

Ponemon Institute: Hetente legalább egy belső visszaélés

- *A szervezetek mindössze 16 százalékánál ismerik fel a felső vezetők, hogy a belső visszaélések kiemelten magas kockázatot jelentenek*
- *A válaszadók 52 százaléka nincs birtokában olyan technológiának, amely segítene megakadályozni vagy gyorsan felismerni a belső visszaéléseket*

Budapest, 2011. november 8. – Riasztó adatbiztonsági trendekre hívja fel a figyelmet a Novell. Az [Attachmate Corporation](#) megbízásából készített felmérésben 700 vállalatot kérdeztek meg a szervezeten belüli visszaélésekről. A tapasztalatok szerint, bár a legtöbb vállalatnál léteznek szabályok a belső visszaélések ellen, azokat csak ritkán ültetik át a gyakorlatba. Az alkalmazottak tevékenységének nem megfelelő követése számos problémát okozhat, beleértve a negatív pénzügyi hatásokat, a jó hírnév csorbulását, valamint a bizalmas vagy titkos adatok eltulajdonítását.

A kutatás fő megállapításai:

- A válaszadók több mint 75 százaléka vallotta be: saját intézményük kiemelt felhasználói korábban bizonyíthatóan, vagy nagy valószínűséggel kikapcsolták, illetve módosították az ellenőrzési folyamatokat, hogy megváltoztassanak fontos adatokat, majd visszaállították a felügyeletet a nyomok eltüntetésére.
- Kiemelkedően nagy (81) százalékuk szerint bizonyíthatóan, vagy nagy valószínűséggel dolgoznak szervezetükben olyanok, akik mások hitelesítési adataival visszaélve jutottak magasabb jogosultsági szinthez, illetve kijátszották a feladatkörök szétválasztására hozott szabályokat.
- A válaszadók átlagosan hetente legalább egy, saját alkalmazott által elkövetett visszaélést fednek fel. A válaszadók 24 százaléka számolt be 100-nál is több esetről az elmúlt 12 hónapban.
- A szervezetek átlagosan 89 nap alatt derítenek fel egy ilyen jellegű eseményt, és további 96 napot vesz igénybe az okok felfedése, illetve a szervezetet érintő következmények meghatározása.

- A válaszadók többsége (62 százaléka) nem, vagy csak hozzávetőlegesen képes felmérni a visszaélések pénzügyi hatásait és valós költségeit.
- A belső vizsgálatok kétharmada során nem kerül elő olyan bizonyíték, amely felhasználható lenne az elkövető(k) ellen, így az ilyen esetek jó része büntetlenül marad, ami növeli az ismételt elkövetés esélyét.

Házon belüli problémák

A válaszadók 52 százaléka – saját bevallása szerint – nincs birtokában olyan technológiának, amely segítene megakadályozni vagy gyorsan felismerni a belső visszaéléseket, például az informatikai erőforrásoknak a nem engedélyezett célra történő használatát. Hagyományosan az informatikai részleg feladata a naplófájlok, ezeken keresztül pedig az alkalmazottak tevékenységeinek elemzése. Ugyanakkor a válaszadók 78 százaléka véli úgy, hogy a naplófájlok kézi átvizsgálása nem megfelelő módszer a megkérdőjelezhető vagy gyanús alkalmazotti hozzáférések, illetve számítógépes tevékenységek megfigyelésére.

A kutatás eredményei szerint azért ennyire elterjedt jelenség a belső visszaélés, mert sok vezérigazgató és felső vezető nem tartja kiemelt szervezeti feladatnak ezek megakadályozását. A válaszadó szervezetek mindössze 16 százalékánál ismerték fel a vezérigazgatók és egyéb felső vezetők, hogy a belső visszaélések kiemelten magas kockázatot jelentenek. Egy ilyen jellegű esetnek számos következménye van, a pénzügyi hatásoktól, a cég megítélésén keresztül, a bizalmas adatok eltulajdonításáig. Ennek ellenére a belső visszaélések továbbra is magas kockázatot jelentenek a szervezetek számára, mivel nem különítenek el megfelelő erőforrásokat az ilyen események megakadályozására, illetve gyors felderítésére.

„A kutatás eredményeivel szeretnénk ráébreszteni a megfelelő döntéshozókat, hogy a belső visszaélések valós kockázatot jelentenek, és a probléma annál súlyosabb lesz, minél később tesznek ellene” – mondta Szittyta Tamás, a Novell Magyarország ügyvezető igazgatója. „A felismerés természetesen csupán az első lépés, érdemes minél hamarabb kiküszöbölni a veszélyt egy alapos állapotfelmérés után. A Novell rendelkezik egy átfogó biztonsági portfólióval és így termékeink, mint pl. az [Access Manager](#), a [Sentinel Log Manager](#), vagy a [Novell Identity Manager](#) komoly segítséget nyújtanak az adatbiztonság javításában. Emellett nagy szakértelemmel bíró tanácsadó csapatunk, valamint partnereink hatékony támogatást nyújtanak az ügyfelek számára a kockázat áttekintésben és az optimális megoldás kidolgozásában” – tette hozzá Szittyta Tamás.

További információ a Novell biztonsági megoldásairól:

<http://www.novell.com/hu-hu/solutions/identity-and-security/>

A Novellről

A Novell a vállalati szoftvermegoldások egyik vezető szállítója. Kiemelt területein – Linux, Biztonság, Rendszerfelügyelet – a munkaállomásoktól az adatközpontokig teljes körű megoldásokat kínál. Termékeivel, hazai konzultációs részlegével és partnereivel segíti ügyfeleit a kritikus fontosságú üzleti alkalmazások biztonságos, költséghatékony, és megbízható üzemeltetésében a fizikai, virtuális és felhő alapú környezetekben egyaránt. További információért kérjük, látogasson el a <http://www.novell.hu> weboldalra.

Sajtókapcsolat

Jekler Rudolf

Kommunikációs vezető

Novell Magyarország

(06-1) 489 4600

06 20 9 675 565