

Informatikai intelligencia

Novell Sentinel

Az informatikai megoldások folyamatos fejlődése, bővülése, az összetett alkalmazások térnyerése és a hálózatok kialakulása révén a biztonság kérdése is bonyolultabbá válik egy vállalat életében. Az informatika világában sokszor történnek előre nem látható események; bármikor érheti külső vagy akár belső támadás a napjainkban már egyre összetettebb informatikai rendszereket komoly anyagi károkat okozva ezzel a vállalatoknak. Tovább bonyolítja a kérdést az előírásoknak, törvényi szabályozásoknak való megfelelési kötelezettség, hiszen így egy szervezet olyan komplex megoldást igényel, amely integráltan magába foglalja a biztonsági eseményeket, a rendszer, a személyazonosság és a hozzáférés kezelését egyaránt.

A vállalatoknak „Informatikai Intelligencia” rendszerre van szükségük, amely biztosítja számukra a magas rendelkezés-reállást és üzletfolytonosságot. Ahhoz pedig, hogy ez a biztonság elérhetővé váljon, olyan megoldást kell bevezetniük, amelynek segítségével azonnal és jól látható minden a hálózatban történő folyamat, továbbá hatékonyan elháríthatók az esetleges incidensek és az ellenőrzéseket végzők jól követhetik, hogy az IT rendszer a szabályozásoknak megfelelően működik-e.

Ennek megvalósításához követelhetünk szigorúbb előírásokat, alkalmazhatunk több biztonsági szakembert, de mindezeknek jelentős költségvonzata van. Célszerűbb olyan informatikai eszközöket igénybe venni, amelyek alkalmasak szabálykésztésre, monitorozásra és a szokatlan események jelzésére egyaránt. A piacon számos ilyen megoldás létezik, de a cikkünkben bemutatott Novell Sentinel, amelyet több nemzetközi nagyvállalat, közöttük a világ legnagyobb hírszerző hivatala, a CIA is évek óta használ, teljeskörű megoldást kínál mindehhez. Használatával jól láthatóvá válik minden hálózatban lejátszódó folyamat, így a termék előnyeit a vállalatok informatikai- és a biztonságért felelős szakemberei egyaránt kihasználhatják a saját területeiken.

A Sentinel további előnye, hogy használatával az egyre összetettebb törvényi szabályozásoknak, különböző követelményrendszereknek, szabványoknak, ajánlásoknak (példul Sarbanes-Oxley (SOX) törvény szigorú előírásainak, a Bazel II-nek, illetve a PSZÁF auditoknak) való megfelelés biztosítottá válik.

A Novell Sentinel használatából adódó lehetőségek a biztonság és üzemeltetés-támogatás területén. A jelenleg használatos logelemző projektek 30 százaléka foglalkozik csak a biztonság problémájával, a fennmaradó 70 százalékot az üzemeltetés-támogatás és monitorozás teszi ki (pl. disc betelésének előrejelzése, üzletbiztonság, egyéb összefüggések vizsgálata).

> Üzemeltetés-támogatás és monitoring

A logokat eddig csak utólag elemezték, a Novell Sentinelnek köszönhetően viszont az előzetes monitorozás lehetősége miatt eleve megelőzhetjük a problémákat. Ez rendkívül fontos, hiszen nem csak akkor állhatunk neki a probléma megoldásnak amikor a rendszer már leállt, hanem korábban, ezáltal zavartalan munkafolyamatot biztosíthatunk és bevételkieséssel sem kell számolnunk.

