

A Novell kutatása szerint komoly kockázatot jelentenek a vállalatoknak a végponti eszközök biztonsági rései

- *Az elmúlt 15 évben közel 220 millió érzékeny vállalati információt tartalmazó adat került ki biztonsági réseken keresztül, a vállalatoknak okozott károk csak az Egyesült Államokban éves szinten a 13 milliárd dollárt is meghaladják*
- *A felmérésben résztvevő informatikai vezetők szerint a legjelentősebb végpont-pont-védelmi problémák: a nem megfelelő adatvédelem, a mobil hozzáférések hiányos házirendjei és a rendszerintegritás hiánya*

Budapest, 2009. november 12. – A Novell bejelentette az informatikai fenyegetések értékelését célzó Threat Assessment felmérésének első eredményeit, amely szerint sok vállalat még mindig ki van téve olyan biztonsági fenyegetéseknek, amelyek könnyűszerrel megelőzhetőek lennének. A kritikus fontosságú adatok visszaszerzése és helyreállítása döbbenetes összeget emészt fel, de az ügyfelek bizalmának megrendülése akár egy vállalat végét is jelentheti. A Novell felmérésével az informatikai szakemberek munkáját kívánja segíteni a vállalati hálózati végpontok – például az asztali számítógépek, laptopok, intelligens telefonok, MP3-lejátszók és USB-kulcsok – megfelelő kiértékelésével. A felmérés olyan fontos sebezhetőségi pontokat tár fel, amelyeket a nem megfelelő adatvédelem, az elégtelen mobil hozzáférési házirendek, valamint az alkalmazásellenőrzés és a végponti eszközök rendszerintegritásának hiánya okoz.

„A végpontok biztonságát fenyegető támadások nagyon gyors ütemben fejlődnek” – mondta Grant Ho, a Novell [végpont-felügyeleti](#) megoldásokért felelős vezetője. „Létfontosságú ügyfeladatok vesznek el naponta a hanyag biztonsági gyakorlat miatt. Az informatikai fenyegetések értékelését célzó Threat Assessment felmérést úgy alakítottuk ki, hogy a vállalatok számára a lehető legjobban bemutassa sebezhetőségüket, továbbá útmutatást adjon a végpontok biztonságának, valamint az érzékeny vállalati és ügyfeladatok védelmének biztosításáról” – tette hozzá Grant Ho.

A Novell Threat Assessment felméréseinek megállapításai az alábbi legfontosabb területeken:

- **Nem megfelelő adatvédelem**

- A vállalatok 71 százaléka a laptopokon, míg a 73 százaléka a cserélhető adathordozókon tárolt adatokat sem titkosítja, ezzel jelentős kockázatnak teszik ki a vállalatot az eszközök elvesztése vagy eltulajdonítása esetén.
 - A válaszadók 72 százaléka állította, hogy nem ellenőrzik a cserélhető adattárolókra vagy optikai írókra másolt adatokat, és 78 százalékuknál nem készül jelentés a cserélhető adattárolókra másolt adatokról, így adatkezelési és megfelelőségi problémákat idézhetnek elő.
- **Elégtelen mobil hozzáférési házirendek**
 - A válaszadók 90 százaléka szerint a vállalati felhasználók irodán kívül (például wifi hotspotokon, hotelekben, kávézóknál) nyílt, nem biztonságos vezeték nélküli hálózatokat használnak, ezáltal támadások esetén a végpontok és az adatok sebezhetővé válnak.
 - A vállalatok 76 százaléka állította, hogy nem képesek biztosítani a végponti eszközök rendszereinek épségét, sértetlenségét és biztonsági megfelelőségét a szervezet hatókörén kívül.
- **Az alkalmazásellenőrzés és a rendszerintegritás hiánya**
 - A válaszadók 53 százaléka nem képes megelőzni, hogy a peer-to-peer fájlcsere forgalom, például a Bit Torrent és a Gnutella hozzáférjen a hálózatukhoz, így ezek a rendszerek kiszippolyozzák az értékes vállalati informatikai erőforrásokat, továbbá a vállalati adatokhoz való hozzáférés veszélye miatt is kockázatot jelentenek.
 - A válaszadók 65 százaléka nem képes megelőzni, hogy a rendszer sértetlenségét ellenőrző és vírusirtó szoftverrel nem rendelkező felhasználók hozzáférjenek a vállalati hálózathoz. További 73 százalékuk a biztonsági előírásoknak nem megfelelő végpontok esetében nem tudta megakadályozni abban, hogy azok fertőzéseket terjesszenek vagy megfertőzödjenek.

