

Security 2.0: régi és új biztonsági kockázatok

A biztonsági kockázatok hatékony kezeléséhez jelentős kulturális és attitűdbeli változás szükséges, mivel a biztonság nem pusztán technológiai, hanem emberi kérdés. A szemléletbeli váltásra azért is van szükség, mert az informatikai rendszerek elleni támadások egyre komplexebbek – figyelmeztetett a Stratis tanácsadója.

Vajon ki mit tart vezető biztonsági kockázatnak? Ezt általában az határozza meg, hogy az illető milyen tapasztalatokat élt meg, és ebben az IT-biztonsági szakértők sem különböznek. Nagy az egyetértés közöttük abban, hogy az első számú kockázatot továbbra is a belső dolgozók – szándékos vagy gondatlan – szabálysértő magatartása, illetve jogosulatlan adatkezelése jelenti – hangsúlyozta *Tim Zoltán*, a Stratis vezető tanácsadója. Ez a kérdés azért is foglalkoztatja jobban a biztonsági vezetőket, mert a munkatársak elvileg megbízhatóak, a biztonsági zónán belül tartózkodnak, az információkhoz könnyebben hozzáférnek.

Kifinomult támadók

A külső támadások két fő csoportját különböztetjük meg: a vállalatoknak „csak” kellemetlenséget és költséget okozó, illetve az információbiztonságuk ellen irányuló támadásokat. Az első csoportba tartoznak a mindenkit érintő spamok, azaz a kéretlen reklám e-mailek, amelyek növekvő vállalati erőforrásokat kötnek le. A második csoportból számosságukkal kiemelkednek a rosszindulatú kódok, illetve malware programok (vírusok, férgek, trójaiak, reklám és kémprogramok), amelyek terjesztésére a felhasználót és a védelmi rendszert félrevezető technikákat alkalmaznak.

Újabb keletű probléma az egyre nagyobb mennyiségű adatot tárolni képes hordozható eszközök (például PDA, okostelefon, pendrive) elterjedése, amelyekre nem raknak fel biztonsági szoftvereket (antivírus- vagy tűzfalprogramot), és a belső hálózathoz kapcsolódnak. Ezzel hátsó ajtó nyitnak a vállalat védelmi rendszerén.

A mobilkészülékek elvesztését, ellopását a kisebb kockázatok között tartják számon a biztonsági szakemberek annak ellenére, hogy az ilyen esetek egyre gyakoribbá válnak.

A feltételező kockázatok között szerepelnek – *Tim Zoltán* szerint – az elektronikus csalások, a phishing (azaz az adathalászat) vagy a felhasználó számára kevésbé nyilvánvaló pharming (amikor a szokásos internetcímet beírva a felhasználót a csalók webol-

dalára irányítják át). Az ilyen támadások gyakorisága az elektronikus kereskedelem hazai elterjedésével együtt fog nőni. Viszonylag ritkán fordul elő, ezért az alacsonyabb kockázati kategóriába tartozóként kezelik az elektronikus vandalizmust, szabotázszt, illetve zsarolást. A rendszerek megbénítására irányuló DoS-támadások kockázati megítélése függ attól, hogy mennyire vonzó célpont az adott vállalat.

Kritikus adatvagyon

– Az előbbieken említett fenyegetések mindegyike a meglévő hiányosságokra épít – figyelmeztetett *Tim Zoltán*. – Az információk gyenge védelme annak tulajdonítható, hogy a vállalatok sokszor nem tudják, melyek a kritikus adatvagyon elemei, és ezek hol találhatóak. Ma Magyarországon elsősorban a pénzügyi szektorra jellemző, hogy az információk biztonságára jelentős összegeket fordítanak, de esetükben is ezt külső behatások segítették elő. Ők is csak annyit költenek a biztonságra, amennyit a hatósági előírások teljesítése megkövetel. Visszhangot keltő adat- vagy személyazonosság-lopás itt hon még nem fordult elő, de a tanácsadó arra figyelmeztet, hogy az amerikai cégek és hatóságok is csak akkor kezdtek el behatóbban foglalkozni a kérdéssel, amikor illetéktelenek már jelentős mennyiségű személyes adathoz jutottak.

