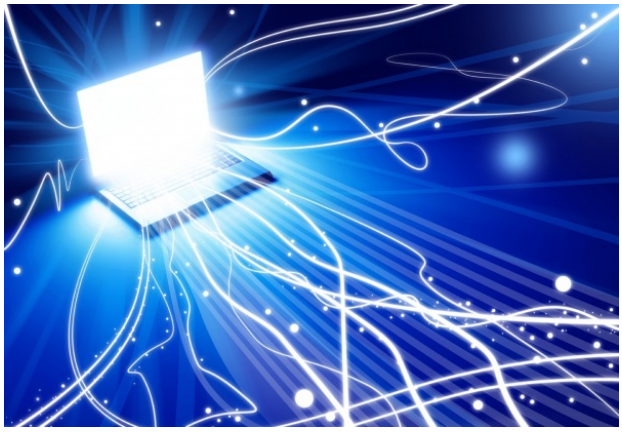
IT-biztonság: Mi van a buzzwordök mögött?

http://computerworld.hu/it-biztonsag-mi-van-a-buzzwordok-mogott-20121004.html October 5, 2012

Dávid Imre

Az olyan rendkívül talányos és jobbára lefordíthatatlan kifejezések, mint a "cloud security" vagy az "APT" mára az IT-biztonsági iparág kedvenc jelszavaivá váltak. A szakemberek mellett a laikusok számára is fontos lehet, hogy megértsék, mit takarnak ezek a furcsa betűsorok.



Az informatikai ipar sohasem idegenkedett a betűszavak és a nehezen érthető szakzsargon használatától. Különösen igaz ez az IT-biztonsági cégekre, amelyek rendre különféle, a beavatatlanok számára nehezen értelmezhető kifejezésekkel próbálják körülírni a biztonságtechnikai kérdéseket és fenyegetéseket.

Pedig egy olyan időszakban, mint a mostani, amikor nap mint nap hallani egy újabb nagystílű szerverfeltörésről, adatlopásról vagy egyéb hasonló fiaskóról, kiemelten fontos lenne, hogy a vállalatok és azok vezetői is megismerjék, mi van a jól csengő szakszavak mögött – már csak azért is, hogy tudják, mi ellen kellene védekezniük.

Nagy a fejetlenség

Roman Foeckl, a CoSoSys biztonsági cég vezérigazgatója szerint egyre több magánszemély és szervezet szembesül azzal, hogy arctalan idegenek az internetes fiókjaikban, a számlájukon vagy éppen a céges hálózatukban turkálnak. A felhasználók egyre zavarodottabbak; az általános pánikot csak tovább fokozza, hogy rengeteg gyártó kínálgatja a portékáit a piacon, ami elkerülhetetlenül hozzájárul a megrendelők növekvő bizonytalanságához – és persze a szakzsargon mértéktelen túlburjánzásához is.

Pedig fontos lenne, hogy az illetékes vezetők, döntéshozók tudják, mit jelentenek a gomba módra szaporodó szakkifejezések. A félreértések rossz döntésekhez vezethetnek: ha a tájékozatlan ügyfelek nem a nekik megfelelő termékeket, szolgáltatásokat választják, könnyen előfordulhat, hogy saját, féltve őrzött adataikat teszik ki felesleges veszélynek – arról nem is beszélve, hogy alaposan megterhelik a költségvetésüket, és végső soron egész kockázatkezelési stratégiájukat is tönkre vághatják – vélekedett Foeckl.

A Computerworld szerkesztősége szeretné megkönnyíteni az olvasók számára az IT-biztonság világában való eligazodást, ezért úgy döntöttünk, ösvényt vágunk a buzzword-dzsungelben, és megpróbáljuk tisztázni, mit takarnak a legtöbbet emlegetett szakszavak és kifejezések.

Cloud security (Felhőbiztonság)

Sokan vannak, akik összekeverik a cloud security és a cloud-delivered security-as-a-service kifejezések jelentését. Nem hibáztatjuk őket, már csak azért sem, mert ez a két, kétségkívül egymásra rímelő betűsor ugyanannak az éremnek a két – igaz, egymástól nagyban különböző – oldalát jelöli.

A „cloud-delivered security-as-a service” kifejezés alapvetően azokat a számítási felhőkben –

általában a szolgáltató saját szerverein – futó biztonsági megoldásokat jelöli, amelyeket SaaS (Software as a Service – szotver, mint szolgáltatás) konstrukcióban, előre kialkudott havidíj megfizetése ellenében vehetnek igénybe a megrendelők.

A „cloud security" jelentését már valamivel nehezebb körülírni: annál is inkább, mivel az újabb és újabb technológiák, szabályozások, iparági sztenderdek és gyakorlatok megjelenésével párhuzamosan folyamatosan formálódik, változik és gazdagodik.

A cloud security nem egyetlen témakört, hanem több, egymással laza összefüggésben álló területet jelöl. Többek között a felhőben tárolt adatok biztonságát, és az információk védelméhez szükséges biztonsági technológiákat – mint például a titkosítás. De – ha például katasztrófaelhárítási szempontból vizsgáljuk a jelentéstartalmát – vonatkozhat az olyan, elsősorban a spontán adatvesztést megelőző mentési eszközökre is, mint amilyenek például a backup szerverek.

