Connection

Novell Connection Magazin
VII. ÉVFOLYAM 1. SZÁM/2007

A Novell átfogó biztonsági megoldásai

A Novell biztonságfilozófiája

Hozzáférés-kezelés a Novell Access Managerrel

Jogosultság-kezelés: Novell Identity Manager

PC-biztonság a SecureWave Sanctuary Suite-tel

Informatika az őrtoronyban: Sentinel

Kiút a jelszavak útvesztőjéből: Novell SecureLogin 6.0

Novell

RACIONALIZÁLJA INFORMATIKAI KÖLTSÉGEIT!

Az Open Workgroup Suite Linux alapú változata most rendkívül kedvező áron kapható, és a termékhez akár

18 366 Ft*

felhasználónkénti áron is hozzájuthat.

*Az árak tájékoztató jellegű nettó végfelhasználói listaárak, és 260 HUF/EUR árfolyamon lettek megállapítva.
További információért keresse helyi Novell-megoldás szállítóját, vagy forduljon a Novell irodához az (1) 489-4600 vagy az (1) 489-4612 telefonszámon.

A csomag komponensei:

Open Enterprise Server
Nagyteljesítményű Linux alapú kiszolgáló.

GroupWise 7
Teljes értékű csoportmunka megoldás.

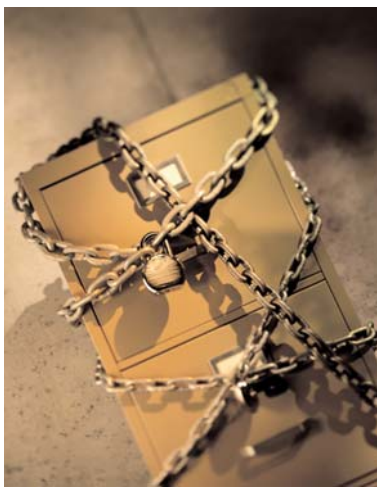
ZENworks 7
Hatékony rendszerfelügyeleti szolgáltatás.

OpenOffice for Windows Novell Edition
MS Office formátumokat kezelő irodai programcsomag.

SUSE Linux Enterprise Desktop
Teljes értékű irodai munkahely.

Novell Connection Magazin
2007/1. SZÁM


6

10


22


Online: novell.com/hungary/novellconnection

Beköszöntő

Rendszeresen olvashatunk a vezető elemző társaságok előrejelzéseiről, amelyek szerint a Linux jövője, robbanásszerű fejlődése elkerülhetetlen és ezt már a korábban bejelentett – és nagy meglepetést okozott – Microsoft és Novell által aláírt megállapodás is bizonyítja. Egy felmérés szerint a megállapodást az ügyfelek 95 százaléka üdvözölte, és az ebből származó előnyöket elsőként kihasználó vállalatok között van az AIG Technologies, a Deutsche Bank AG, a Credit Suisse és a Wal-Mart Stores Inc. A PSA Peugeot Citroen is a Novell megoldásainak bevezetése mellett döntött, így a jövőben 20 000 SUSE Linux Enterprise Desktop asztali operációs rendszert és 2 500 SUSE Linux Enterprise Servert telepítenek Európa második legnagyobb autógyártójánál. A Linux hazai előretörésének érdekében régió szintű stratégiai együttműködésről állapodtunk meg a Synergon Informatika Nyrt.-vel, Magyarország egyik vezető rendszerintegrátorával, amelynek értelmében a vállalat az elsők között veszi fel stratégiai platformjai közé a Linuxot és ami a legfontosabb, a Novell SUSE Linux technológiáját, illetve terméktámogatási hátterét tartja a legerősebbnek a piacon. Az elmúlt hónapokban a fejlesztés irányába is jelentős lépéseket tettünk, hiszen a Mono projekt tagjaként bejelentettük a Visual Basic fordító elérhetőségét, amely lehetővé teszi a fejlesztők számára a Microsoft Visual Basic programozási nyelven írt alkalmazásaik többféle platformon való használatát a forráskód módosítása nélkül.

Kellemes és hasznos informálódást kívánok!

