Teljes körű megfelelés és biztonság

Compliance

A vállalatok napról napra egyre több kihívással szembesülnek a biztonság terén. Egyre bonyolultabb rendszerekben kell fenntartaniuk a biztonságot, és folyamatosan új előírásoknak kell eleget tenniük. A NetIQ és a Novell biztonsági termékei egymást kiegészítve segítenek abban, hogy a szervezetek teljesítsék ezeket a követelményeket és feladatokat.

Bevezetés

A legújabb informatikai trendek minden szervezetet arra kényszerítenek, hogy átalakítsák a vállalati biztonsággal kapcsolatos hozzáállásukat. Az évekkel ezelőtt kialakított biztonsági rendszerek és stratégiák ma már nem állják meg a helyüket a megváltozott körülmények között, például a felhő technológiák terjedése és a mobil eszközök térhódítása mellett, vagy az egyre gyakoribb, nagyvállalatokat és kisebb cégeket egyaránt érintő támadások közepette. Ráadásul folyamatosan csökkenő IT költségvetésből kell fenntartani a biztonságot a megújult feltételek mellett.

A megoldást a teljes átláthatóság és kontroll jelenti. A vállalatoknak a kockázatok kezelésére kell koncentrálniuk, és folyamatosan tisztában kell lenniük azzal, milyen tevékenységeket végeznek a felhasználóik, illetve figyelniük és monitorozniuk kell minden aktivitást a kritikus területeken. Emellett természetesen továbbra is eleget kell tenniük a rájuk vonatkozó előírásoknak is.

Előírások, követelmények

Számos magyarországi vállalat biztonsági stratégiáját meghatározza a 2012-es adatvédelmi törvény, illetve a PCI DSS vagy az ISO27001:2005 szabványok követelményei. A 2013-ban elfogadott, az elektronikus információbiztonságról szóló törvény szintén széles kör számára teremtett új követelményeket, hiszen a teljes hazai közigazgatás mellett érvényes minden olyan társaságra is, amely adatfeldolgozást végez a közigazgatás számára, a nemzeti adatvagyon adatfeldolgozójának számít, vagy kritikus információs infrastruktúrát szolgáltat.

A törvények és szabványok szigorú feltételeket szabnak a szervezeteknek számos területen, amelyek teljesítése komoly kihívásnak számít – ha a szervezet nem rendelkezik a megfelelő eszközökkel és megoldásokkal. A NetIQ Novell SUSE Magyarországi Képviselet a NetIQ és a Novell biztonsági megoldásait integrálja, így egyedi portfólióval kínál megoldást a legfontosabb szabályozásokkal kapcsolatos követelményekre.

Információs rendszerek védelme

Az információbiztonsági törvény, az ISO27001 szabvány és a PCI DSS tanúsítvány is előírja, hogy a szervezeteknek védeniük kell információs rendszereiket. Ebben a feladatban is hatékony támogatást nyújtanak a NetIQ termékei.

A **Secure Configuration Manager** proaktív módon felméri, hogy a rendszerkonfigurációk megfelelnek-e a szabályozási követelményeknek és a bevált gyakorlatoknak. A megfelelőség bizonyítását és az auditokra történő felkészülést riportkészítési funkciókkal támogatja és ezen felül az üzleti felhasználáshoz igazodó kockázatelemzést is biztosít.

A **Change Guardian** szintén aktívan hozzájárul az információs rendszerek védelméhez, hiszen részletes audit információkat biztosít Windows, Linux és Unix platformok alatt egyaránt. A termék valós idejű védelmet biztosít a kulcsfontosságú fájlok és rendszerek számára. Segítségével észlelheti a felügyelet nélküli módosításokat, a kritikus adatokhoz való illetéktelen hozzáférést, az engedély nélküli, kiemelt jogosultságot igénylő tevékenységeket és ezáltal jelentősen csökkentheti az informatikai rendszerekre leselkedő biztonsági kockázatokat.

NetIQ megoldások

- Compliance előírások teljesítése

A 77/2013. (XII. 19.) NFM rendeletben előírt logikai védelmi intézkedések támogatása:

Konfigurációkezelés

- ZENworks Configuration Management

Üzletmenet (ügymenet) folytonosság tervezése

- PlateSpin Forge

Adathordozók védelme

- ZENworks Full Disk Encryption

Azonosítás, hitelesítés

- Access Manager, CloudAccess, MobileAccess
- SecureLogin
- Advanced Authentication Framework
- Privileged User Manager

Hozzáférés ellenőrzése

- Identity Manager
- Access Governance Suite
- Privileged User Manager

Rendszer- és információsértetlenség

- Secure Configuration Manager
- Change Guardian

Naplózás és elszámoltathatóság

- Sentinel Log Manager

Rendszer és kommunikációvédelem

- ZENworks Application Virtualization

Reagálás a biztonsági eseményekre

- Sentinel

Kapcsolódó szabályozások, előírások

- Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény
- 77/2013. (XII. 19.) NFM rendelet
- Adatvédelmi törvény (2011. évi CXII.)
- Információbiztonsági irányítási rendszer (ISO27001:2005)
- PCI DSS szabvány

NetIQ®

A NetIQ és Novell biztonsági termékek széles skálájának és kiterjedt funkcionalitásának köszönhetően a NetIQ Novell SUSE Magyarországi Képviselet kínálja a legátfogóbb, a legfontosabb biztonsági és compliance előírásokra megoldást biztosító portfóliót. A kínálatban minden vállalati és állami ügyfél megtalálja az igényeinek és a rá vonatkozó előírásoknak megfelelő szoftvereket.

www.netiq.hu

Üzletmenet folytonosság tervezése

Az információbiztonsági törvény előírja, hogy a szervezeteknek biztosítaniuk kell az információs rendszer és elemeinek rendelkezésre állását, illetve az ISO 27001 szabvány követelményei között is szerepel az üzletfolytonosság kezelése. Az adatvédelmi törvény szövege pedig azt írja elő, hogy a telepített rendszerek helyreállíthatók legyenek üzemzavar esetén.