A Sentinel összeveti a szervezet teljes hálózati infrastruktúrájából származó, biztonsággal kapcsolatos és egyéb információkat. Ilyen információk többek között a személyazonosság- és hozzáférés-kezelési termékek - Novell Identity Manager és a Novell Access Manager - adatai, valamint a külső fejlesztői rendszerekből és eszközökből származó adatok. A Sentinel segít rendszerezni a begyűjtött információkat, azonosítja a biztonsági és megfelelési problémákat, nyomon követi a hibajavítási műveleteket. Emellett

jelentősen leegyszerűsíti a korábban munkaerő-igényes és hibalehetőségeket rejtő folyamatokat, ezáltal a felhasználók szigorúbb, előre látható biztonság- és megfelelés-figyelési programot építhetnek fel. A Sentinel 6 a Novell Identity Manager 3.5 és a Novell Access Manager 3 termékekkel együtt integrált személyazonosság-kezelő és biztonságfelügyeleti megoldást nyújt a vállalati ügyfelek számára, amely a törvényi szabályozások mellett támogatja a kormányzati előírásoknak való megfelelést is.

> A Biztonság területe

Nagyvállalati környezetben hatalmas mennyiségű adathalmazt tárolnak. Ezeknek az adatoknak az állandó ellenőrzése és elemezhetősége kardinális kérdés, mivel az értelmezhetetlen adatok tömege olyan, mintha a vállalatnak nem is lennének adatai. Ha tehát a biztonságról beszélünk, könnyen megállapíthatjuk, hogy ebben az esetben a manuális ellenőrzés nem működik és a megoldást az adatok online formában történő elemzése jelentheti. A hangsúly ma már az automatizáláson és az eredmények jelentésén, illetve az események és a megfelelést sértő tevékenységek azonnali automatikus

A Novell Sentinel megoldása nemcsak egy riportolási lehetőség, hanem a szabályok kikényszerítésének és a megfelelőség biztosításának az eszköze is.

Használatával lehetővé válik a rendszer SLA-k szerint szabályozott üzemeltetése.

kezelésén van, hiszen az ellenőrzés nagyszerű dolog, de az igazán hatékony megoldás a folyamatos riportolási lehetőségben rejlik. A Novell Sentinel megoldása pont ezekre a kérdésekre ad azonnali választ, mert a rendszer nagy teljesítménye elősegíti az azonnali adatgyűjtést és összevetést akár másodpercenként több ezer legújított eseményből is. Így a valós idejű események összevetése és az ezekre történő gyors reagálás nagy segítséget nyújt a szervezetnek ahhoz, hogy elkerülje a biztonsági résekkel kapcsolatosan a jelentős és váratlan kiadásokat.

> Összegzés

A zavartalan üzletmenet legfontosabb kérdése az elektronikusan tárolt adatok biztonságában rejlik, hiszen az adatvesztés jelentős anyagi és versenyhátrányhoz juttathat egy vállalatot. Ezért nem szabad megfeledkezni arról, hogy az informatikai rendszerek üzemeltetésénél az adatvesztések megelőzésének költsége töredéke a kárelhárítási költségnek. Napjaink előírásainak, törvényi feltételeinek való megfelelés is egyre bonyolultabb, így a vállalatok olyan komplex megoldásokat igényelnek, ame-

lyek a biztonsági eseményektől kezdve a személyazonosság- és hozzáférés kezelést egyaránt magukban foglalják. A vállalatoknak tehát egy „Informatikai Intelligencia” rendszerre van szükségük, amely azonnali visszacsatolásaival biztosítja a magas rendelkezésreállást és üzletfolytonosságot. A Novell Sentinel az „Informatikai Intelligencia” eszköze, az egyetlen olyan információbiztonsági termék a piacon, amely magas szintű átláthatóságot biztosít és az emberi erőforrásokat, a rendszereket és folyamatokat egyszerre felügyelő, valós idejű, átfogó megfelelőségi megoldást nyújt a szervezetek számára. **N**

A Sentinel a biztonsági és eseményfigyelési, valamint reagálási és jelentéskészítési képességek segítségével teljes mértékben együttműködik a Novell platformjával, többek között a SUSE Linux Enterprise Server rendszerrel és a személyazonosság-kezelési megoldásokkal.

A Novell a termék új frissítésével jelentősen leegyszerűsíti a korábban munkaerő-igényes és hibalehetőségeket rejtő folyamatokat, ezáltal a felhasználók szigorúbb, előre látható biztonság- és megfelelőség-figyelési programot építhetnek fel.