Szittya Tamás
ügyvezető igazgató

TARTALOM

Ingyenes terjesztésű kiadvány
Novell Connection – A hálózati szakértők magazinja
Novell Kft. MOM Park, Sas torony, 1124 Budapest, Csörsz utca 45. Tel.: 36 1 489-4600; E-mail: info@novell.hu; www.novell.hu
Felelős kiadó: Szittya Tamás – Felelős szerkesztő: Hargitai Zsolt – A kiadványt gondozta: Sásdi Gábor – Fordítási és egyéb munkák: Morpho Communications.

Connection a Világgal

> Korábban elképzelhetetlen szintű nyílt forráskódú fejlesztések Magyarországon és a régióban
A Novell Magyarország és a Synergon Informatika Nyrt., Magyarország egyik vezető rendszerintegrátora régió szintű stratégiai együttműködésről állapodott meg a nyílt forráskódú technológia támogatására. A bejelentés értelmében mostantól a Linux – a nyílt forráskódú technológia – a Synergon egyik fontos stratégiai platformjává válik, mint a jövőbeni fejlesztések egyik alapja, és mindehhez stratégiai partnere a Novell és annak vezető Linux technológiája a SUSE Linux Enterprise. A vezető elemző társaságok előrejelzése szerint a Linux jövője, robbanásszerű fejlődése elkerülhetetlen és ezt már a Microsoft és a Novell által aláírt megállapodás is tovább segíti. Ezért a Synergon fejlesztéseit az ügyfél-igényeknek megfelelően nyílt forráskódon is piacra viszi. A Novell Magyarország és a Synergon Informatika együttműködése Magyarország mellett a régióra is kiterjed, hiszen mindkét társaság regionális irányító szerepet is ellát. Ennek köszönhetően a két társaság a nyílt forráskódú fejlesztések magas megtérülésére számít, hiszen a fejlesztések könnyen lokalizálhatók és implementálhatók a környező országokban is. N

> A Novell bemutatta legújabb nyílt vállalati megoldásait a BrainShare 2007 konferencián
A Novell évente megrendezendő BrainShare konferenciáján bemutatta nagyvállalati felügyeleti megoldásait Linuxra és vegyes platformokra. Bejelentésre kerültek többek között Linux-disztribúciójának frissítései – például egy vékony klienstermék -, egy új Linux felügyeleti megoldás és a Novell Open Enterprise Server 2 nyílt bétaverziója. A vállalat ismertette továbbá vezető biztonsági és személyazonosság-kezelési megoldásainak frissítéseit, és az új csoportmunka-eszközöket. N

> A Novell Open Workgroup Suite további előnyöket kínál az ügyfeleknek
A Novell Open Workgroup Suite segítségével világszerte számos vállalat és intézmény csökkenti költségeit és használja ki a nyílt forráskódú szoftverek nyújtotta rugalmasságot. A programcsomag minden olyan szolgáltatást biztosít, ami egy korszerű irodai infrastruktúra kialakításához szükséges, és a legfontosabb szerver oldali szoftverektől kezdve a teljes értékű irodai munkaállomásig minden lényeges alkalmazást tartalmaz. Az új Value Pack program más gyártóktól származó szoftvertermékekre is jelentős kedvezményeket kínál, a Novell Magyarországnál pedig 2007. június 29-ig minden eddiginél kedvezőbb áron érhető el a termékcsomag. N

> Automatizált munkaállomás felügyeleti megoldás a Novelltől Microsoft hálózatokhoz
A Novell ZENworks Configuration Management jelentősen leegyszerűsíti a Windows operációs rendszerek, többek között a Vista munkaállomás-felügyeletét. Az új megoldás a zökkenőmentes felügyelethez biztosít előnyöket függetlenül attól, hogy milyen a környezet. A Microsoft Active Directory és a Novell eDirectory címtárakkal egyaránt integrált Novell ZENworks Configuration Management az első olyan termék a piacon, amely valós idejű, személyazonosság-alapú rendszerfelügyeletet tesz lehetővé a hatékonyabb szolgáltatásnyújtás és a megfelelő munkaállomás-konfiguráció biztosítása érdekében. N

