam, phishing, kémprogram, trójai program alapú pénzszerzéseken túl célzott támadásokkal, bennfentes információkon alapuló tőzsdei részvény manipulációkkal egészítsék ki tevékenységüket.

A veszélyek csökkentése

Térjünk a lényegre! Hogyan tudjuk a kockázatokat csökkenteni úgy, hogy minél kisebb mértékben érintse az üzletmenetet, és okozzon kényelmetlenséget a belső felhasználóknak? A fenyegetések nagy részét a kiemelt munkakörökben dolgozó belső munkavállalók képzik. Ők azok, akik ismerik a rendszereket, tudják az információ értékét, sok esetben ismerik a gyenge pontokat.

Az alábbi biztonsági kontrollok bevezetését javasolja a kancellár.hu:

1. Csökkentsük a minimumra a kiemelt jogosultságokkal rendelkezők számát. Implementáljunk és működtessünk megfelelő jogosultság-kezelési folyamatokat.
2. Limitáljuk az egy dolgozó által hozzáférhető bizalmas információk mennyiségét, alkalmazzuk a „need to know” és „least privilege” elvét, azaz mindenki csak annyi információnak és jogosultságnak legyen a birtokában, amennyi a feladata elvégzéséhez szükséges.
3. Osszuk meg a feladatokat, állítsunk fel kizárási szabályokat az egyes munkakörök közé (SOD – Segregation of Duties), és képezzünk egymást átfedő, ellenőrző feladatköröket. Állítsuk úgy fel a kritikus folyamatokat, hogy legalább két különböző dolgozó kelljen a teljes folyamat végig viteléhez.

Felelősség kizárás:

Felhívjuk tisztelt ügyfeleink figyelmét, hogy a sorozatban megjelenő publikációk a Kancellár.hu véleménynyilvánításának minősülnek, az azokban megjelent tartalmak további felhasználásából eredő bármilyen következményért, kárért, hátrányért a Kancellár.hu felelősséget nem vállal. A Kancellár.hu nem vállal felelősséget a publikációkban található információk értelmezéséért, sem azokért a cselekvésekért, amelyeket a publikációban található információk alapján hajtanak végre a felhasználók.

4. Az adatlopások megelőzésére használjunk DLP (Data Loss Prevention) megoldást, amely megfelelő implementáció esetében képes detektálni vagy megelőzni a bizalmas adatok eltulajdonítását.
5. Auditáljunk rendszeresen, és ha felfedezzük, hogy valaki visszaélt a bizalommal, határozottan lépünk fel vele szemben.

Egy hatékony védelmi rendszer több, egymással együttműködő komponensből tevődik össze. A Fannie Mae IT szervezetében is több kontroll jól működött, azonban a változások kezelésére, azok auditálására valószínűleg nem alakítottak ki megfelelő folyamatokat.

Végezetül ne felejtjük el, hogy az intézkedéseket kockázat-arányosan kell meghoznunk. A dolgozók többsége lojális, nem fog visszaélni a rábízott információkkal, a biztonsági intézkedések egy kártékony, jóval kisebb létszámú csoporttal szemben szolgálnak védelemül.

Elbocsátás előtt

Napjainkban sajnálatosan sokat hallott kifejezés az elbocsátás, csoportos leépítés fogalma. Miután az üzleti döntés megszületett az információ biztonságának is feladatai vannak, fel kell készülni rá. A tennivalók többé-kevésbé azonosak egyéni és csoportos leépítés esetében. Az első lépésben át kell tekinteni egyesével, hogy az elbocsátásra kerülők milyen rendszerekhez és információkhoz rendelkeznek hozzáféréssel. El kell különíteni az informatikai rendszerhozzáféréssel rendelkezőket és az üzleti felhasználókat. A legjobb módszer, ha kockázati csoportokba soroljuk őket. Első megközelítésben elég a felhasználókat négy csoportba sorolni (normál felhasználó, kiemelt felhasználó, informatikai munkatárs, kiemelt rendszergazda). A kockázati csoportokhoz lehet hozzárendelni az intézkedési tervet, mert teljesen más kezelést igényel, ha valakitől csak egy belépő kártyát kell visszavonni vagy rendszeradminisztrátori jogosultságokat. Készüljünk rá, hogy az elbocsátás híre kiszivároghat és már azt megelőzően a magasabb kockázati csoportok esetében állítsunk be erősebb audit feltételeket. Gondoljuk át, hogy vannak-e olyan közösen használt jelszavak, technikai azonosítók melyeket többen is ismernek és készítsünk tervet megváltoztatásukra. Csoportos leépítés esetében igényeljünk külső segítséget a nagy tömegű adatok feldolgozásához, helyszíni jelenlétet az esetleges informatikai biztonsági incidensek kezelésére.

Szerző: Bártfai Attila
kancellár.hu
CISSP, CISA, CISM, üzletfejlesztési igazgató

Ellenőrizte: Tiborcz József
kancellár.hu
információbiztonsági tanácsadó

Felelősség kizárás:

Felhívjuk tisztelt ügyfeleink figyelmét, hogy a sorozatban megjelenő publikációk a Kancellár.hu véleménynyilvánításának minősülnek, az azokban megjelent tartalmak további felhasználásából eredő bárminemű következményért, kárért, hátrányért a Kancellár.hu felelősséget nem vállal. A Kancellár.hu nem vállal felelősséget a publikációkban található információk értelmezéséért, sem azokért a cselekvésekért, amelyeket a publikációban található információk alapján hajtanak végre a felhasználók.