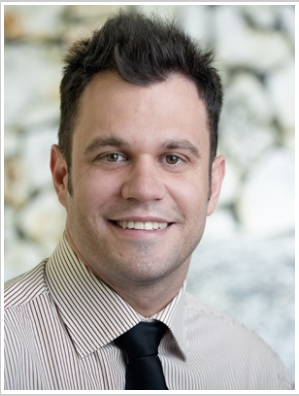
Beszélgetés az IT biztonságról - Csizmazia István és Béres Péter

2013.10.07.

Tetszik 5 g+1

Az alábbi interjúban Csizmazia Istvánt, az antivirus.blog.hu szerzőjét, valamint Béres Pétert, a Sicontact Kft. vezető It tanácsadóját faggatjuk arról, milyennek látják ők a hazai IT biztonság, szervervédelem kérdését.

Mi a helyzet Magyarországon, mennyire valósul meg a biztonság a szerverek tekintetében?



B.P.: Alapvetően sok céghez járunk ki, sok szakemberrel, vállalattal vagyunk kapcsolatban. Először csak hallottuk, hogy elég rossz a helyzet, nem hittük el, hogy ennyire. Pontos számadatok nincsenek, de hallottunk már olyan becslést, hogy az üzemeltetett weblapok 10 százalékánál is kevesebbje rendelkezik megfelelő védelemmel. Ez csak nagyságrendi szám, de ijesztő. Ez azt jelenti, hogy alapvető dolgok hiányoznak, mint mondjuk egy tűzfal, esetleg egy UTM megoldás, vagy bármilyen "fal", ami legalább figyelmeztet arra, hogy valamilyen támadás történik. Ezért van az, hogy könnyen megfertőznek olyan oldalakat, amiről nem is gondolnánk, hogy rosszindulatú lehet. Beszúrnak egy iframe-et vagy javascriptet, és ha meglátogatod, megfertőződsz. Aki mondjuk három éve nem frissített WordPresst vagy Joomlat használ, ne csodálkozzon, ha kihasználják a rendszer ismert gyengeségeit, sérülékenységeit.

Gondolom, sokan arra gondolnak, csak nem őket szúrja ki egy hacker.

B.P.: Pontosan. Arra azonban nem gondolnak, hogy ezek már automatikusan működnek, olyan programok hajtják végre a támadást, amik nézik, hogy vannak sérülékenységek, és megpróbálják ezt kihasználni. Ha pedig sikerül, mennek tovább.

A szemlélet hiányzik, vagy a pénz?

B.P.: Kis- középvállalkozásoknál az a tapasztalat, hogy nincs se pénz, se szaktudás, se idő a biztonságra. Ez szokott lenni az utolsó a vezetésnek. Ha azt hallják, 5 százalék az esély arra, hogy egy éven belül elérhetetlen lesz a szerver, azt mondják, oké. Ez nekik belefér, hogy ne kelljen nagyon foglalkozni a problémával. Amikor azonban probléma van, már késő azt mérlegelni, mennyivel lett volna jobb döntés a védelem kiépítése.

CS.I.: Sokan előbb kapnak a Google-tól figyelmeztetést, hogy a weboldalukat letiltották, mint hogy saját maguk integritás-ellenőrzéssel vagy más módon értesülnének a problémáról. Ha betörnek a házadba, és elviszik a tévédet, az biztosan rossz érzés. De ha rájössz, hogy már tizenötször betörtek hozzád, és nem tudod, mit csináltak, mit vittek el, vagy mit hagytak ott, az még rosszabb. A probléma mindennapos. Keress például az ismerőseid között olyanokat, akik GPG vagy PGP-t használnak a levelezésben, alá tudják hitelesen írni az üzenetet, vagy tudnak cserélni veled publikus kulcsot, hogy láthasd, ők írták az emailt. Keress meg cégvezetőket, orvosokat, és

Keresés

Internet, szerverek nélkül

Amit a mikroszerverek legjobban várnak 2014-ben: ARM alapú szerverek

Van esélye az AMD-nek visszatérni a szerverpiac élére?

Kihasználatlan a cloud, pedig Magyarország sereghajtó

Hírek

Cikkek

2013 11

2013 10

2013 09

2013 08

2013 07

2013 05

2013 03

kérdezd meg, hányan használnak titkosítást a gépükön. Kinevetik az MI6 emberét, aki elhagyja a gépét, tele bizalmas információval, de ők sem készültek fel ugyanerre.

A biztonság hiányáról csak a cégvezetők tehetnek?

B.P.: Nem, a probléma mindent átsző. Például programozói szinten is kevés idő van a security problémáit orvosolni, erre már alig marad idő a feszített tempóban. A biztonsági hibák is nagyon sokszor ide vezethetőek vissza. Sokszor előfordul, hogy egyeztetünk egy céggel, kérünk hozzáférést, és erre kapunk egy sima ftp elérést. Megkérdezzük, gondolkoztak-e már a titkosított csatornán. Bele sem gondolnak, nincs a köztudatban úgy, mint ahogy a mára alaptétellé vált állítás: egy windowsos gépre fel kell telepíteni egy vírusirtót.