> Virtualizáció SUSE Linuxon SAP alkalmazásokhoz
A Novell elérhetővé tette a Xen virtualizációs technológiát is tartalmazó Novell SUSE Linux Enterprise Server 10-et az SAP NetWeaver és mySAP Business Suite rendszerekhez. A Novell és az SAP által közösen tesztelt, Xen virtualizációs megoldással kiegészített SUSE Linux Enterprise Server teljes mértékben megfelel az SAP virtualizált környezetekben futó SAP-alkalmazásokkal szemben támasztott szigorú követelményeinek. Ezzel az új, ellenőrzött megoldással, a SUSE Linux Enterprise Server használatával az ügyfelek könnyedén telepíthetik SAP-alkalmazásaikat virtualizált környezetbe, így megbízhatóbb, rugalmasabb és költséghatékonyabb platformmal támogathatják a kulcsfontosságú számítástechnikai tevékenységeket. N

> Több mint 20 000 asztali gépéhez vásárolt Novell SUSE Linuxot a PSA Peugeot Citroën
A PSA Peugeot Citroën, Európa második legnagyobb autógyártója és a Novell több évre szóló szerződést írt alá. A megállapodás keretében a Novell 20 000 SUSE Linux Enterprise Desktop asztali operációs rendszer és 2 500 SUSE Linux Enterprise Server telepítését biztosítja az óriásvállalat részére. A francia autógyártó óriásvállalat a költségcsökkentési lehetőségre, a könnyű használhatóságra, az integrációra és a széleskörű támogatásra hivatkozva váltott Linux asztali rendszerre. N

> Az ügyfelek támogatják a Microsoft és a Novell közötti együttműködést
A technológiai döntéshozók körében végzett független felmérés szerint az ügyfelek támogatják a Microsoft Corp. és a Novell Inc. között november elején kötött üzleti és műszaki megállapodást, amelynek célja a Windows és a Linux rendszerek közötti együttműködés fejlesztése. A válaszadók többsége egyetért a megállapodás kiterjesztésével és hatékonyan együttműködő termékeket, valamint a Windows és Linux rendszereket is tartalmazó vegyes forráskódú környezetek felügyeletét leegyszerűsítő eszközöket szeretne használni. A megkérdezettek több mint háromnegyede fontosnak tartja a vezető Linux-disztribútorok és a Microsoft szorosabb együttműködését, 67 százalékuk pedig nagyobb valószínűséggel a Novell SUSE Linux Enterprise termékét választaná adatközpontjában. A felmérést a Microsoft és a Novell közös megbízásából a Penn, Schoen & Berland Associates Inc., egy elismert független piacelemző cég készítette. N

> Megjelent az új Mono Visual Basic fordító
Az új Mono Visual Basic fordító lehetővé teszi a fejlesztők számára a Microsoft Visual Basic programozási nyelven írt alkalmazásaik többféle platformon való használatát a forráskód módosítása nélkül. Az új Mono Visual Basic fordító segítségével a fejlesztők továbbra is a megszokott Visual Basic/Visual Studio környezetben dolgozhatnak. A forráskód lefordítását követően pedig számos különböző platformon és architektúrán – többek között a Windows, Linux és Mac OS rendszereken – futtathatják a programot. A Mono hatékony és rugalmas megoldást kínál, így lehetővé teszi, hogy a fejlesztők és az ügyfelek maximálisan kihasználhassák a számukra fejlesztett szoftverek biztosította előnyöket saját szervezeteiken belül. N