Tippek a Novelltől – a végpontbiztonsági felügyelet bevált gyakorlatai

A Novell a Threat Assessment felmérés eredményei alapján meghatározta a három legfontosabb végpontbiztonsági gyakorlati tippjét az adatvédelem, a mobil hozzáférés-ellenőrzés és a rendszerintegritás területén.

1. A szervezeteknek először egyszerűsíteniük kell a végpontbiztonsági igényeiket az egyes végpontokon működő biztonsági megoldások egyetlen felügyeleti konzolon való egyesítésével, amellyel csökkenthetik az IT-költségvetést is.
2. Ezután a rendszergazdáknak biztonságossá kell tenniük a mobil végpontokat. Olyan informatikai megoldásokkal kell védeniük az adataikat, amelyek ellenőrzik a cserélhető

adathordozókat, a tárolókat és a wifit használó eszközöket, miközben fenntartják a rendszer sértetlenségét a hét minden napján napi 24 órában – akár kapcsolódnak a végpontok a hálózathoz, akár nem.

3. Végül a hálózati hozzáférés-vezérlő technológia segítségével a szervezetek megelőzhetik, hogy a biztonsági fenyegetések a hálózatra jussanak és más eszközök megfertőzésével akadályozzák az üzletmenetet.

A Novell megoldása – a ZENworks termékcsalád

A Novell ZENworks rendszerfelügyeleti megoldásai a mobil eszközöktől az adatközpontokig biztosítják az informatikai eszközök egységes felügyeletét és minden lehetséges kézi folyamatot automatizálnak, így mentesítik a rendszergazdákat a hosszadalmas, sok hibalehetőséget rejtő manuális munkavégzés alól. A Novell ZENworks Network Access Control például a hálózati hozzáférés-vezérlést további frissítések vagy hálózati elemek beszerzése nélkül valósítja meg, így biztosítja a külső és belső szabályozásoknak való megfelelést. A vállalati biztonság szempontjából fontos, hogy a rendszergazdák tudatában legyenek annak, hogy az egyes felhasználóknál milyen szoftverek lettek sikeresen telepítve. A Novell megoldása erre a problémára a ZENworks Asset Management, amellyel bármikor lekérdezhető a szoftver- és hardverállomány állapota és terhelhetősége. A ZENworks Configuration Managementtel automatizálható az informatikai erőforrások felügyelete, segítségével egységes vállalati házirendek és konfigurációk alakíthatók ki. A ZENworks Patch Management segítségével pedig akár munkaállomások és szerverek százaira is gyorsan és egyszerűen telepíthetők a biztonsági javítócsomagok.

A Novell Treat Assessment felmérésről

A felmérések eredményei a [Novell Threat Assessment Tool](#) internetes tesztre adott válaszokból származnak. A teszt segítségével a rendszergazdák és döntéshozók kiértékelhetik a végpontbiztonsági gyakorlataikat, eljárásaikat és a fenyegetések jelentette kockázatokat. A Novell Threat Assessment Tool ingyenes eszköz használatával a vállalatok beazonosíthatják a sebezhető területeket a cserélhető tárolóeszközöktől a VPN-hálózat használatán keresztül az adattitkosításig és a személyes tűzfalakig. Az eszköz olyan javaslatokat kínál a vállalatok számára, amelyekkel megoldhatják a végpontok sebezhetőségi problémáit. A Novell Threat Assessment eszköz elérhető a <http://www.novell.com/systemsmanagement/secure-desktop/threat-assessment/threatassessment.html> weboldalon.