Több kártevő leselkedik a cég adataira, mint eddig?

CS.I.: Nem tűnnek el a régi kártevők, ez benne a nehéz. 25 év összes kártevője mellett kell figyelni az újakra. Van, hogy az új malware még kipotyogtat magából régieket, hogy hátha a master boot recordot felül lehet írni. Nem teheted meg, hogy legyintesz rá: az már egy nagyon régi vírus, nem kell készülni rá. Mindre kell figyelni, és sajnos természetes, hogy egyre több van. Az elektronikus kémkedésnek pedig a vállalati titkok is célpontjai.

Emiatt aztán egyre többen a szerverbérlés, szerverhoszting felé fordulnak, hiszen ott a biztonságot, legalábbis egy részét átvállalja az erre szakosodott cég.

B.P.: Kis cégeknek már inkább megéri külső szolgáltatókat igénybe venni, már csak azért is, mert olcsóbbak lettek a szerverbérlés, szerverhoszting szolgáltatások az utóbbi években. Vannak olyan szolgáltatások, amiket kifejezetten jó ötlet kiszervezni. Persze egy ötfős cégnél felesleges SharePointot használni, de van, ahol ez kell. Nagyon fontos azonban szerintünk, hogy titkosítva legyen minden, ami kikerül a cégtől.

CS.I.: Egy céges biztonsági policy nem egy hét alatt összeütött tákolmány, hanem optimális esetben hosszú évek tapasztaltain alapuló, mindenre kiterjedő intézkedéshalmaz. Ehhez hozzátartozik az is, hogy milyen céget bízunk meg az adataink kezelésével, és hogy mennyire bízunk meg benne. És ha van ilyen policy, akkor nem azon fog múlni a végső döntés, hogy melyik adja egy forinttal olcsóbban a papíron ugyanannak tűnő szolgáltatást.

És egy mindenre kiterjedő szabályozás nyilván az alkalmazottakra is figyel…

B.P.: Belső emberre általában nem gyanakodnak. Pedig volt olyan eset, hogy egy cégtől távozó alkalmazott tett fel egy merevlemezt formázó kártékony alkalmazást a szerverre, ami aztán lefutott néhány gépen. Ez mondjuk extrém példa, de az ennél sokkal alapvetőbb jogosultságkezelés sincs megfelelő szinten. Sok cégnél nem tudják, melyik alkalmazott milyen adathoz fér hozzá, mi kerül ki a cégtől. És még ha fel is jegyzik az esetleges gyanús tevékenységeket: az sem mindegy, hogy milyen log fájlt viszel a bíróság elé, ha egy egyszerű, bármikor szerkeszthető txt-vel próbálkozol, nem tudod bizonyítani az igazad.

Hogy látjátok a security jelenét az országban? Mit tanácsoltok, hogy jobb legyen?

CS.I.: Számomra azt a legelkeserítőbb látni, hogy azoknál a projekteknél sem figyelnek a biztonságra, amik csillagászati összegekből, óriási támogatási pénzekből valósulnak meg. Pedig ezek lehetnének a kirakatpéldák, referenciamunkák, hogy na, így kellene működnie mindenhol. Hackerek, jöhettek. De nem ez történik, észre sem veszik a támadást, ha írsz nekik, nem válaszolnak, ha nyilvánosságra hozod, perrel fenyegetnek. Látszólag semmilyen incidens nem történik, de ennek a látszatnak nem szabad bedőlni. Az a szemlélet is hiányzik, hogy az évenként lefuttatott biztonsági vizsgálat eredményeit ne a fiókba süllyesszük, hanem a feltárt hiányosságokat megoldjuk.

B.P.: És ne higgyük azt, hogy a biztonság megvalósulhat úgy, hogy nem folyamatként tekintünk rá. Láttam olyat, hogy egy cég költött hardveres biztonsági rendszerre, úgy, hogy semmilyen hozzáférése nem volt az eszközhöz. Vagyis nem láthatta, hogy megvalósul-e a biztonság, csak nyugtázta magában, hogy ő mindent

megtett, amikor kifizette a profi benyomást keltő szakembereket. A biztonságra időt, pénzt és energiát kell fordítani, ha ezt elfogadja mindenki, az már egy jó irány.

Mennyire bízhat meg a DoclerWeb szolgáltatásaiban? Mennyire figyelünk a biztonságra? Kijátszható-e a védelmünk? Jöjjön el szerverterem-látogatásra, és győződjön meg a saját szemével.

« Vissza az előző oldalra

ITbiztonság security interjú

Tetszik 5 g+1

DOCLERWEB
+36-1-432-31-35
info@doclerweb.com

g+1