> Újabb három vállalat részesül a Microsoft és a Novell együttműködésének előnyeiből
A Novell ügyfelei közül a Deutsche Bank AG, a Credit Suisse és az AIG Technologies az elsők között részesül a Microsoft Corp. és a Novell Inc. – Windows és Linux rendszerek együttműködését javító – széles körű üzleti és műszaki megállapodásának eredményeiből. A Microsoft három különálló ügyfél-megállapodás keretében mindegyik vállalat részére SUSE Linux Enterprise előfizetési tanúsítványokat biztosít, így lehetővé teszi számukra a Microsoft és a Novell között született megállapodás előnyeinek kihasználását. A Credit Suisse, a Deutsche Bank és az American International Group Inc. tagjaként működő AIG Technologies hangsúlyozza, hogy az együttműködés legfőbb előnyei, a szabadalmi együttműködési megállapodás és a kétirányú virtualizációs megoldásokra vonatkozó tervek döntő tényezők voltak választásuk során.
A Novell és a Microsoft között létrejött széles körű üzleti és műszaki megállapodásról további információt a http://www.novell.com/hungary/news/061108_microsoft_novell_agreement_h.html weboldalakon talál. N

> Erősödik az OpenOffice.org és a Microsoft Office közötti együttműködés
Az OpenOffice.org irodai programcsomag Novell kiadása támogatta a Microsoft Office Open XML formátumot, így javult az együttműködés az OpenOffice.org és a Microsoft Office következő generációja között. A Novell a Microsofttal és más vállalatokkal együttműködve dolgozott azon a projekten, melynek célja kétirányú nyílt forrású fordítók létrehozása az OpenOffice.org és a Microsoft Office szöveges dokumentumai, táblázatai és prezentációkészítői között. A szöveges dokumentumokhoz készült fordítóprogram 2007. január végén megjelent. A fordítóprogramok beépülő modulként elérhetőek a Novell OpenOffice.org termékéhez. A Novell nyílt forrásúként jelentette meg azt a kódot, amely az Open XML formátumot a Novell OpenOffice termékkel kompatibilissá teszi, és javasolta, hogy az OpenOffice.org projekt része legyen. Így a felhasználók könnyebben oszthatják meg fájljaikat a Microsoft Office és az OpenOffice.org között, hiszen a két irodai programcsomag dokumentumai egységesebben jelenítik meg a formátumokat, képleteket és stílussablonokat. N

> A Gartner szerint a Novell a hozzáférés-kezelés területének egyik vezető szállítója
A Novell hozzáférés-kezelési megoldásának következő generációs változata, a Novell Access Manager 3 biztosítja a tágabb értelemben vett vállalati környezet, azaz az ügyfelek, partnerek és alkalmazottak problémamentes, biztonságos hozzáférését a web alapú tartalomhoz és vállalati alkalmazásokhoz – a biztonsági szint és az információk elérhetőségének korlátozása nélkül. Problémamentesen integrálja a Novell biztonsági megoldásait, amelyekkel csökkenthetőek a kockázatok és fellendíthető az ügyfelekkel és partnerekkel való kapcsolattartás. A Novell Access Manager platformok és címtárszolgáltatások széles körét támogatja, és megfelelő rugalmassággal kezeli akár a legbonyolultabb multinacionális vállalat informatikai környezetét is. A Gartner Inc. a 2006 második félévére vonatkozó, a webes hozzáférés-kezelést vizsgáló Magic Quadrant jelentésében a Novellt a vizsgált terület egyik vezető szállítójának minősítette. N

> A Novell innovációkkal segíti a nyílt forráskódú fejlesztést
A Novell a teljes nyílt forráskód közösség számára elérhetővé tette az openSUSE™ Build Service innovatív keretrendszert és a KIWI rendszerképkészítő eszközt. Az openSUSE™ Build Service egy komoly infrastrukturális hátteret biztosít a szoftverfejlesztők számára, amellyel a különböző Linux-disztribúciókhoz könnyedén létrehozhatják és lefordíthatják szoftvercsomagjaikat. A KIWI képkezelő eszköz segítségével pedig futtatásra alkalmas adathordozókat, például Xen virtuális képeket hozhatnak létre. A nyílt forráskódú megoldások fejlesztői az openSUSE Build Service által biztosított infrastruktúrával gyorsabban és könnyebben állíthatják elő programjaik különböző platformokra és disztribúciókra optimalizált változatát, valamint elkészíthetik az igényeiknek megfelelő, testre szabott Linux-disztribúciót. A fejlesztők munkáját a későbbiekben is jelentősen támogatja, hogy a futtató környezet frissítése (például új openSUSE verzió megjelenése) esetén a Build Service automatikusan legenerálja a fejlesztő kódját az új verzióra is. N