Aztán ott vannak még a hozzáférés-kezelő (acces management) megoldások is, amelyek révén szabályozhatóvá válik, hogy az egyes felhasználók milyen, a felhőben tárolt adatokhoz és információkhoz férhetnek hozzá. Ezeket szintén a cloud security terminussal szokták jelölni a szakemberek – ahogy az engedélyeztetési és megfelelőségi előírásokat, mindenféle rendű-rangú policyket és más hasonló praktikákat is.

Advanced Persistent Threat, APT (Fejlett Állandó Fenyegetés)

Az APT-k általában olyan célzott támadások, amelyek hosszabb ideig tartanak, és többnyire valamilyen szellemi tulajdon, gazdasági vagy politikai információ megszerzése a céljuk, természetesen az áldozat tudta nélkül – elemezte a buzzwordöt *Michael Sentonas*, a McAfee Asia-Pacific technológiai igazgatója.

A kifejezés az utóbbi időben nagy népszerűségre tett szert a közvélemény körében: nem csoda, hogy gyakran hibásan használják – például a gyors pénzkeresést célzó „hétköznapi támadások" (mint a bankszámlák megcsapolása), internetes csalások esetében. „Az ilyen, általában egyszerű eszközök segítségével kivitelezett 'behatolok-eltűnök' támadások erős biztonsági architektúrával és többrétegű védelemmel könnyen kivédhetők" – magyarázta Sentonas.

„Az APT-támadásokhoz ezzel szemben magas szintű tudás szükséges: ezekkel általában csak azok a képzett, jól felszerelt és motivált hackerek próbálkoznak, akiknek van türelmük ahhoz, hogy számos támadási vektort kipróbáljanak, míg végül célhoz érnek és feltörik a célpont felhasználói fiókját vagy hálózatát" – hangsúlyozta a CTO.

Mobile Malware (Rosszindulatú Mobilszoftverek)

A mobil eszközök – okostelefonok, táblagépek és a többi – egyre nagyobb szerepet játszanak a mindennapjainkban. Ma már nem csak szabadidőnkben használjuk őket, de a munkahelyen – vagy inkább: munkaidőben – is; nem csoda, hogy egyre nagyobb fenyegetést jelentenek az olyan népszerű, sokak által használt szoftveres platformok ellen irányuló támadások, mint amilyen az Apple iOS-e, a Google Androidja, vagy a Microsoft Windows Phone operációs rendszere.

„Ha mélyebbre ásunk, megállapíthatjuk, hogy a mobil malware-ek jelentette veszély a hálózatok konvergenciájával és az egyre szofisztikáltabb kommunikációs eszközök megjelenésével párhuzamosan, egyre nő" – fejtegette Sentonas, hozzátéve: a felhasználók egyre értékesebb információkat tárolnak a mobil eszközeiken, így a kiberbűnözők is egyre nagyobb elszántsággal igyekeznek feltörni ezeket a rendszereket.

„A legnagyobb problémát az jelenti, hogy sokan még csak nem is hallottak azokról a biztonsági

megoldásokról, amelyek révén megóvhatnák a mobil eszközeiken tárolt szenzitív adatokat” – vélekedett Sentonas.

Mobile device management, MDM (Mobil Eszközmenedzsment)

A szakemberek rengeteg különféle szak- és betűszót kitaláltak már a tipikusan civil fogyasztóknak szánt eszközök munkahelyi megjelenésének leírására: a legismertebb ilyen kifejezés a BYOD (Bring Your Own Device – Hozd a saját eszközödet). A munkavállalók saját okostelefonjainak, tabletjeinek, ultrabookjainak „üzleti hasznosítása” számos előnnyel jár. Kényelmes nekik, a dolgozóknak, hiszen a jól megszokott, igényeiknek leginkább megfelelő eszközöket használhatják a mindennapi munkavégzés során, és egyúttal a munkaadóknak is, akiknek így nem kell a felhasználói hardver beszerzésével bajlódniuk. Ugyanakkor jelentős veszélyeket is magában rejt ez az egyre inkább elharapózó trend: az IT-szakembereknek a céges hálózat és a különféle platformok összehangolása mellett a biztonsági kihívásokkal is számolniuk kell.

Utóbbinak egyik széles körben elterjedt metódusa az MDM: a kurta (mással)hangzótorlódás mögé számos, a végfelhasználók mobil eszközeinek kezelésével és a kapcsolódó biztonsági megoldásokkal kapcsolatos eszköz és módszer felsorakoztatható.

„A kifejezés jelentése jelenleg is átalakulóban van, de az MDM-szakemberek alapvetően a BYOD-trend különféle biztonsági apektusait próbálják kezelni – mondta Foeckl. – Míg a mobil alkalmazásmenedzsment elsősorban a vállalati applikációk biztonságos használatával foglalkozik, addig az MDM a mobil eszközökön tárolt adatok biztonságát hivatott szavatolni."