A Stratis vezető tanácsadója szerint érdekes trend, hogy az otthoni gépek – védelem és szakértelem hiányában botnetek tagjaként – egyre nagyobb szerepet kapnak a kormányzati, illetve a vállalkozások informatikai rendszerei ellen irányuló támadásokban. A botnetek között megfigyelték, hogy a fertőzött gépekkel peer-to-peer alapon tartják egymással a kapcsolatot, a központi vezérelt botnetek pedig titkosítást használnak. A bethálózatok száma ugyan csökken, de a fertőzött gépeké folyamatosan nő, ami arra utal, hogy a vállalatok egyre képzetesebb és felkészültebb támadókkal állnak szemben.

Összességében is egyre inkább az látszik, hogy erősödik az alvilág jelenléte a világhálón, amely már átfogó támadások végrehajtására alkalmas erőforrásokkal és ismeretekkel rendelkezik.

Összetett támadások

A támadások kezdenek komplexsége válni, azaz több támadási formát, illetve gyengésséget kombinálva készítik elő akcióikat. Így például a webes alkalmazások sérülékenységét kihasználva rejtett bejáratot nyitnak, amelyen a támadáshoz szükséges további programokat juttatnak be a belső hálózatra, ahonnan koncentrált, jól kidolgozott támadásokat lehet indítani.

Aggodalomra ad okot, hogy egyre nagyobb számú, könnyen, általában távolról kihasználható sérülékenységre derül fény. A Symantec felmérése szerint a hibajavítások átlagosan 47 nap múltán állnak rendelkezésre. Az automatikus patchelés alkalmazásához a szoftverfejlesztőknek meg kell szerezni a felhasználók bizalmát. Sajnos előfordult már, hogy patchelés címén pont a szoftvergyártó telepített nem kívánatos szoftverkomponenseket a felhasználó gépre.

A jövő

A jövőben a felhasználóknak kifinomultabb, összetettebb támadási formákkal kell számolni. A támadók magas szintű ismeretek birtokában változatos módon kombinálják a támadási formákat (például a spamet és phishinget social engineeringgel).

A Windows Vista megjelenése új frontot nyit: a szakértők arra számítanak, hogy a jövőben a támadások nem a Vista ellen irányulnak, hanem a rá fejlesztett alkalmazások ellen, mivel úgy gondolják, hogy a kisebb cégek nem fektetnek annyi energiát a biztonságos fejlesztésbe. – Az alkalmazásfejlesztők prioritáslistáján a biztonság továbbra is a funkcionális és a teljesítménykövetelmények mögött kullog – húzta alá *Tim Zoltán*. – Egyre nagyobb gondot okoznak majd a virtualizációból fakadó fenyegetések is: a virtuális gépek védelme gyakran nem egyezik meg azazal, mintha az önálló hardveren futna; ezáltal a gazdagép erősebb védelme hamis biztonságérzetet ad.

Az új biztonsági kockázatok kezelése jelentős kulturális és attitűdbeli változást igényel, mivel a biztonság nem pusztán technológiai, hanem emberi kérdés: hogyan viszonyulnak az emberek azokhoz az eszközökhöz, amelyek biztonsági kockázatot hordoznak. A biztonságot a cégek üzleti kérdésként kezelik, és racionális döntéseket hoznak, amikor csak annyit költenek rá, amennyit feltétlenül muszáj. Nagyobb biztonság akkor várható, ha a biztonsági események következményei a jelenleginél drágább lesz számukra – fejezte be a beszélgetést a Stratis vezető tanácsadója. ■



Tim Zoltán
vezető tanácsadó
Stratis Kft.

Tippek biztonsági menedzsereknek

Hogyan „adjuk el” a biztonságot a cégvezetésnek?

- A vállalati hierarchiának megfelelő nyelvezeten szólítsuk meg az embereket
- Tettekkel, kommunikációval szerezzünk vizibilitást, erőforrásokat, befolyást
- Mutassuk ki a biztonsági intézkedéseink hatékonyságát
- Az embereket menedzseljük, ne a technológiákat
- A biztonságot nem eladni kell, hanem az igényt megteremtani

5 dolog, amire a biztonsági menedzserek figyelnie kell

- Szerezze meg a menedzsment támogatását
- Gondolkozzon rendszerben és biztonsági folyamatokban
- Hangolja össze a biztonságot az üzleti igényekkel
- Proaktívan menedzselje a kockázatokat, és ne a problémákat kezelje
- Tartson lépést a biztonsági menedzser szerepének a változásával