> Továbbfejlesztett Windows virtualizáció Linuxon
A Novell és az Intel Corp. elérhetővé tették paravirtuális hálózati és blokkeszköz-illesztőprogramjaikat. A közösen fejlesztett illesztőprogramok alkalmazása lehetővé teszi a felhasználók számára a Microsoft Windows Server 2000/2003/XP módosítás nélküli futtatását Xen virtuális környezetben a Novell SUSE Linux Enterprise Server 10 rendszerén és az Intel Virtualization Technology megoldást tartalmazó kiszolgálóplatformokon egyaránt. Az ügyfelek mostantól a módosítás nélküli Linux vendég operációs rendszer SUSE Linux Enterprise Server feletti futtatása mellett biztonságosan válthatnak át újabb és energiatakarékosabb kiszolgálóra, régebbi Windows és Linux megoldásaikat virtuális kiszolgálókra konszolidálva. A Windows SUSE Linux Enterprise Server feletti virtualizálása jelentős költségcsökkentést eredményez, az illesztőprogramok pedig javítják a Windows- és Linux-telepítések rendelkezésre állását fürtözött virtuális rendszerek használatával. A Novell az ügyfelei számára kísérleti virtualizációs programot indított, és nagyvállalati szintű támogatást nyújt a teljesen virtualizált Windows 2000/2003/XP telepítések SUSE Linux Enterprise Server rendszeren történő futtatásához. N

CIO

A természet adta lehetőségek kézzelfogható megoldásai

A Novell biztonságfilozófiája - és ami mögötte van…

Dr. Jeffrey Jaffe, a Novell elnökhelyettese és műszaki igazgatója blogjában összegezte gondolatait a biztonságról, hozzáférés-felügyeletről és személyazonosság-kezelésről


N®

A Novell biztonságfilozófiája – és ami mögötte van…

Dr. Jeffrey Jaffe, a Novell elnökhelyettese és műszaki igazgatója blogjában összegezte gondolatait a biztonságról, hozzáférés-felügyeletről és személyazonosság-kezelésről

> Mi áll a Novell biztonsági stratégiájának hátterében?
Definiáljuk újra a személyazonosság-kezelést, és emeljük egy új, relevánsabb szintre: a cégvezetés szintjére. A változás folyamatának megértéséhez azonban érdemes áttekintenünk a hozzáférés-felügyelet, valamint a személyazonosság-kezelés történetét.

> A személyazonosság-kezelés egyre növekvő szerepe
A hozzáférések ellenőrzése korábban nagyon könnyű feladat volt. A jelszó-mechanizmusok egyszerű csoportja biztosította, hogy egy számítógéphez, egy alkalmazáshoz vagy egy erőforráshoz kizárólag az arra jogosult személyek férhessenek hozzá.
Azóta e terület számos tekintetben sokat fejlődött. A változások akkor kezdődtek, amikor még az IBM üzleti biztonsággal foglalkozó SecureWay egységének vezérigazgatója voltam, az 1990-es évek végén. Azóta ez a piaci szegmens folyamatosan növekszik. A biztonsági tokenek megjelenésével elterjedt a hálózatba való betörések elleni védekezés. Számos megközelítést használtak a hozzáférések ellenőrzésének egyszerűsítésére: egypontos bejelentkezés (több alkalmazásban), címtáron alapuló megoldások a belépési jogok kezelésének megkönnyítésére, és metacímtárak, amelyek összehangolják a különböző címtármegoldásokat.

Napjainkban az informatika már másként tekint a hozzáférés ellenőrzésére. Maga a hozzáférés-ellenőrzés kifejezés azt sugallja, hogy létezik egy erőforrás és egy felügyeleti ügynök, amely a hozzáférést ellenőrzi. Ennélfogva az eredeti nézet középpontjában az erőforrás áll.