A Kürt Zrt. biztonsági szakértőjének véleménye a Novell Sentinelről



Frész Ferenc, a Kürt Zrt. Biztonsági Intelligencia Központjának vezetője az információbiztonsági piac helyzetéről, illetve a Novell Sentinellel kapcsolatos tapasztalatairól nyilatkozott.

> Mivel foglalkozik a Kürt Zrt.?

A Kürt Zrt. 18 éve van jelen az informatikai piacon, nemzetközileg elismert adatmentő, tanácsadói, illetve rendszer-integrátori üzletággal rendelkezik. A cég a 90-es évek végétől foglalkozik biztonsági rendszerek felépítésével és szakértői tanácsadással.

Két éve létrehozta a Biztonsági Intelligencia Központját, amely legális hackelés, network-forensics, valamint logelemzés szolgáltatást nyújt ügyfeleinek.

> Hogyan látja az informatika területén belül a biztonság, illetve az üzemeltetés-támogatás területének jelenlegi helyzetét?

Ma az informatikai biztonság területén a vállalatok ugyan heterogén képet mutatnak, de a legtöbbet már megtették biztonságukért. Olyan védelmi rendszereket építettek, amelyek hatékonyan hárítják el a külső támadásokat és az adatvesztéseket. Az informatikai biztonság iránti növekvő igény olyan komplex rendszereket eredményezett, amelyeket az egyre kevesebb informatikussal nehéz üzemeltetni. Ezért a hardver- és szoftvergyártók üzemeltetés-támogató és biztonsági monitoring rendszereket hoztak létre, hogy a kritikusnak ítélt eseményekre időben és célzottan tudjanak válaszolni. Ilyen céllal készült a Novell Sentinel is, amely a rendszer eseményeinek összegyűjtését és valós idejű monitorozását, elemzését végzi.

> Milyen tapasztalatai vannak a Novell Sentinellel kapcsolatban?

A Novell Sentinellel olyan esemény-monitorozó és elemző funkció építhető fel az informatikai rendszer „felett”, amely valós időben gyűjti össze a különböző szerverek, tűzfalak, alkalmazások eseményeit, magállapítja az események közötti összefüggéseket, valamint automatikus jelentéseket készít és küld. A rendszer működése a klasszikus üzemeltetés-támogató eszközökhöz hasonlóan előre beállított értékeken alapul, de fejlett, tanítható értelmező motorjának köszönhetően, dinamikusan követi az informatikai rendszer állapotváltozásait. Platformfüggetlensége lehetővé teszi bármely operációs rendszer, valamint a legtöbb relációs adatbázis technológia használatát. Az első tapasztalatok szerint a szabványos, jól ismert eszközök, operációs-rendszerek és alkalmazások eseményeit is kezeli, a kevésbé ismert, vagy egyedi alkalmazások, rendszerek logállományaira pedig könnyedén lehet értelmezőket belefejleszteni, hiszen az esemény-értelmező motor tanítható.

> Ön szerint milyen előnyökkel jár egy vállalat számára a „Novell Sentinel Informatikai Intelligencia Megoldások” használata?

A Novell Sentinel használatával egy vállalat nagymértékben növelheti a komplex informatikai rendszerek üzemeltetésének és hibaelhárításának hatékonyságát. Ha a Sentinel intelligenciáját az adott rendszer elemzésének szolgálatába állítják, úgy nem szükséges plusz humánerőforrás bevonása a biztonsági események kezelésére, hiszen a problémák felderítése felautomatikusan, a jelzések, riasztások teljesen automatikusan zajlanak. További előnyt jelent, hogy egy jól kidolgozott eseménykezelői, incidenskezelési munkafolyamat idővel csaknem az összes lehetséges biztonsági eseményre reagál majd. A rendszer jól támogathatja a különböző fejlesztéseket, integrációs folyamatokat, valamint a szabályzatok működésének monitorozását, és elengedhetetlen a különböző szabványügyi, pénzügyi, audit jellegű előírások területén.