A **PlateSpin Forge** tökéletesen ellátja ezeket a feladatokat, mivel Windows és Linux alapú, fizikai és virtuális IT rendszerek védelmére is alkalmas. A „bootolható backup eszköz” alacsony költségek mellett működtethető, egyszerű üzembe helyezést és tesztelést kínál, és nagyszerű RTO és RPO értékeket garantál. Az üzletfolytonosság biztosítását lehetővé tevő, integrált megoldás magában foglalja a tartalékkészüléket, a tárolóterületet és a tükrözési szoftvert egyaránt. Az adatok szükség esetén bármilyen tetszőleges hardverre visszaállíthatók.

Az adatok bizalmassága és sértetlensége

Minden biztonsági előírás kiemelt területként kezeli az adatbiztonságot. Általános elvárás az információ bizalmasságának és sértetlenségének megőrzése, a hozzáférések ellenőrzése, az illetéktelen elérések megakadályozása.

Az adatbiztonság növelésének leghatékonyabb módja a felhasználói jogosultságok integrált és menedzselt kezelése. Az **Identity Manager** a jogosultságok igénylését és jóváhagyását, illetve a felhasználói fiókok létrehozását és megszüntetését automatizálja. Emellett biztonságos jelszófelügyeletet, teljes körű naplózást és a jelenlegi, valamint a múltbeli jogosultságokhoz kapcsolódó keresést és riportkészítést is biztosít.

A **Privileged User Manager** a kiemelt, adminisztrátori jogosultsággal rendelkezdő felhasználók tevékenységének ellenőrzéséről gondoskodik. Kereshető formátumban naplózza a felhasználók teljes aktivitását, akár videófájllal együtt. Az előzetesen rögzített tevékenységekre kockázatelemzést végez, valamint a naplózás és a kockázatok értékelése során központi irányelvek alkalmazására is van lehetőség. A Windows, Linux és UNIX környezetek megfigyelésére egyaránt alkalmas megoldás hozzájárul a megfelelőség igazolásához is.

Rendszeres ellenőrzés

Az információbiztonsági törvény előírja, hogy a szervezetek vezetői rendszeresen végrehajtott biztonsági kockázatelemzéseken, ellenőrzéseken és auditokon keresztül kötelesek meggyőződni arról, hogy a szervezet elektronikus információs rendszereinek biztonsága megfelel a jogszabályoknak és a kockázatoknak. Ilyen jellegű felmérést azon vállalatoknak is érdemes végezniük, amelyekre nem vonatkozik az adott törvény, hiszen a biztonság folyamatos fenntartásáról csak így győződhetnek meg.

Az ellenőrzésben hatékony segítséget nyújt az **Access Governance Suite**, amelynek segítségével felmérhetők és hitelesíthetők a hozzáférések. A megoldás egységes irányítási modellt és rugalmas beállítási lehetőségeket kínál. A jogosultsági adatok az üzleti jóváhagyók számára is érthető megfogalmazásban férhetők hozzá, ami megkönnyíti az ellenőrzési, jóváhagyási és a hitelesítési folyamatokat.

Naplózás és elszámoltathatóság

A minden informatikai eseményt rögzítő naplófájlok emberi feldolgozásra alkalmatlan halmazában a Sentinel Log Manager leegyszerűsíti az események begyűjtését, a logok életciklusának kezelését és a jelentések készítését. A **Sentinel Log Manager** az egyszerű üzembe helyezés érdekében nagy számú beépített kollektorral és előre konfigurált jelentéssel érkezik, és így hatékonyan teljesíthetők a naplóállományok kezelésére és az ezekből származó adatok előállítására vonatkozó biztonsági előírások követelményei.

Reagálás a biztonsági eseményekre

A hatalmas mennyiségű adathalmaz állandó ellenőrzése és elemezhetősége szempontjából a hangsúly az automatizáláson, az események és a megfelelőséget sértő tevékenységek azonnali automatikus kezelésén van. A **Sentinel** (a Sentinel Log Manager által biztosított és az előző paragrafusban ismertetett szolgáltatások mellett) képes a biztonsági eseményfolyam valós idejű megjelenítésére és elemzésére is. Felismeri a rendellenességeket és a behatolási kísérleteket, egy esetleges incidens esetén azonnal és automatikusan megteszi a szükséges válaszlépéseket, és így gyorsan elháríthatók a támadások.

Keresse meg helyi megoldásszállítóját, vagy vegye fel a kapcsolatot a NetIQ magyarországi képviseleti irodájával az alábbi elérhetőségek valamelyikén:

MOM Park, SAS torony
1124 Budapest, Csörsz u. 45.
Tel: +36 (1) 489-4600
Fax: +36 (1) 489-4601
info@netiq.hu
www.netiq.hu

NetIQ | Novell | SUSE

NetIQ