Az alkalmazási terület kibővülése azonban megváltoztatta a középpontot. Az erőforrásokhoz való hozzáférést nyilvánvalóan ellenőrizni kellett, de az erőforrásokra koncentrálva a vállalatok elhanyagolták a problémák egy jóval szélesebb körét. A lingua franca (közvetítő nyelv) többé már nem a felhasználó, a hozzáférés és az erőforrás. Most már szerepekről és munkafolyamatokról, a házirendnek való megfelelés automatikus ellenőrzéséről és az alkalmazásprogramozási felületek (API) egyre hangsúlyosabb szerepéről van szó. Ezek a kifejezések a hozzáférés ellenőrzését a vállalat belső működéséhez kapcsolják. Az olyan személyazonosság-kezelő rendszerek, mint a Novell vezető terméke, az Identity Manager 3 (IDM3) népszerűvé váltak a vállalatok körében. Az olyan hozzáférés-vezérlési termékek pedig, amelyek „nem követik a programot”, kezdenek eltűnni.

> Személyazonosság-kezelés: ellenőrzési pont a vállalat informatikai vezetőinek
Ebben az összefüggésben a személyazonosság-kezelés túllép korábbi mellékes szerepén az informatikában: fő ellenőrzési ponttá válik, mivel egy vállalat alkalmazás felügyeletének körébe tartozik.

Ez számos közvetlen következménnyel jár:
1. A személyazonosság-kezelő rendszer kiválasztása az informatikai vezetők döntési jogköre lesz. A kiválasztott infrastruktúra minden alkalmazást érint, egy-egy alkalmazás kiegészítésére, utólagos módosítására nincs lehetőség.
2. A személyazonosság-kezelés stratégiáit az egész vállalatra kiterjedően kell megtervezni, az üzleti stratégiák tervezésével egyidőben.
3. A személyazonosság-kezelési megoldás szállítója nem feltétlenül azonos az alkalmazás szállítójával. Mindez rugalmasságot biztosít alkalmazások közötti választásban. Ha a személyazonosság-kezelés túl szorosan kapcsolódik egy alkalmazáshoz, az informatikai szervezet több különböző személyazonosság-kezelő rendszert alkalmaz majd, vagy korlátozzák az alkalmazás szállítójának megválasztását.
4. A személyazonosság-kezelő infrastruktúra nem függhet egy meghatározott, alapvető operációs rendszertől, hanem támogatnia kell minden népszerű operációs rendszert.

> A személyazonosság-kezelés folyamatos bővülése a cégvezetés felé irányul
Véleményem szerint a szoftver-infrastruktúra kialakítása fontos terület a cégvezetés problémájának kezelése során, hiszen számos olyan tétel, amelyet a cégvezetés nyomon követ és amelyről jelentést készít, az informatikai infrastruktúrában is szerepel. Hiba lenne az alapoktól kezdeni mindent. A szükséges architektúra alapjainak nagy része már létezik a személyazonosság-kezelő termékekben. A cégvezetés döntési területei közé tartozik és az architektúra egyik legfontosabb alapja: a dolgozókat érintő infrastruktúra. A felhasználók, illetve az alkalmazottak jelentik az alapot a megfelelőségi jelentésekhez és a vezetéshez. A személyazonosság-kezelő rendszerek az alkalmazottakkal foglalkoznak. A gazdagabb címtár-infrastruktúrával rendelkező rendszerek – természetesen – hatékonyabban működnek. Az architektúra másik kulcsfontosságú alapja az a munkafolyamat, amely néhány személyazonosság-kezelő termékben – például a Novell Identity Manager 3 termékében – eredetileg is megtalálható. A Novellnél erre különösen büszkék vagyunk. Az architektúra további alapja az eseményfelügyelet, amely az informatikai infrastruktúra üzleti tevékenységben betöltött szerepét vizsgálja. Ez egy olyan alrendszer, amely kiváló teljesítményt nyújt a felhasználófelügyelet, a munkafolyamat és a rendszerfelügyelet terén, valamint biztosítja, hogy a független szoftverszállítók és a társaság fejlesztői új megfelelőségi vagy irányítási alkalmazásokat hozzanak létre a rendszerek infrastruktúrája számára.

> A hiányzó rész: eseményfelügyelet
Az e-Security felvásárlásával a Novell nem titkolt szándéka, hogy vezető szerepet érjen el a személyazonosság-kezelés újradefiniálásának következő fejezetében. A cégvezetés infrastruktúrája három elsődleges összetevőből áll:

személyazonosság-kezelés, munkafolyamat és eseményfelügyelet. A díjnyertes Identity Manager termékben a címtáralapú személyazonosság-kezelés és a munkafolyamat alkotják az első két pillért. Most pedig beszéljünk a harmadikról: az eseményfelügyeletről.

A személyazonosság-kezelés újradefiniálásához és a cégvezetési infrastruktúra szegmensének kialakításához az ipar legjobb eseményfelügyeleti rendszerére volt szükségünk.

> A hozzáférés-felügyelet következő generációja

Egy egyszerű, könnyen használható hozzáférés-felügyeleti megoldás alkalmazásakor az informatikai vezetőknek a következő kulcsfontosságú kihívásokkal kell szembenézniük:

- a szövetségek (federation) támogatása
- a webes erőforrásokhoz való hozzáférés támogatása
- támogatás a vállalati alkalmazásokhoz való hozzáféréshez
- egypontos bejelentkezés
- a változatos informatikai megoldások (alkalmazások és címtárstruktúrák) támogatása.

A Novell 2007. januárjában jelentette be hozzáférés-kezelési megoldásának következő generációs változatát, a Novell Access Manager 3-at, az első olyan terméket, amely mindezen igényeket kielégíti. Ez az első hozzáférés-felügyeleti termék, amely eleget tesz a XXI. század informatikai kihívásainak, beleértve a webes hozzáférést, a J2EE szerepszámítást, a házirendalapú személyazonosság-ellenőrzést és személyazonosság-szövetségeket (identity federation). Más termékek nem rendelkeznek átfogó web- és szövetségtámogatással (support for Web and federation). A különböző számítástechnikai környezetek (például az eDirectory, az Active Directory, a Sun One kiszolgáló, bármely webes alkalmazás, a J2EE alkalmazások kifinomult támogatása) részletes támogatása számos előnyt biztosít.

A Novell Acces Manager 3 további előnyei:

- Adatabsztrakciós réteg a különböző címtár-hozzáférési eljárások kezeléséhez, amely skálázhatóságot és növekedést biztosít az alapjául szolgáló címtármegoldások különböző változatainak kezeléséhez.
- Valós idejű auditálás, figyelés és jelentés a Sarbanes-Oxley vagy a HIPAA törvények megfelelőségi jelentéseivel együtt. 2006 áprilisában a Novell felvásárolta az e-Security vállalatot, a biztonsági eseményfelügyelet területének egy vezető szállítóját, hogy biztosítsa e képességeknek a személyazonosság-kezelés keretrendszerén belüli szoros integrációját. A vizsgálat a hozzáférési jog megszerzésétől a SOX-megfelelőség szempontjából kritikus alkalmazások vizsgálatáig terjed. A Novell élen jár e képességek integrálásában, hiszen a Novell Access Manager 3 és a Sentinel (e-Security) termékek között biztosított az együttműködés.
- A biztonsági megközelítések széles spektrumának támogatása, beleértve a többtényezős hitelesítést és adattitkosítást.
- Egy felügyeleti eszköz, amely leegyszerűsíti a hozzáférések felügyeletét. Házirenden alapuló felügyeleti technikát építettünk be a felügyelet jelentős egyszerűsítse érdekében. Ez a hozzáférés visszavonását ugyanolyan könnyűvé teszi, mint a hozzáférés megadását.
- Léptékezhetőség: a Novell Access Manager 3 felhasználók milliárdjait támogatja.
- Hibatűrés.
- Webes tartalombiztonság. A biztonsági megoldásunk nem korlátozódik a hozzáférés ellenőrzésére.
- Teljes Liberty Alliance megoldás. A Liberty Alliance a személyazonossági szövetség szabványa. Míg más hozzáférés-felügyelet szállítók eszközkészletekkel biztosítják a Liberty Alliance használhatóságát, addig mi egy integrált, letesztelt, könnyen hozzáférhető támogatást biztosítunk a termék részeként.
- Továbbfejlesztett vállalati támogatás. A szokványos személyazonosság-szövetséget a vállalati használat szintjére emeltük, miután lehetővé tettük az engedélyezett szövetségek és a személyazonossági információ forrásának ellenőrzését. A szokványos személyazonosság-szövetség teljes mértékben támogatott, de emellett azok az eszközök is rendelkezésre állnak, amelyek segítik a vállalatokat a személyazonosságok konszolidálásában és a személyazonosságok számának csökkentésében.

> Az elmúlt év eredményei az informatikai rendszerek biztonsága terén

2006 kulcsfontosságú év volt a Novell számára a személyazonosság és a biztonság felügyelete terén, hiszen jelentős mértékben továbbfejlesztettük heterogén felügyeleti stratégiánkat. Az év az Identity Manager 3 megjelentetésével kezdődött, amely hamarosan a Novell leggyorsabban fejlődő termékévé vált. Az évet az Access Manager 3 termékünk bejelentésével zártuk, amely áttörést jelent a webes hozzáféréskezelés és a vállalati hozzáférés-kezelés integrálásának területén. Évközben felvásároltuk az e-Security vállalatot a többplatformos megfelelőségi megoldások biztosításához, melynek segítségével kialakítottuk az iparág vezető kínálatát.

A tágabb értelemben vett rendszer-felügyelet területén elért legjelentősebb eredményünk az adatközponti felügyelet felé történő elmozdulás volt. Nemrégiben mutattunk be három terméket, amelyek az adatközpontok kihívást jelentő témáira koncentrálnak: az együttműködésre, a virtualizációra, az egyenletes munkaterhelésre és a házirenden alapuló automatizálásra. Ezek a termékek a ZENworks Orchestrator, a ZENworks Virtual Machine Management és a ZENworks High Performance Computing.

Egy másik kulcsmomentum, hogy a munkacsoport-szolgáltatásainkat Linux platformra helyeztük át. 2006-ban nagyot léptünk előre az Open Enterprise Server/NetWare esetében a fájl-, a nyomtatás- és a tárolás-felügyelet alapjainak zárt NetWare szolgáltatásokról a Linux-alapú szolgáltatásokra való áthelyezése terén. Így ezeket a munkacsoport-felügyeleti szolgáltatásokat heterogén rendszerekkel kapcsolatos stratégiáink közé emeltük. Továbbra is folytatni kívánjuk a Linux-alapú GroupWise fejlesztését: jelentős mobilitási funkciókat építünk be a termékbe, a munkacsoportos számítástechnika csomagalapú megközelítésével pedig még hatékonyabbá tesszük a működését. N

Termék

„A képzelet az alkotás kezdete.
Elképzeljük amire vágyunk, azt akarjuk amit elképzelünk, s végül megalkotjuk amit akarunk.”
–George Bernard Shaw–

Ki, mikor, mit és hol?
Novell Identity Manager 3

Informatika az őrtoronyban
A biztonsági információ felügyelete és a megfelelés folyamatos ellenőrzése a Sentinel 5 által

Novell Access Manager 3
Hogy biztosan csak a megfelelő emberek férhessenek hozzá az adatokhoz

Ki, mikor, mit és hol?

Novell Identity Manager 3

Az üzleti sikerhez nagymértékben hozzájárul, hogy szükség esetén a megfelelő embereknek rendelkezésére állnak-e a megfelelő eszközök és adatok. Ehhez viszont hatékonyan kell kezelni a személyazonosságokat – az embereket és az erőforrásokat az egész vállalatra kiterjedően.

Viszonylag egyszerű a képlet: a személyazonosság-felügyelettel egyszerűbb javítani a szolgáltatásokon, könnyebb eltűntetni a biztonsági réseket és csökkenteni az informatika adminisztrációs költségeit. Nélküle az új alkalmazottak tétlenül ülnek, várva, hogy elérhessék a számukra szükséges üzleti eszközöket, míg a kilépett alkalmazottak esetleg még napokig, sőt, hetekig hozzáférhetnek ezekhez az eszközökhöz.

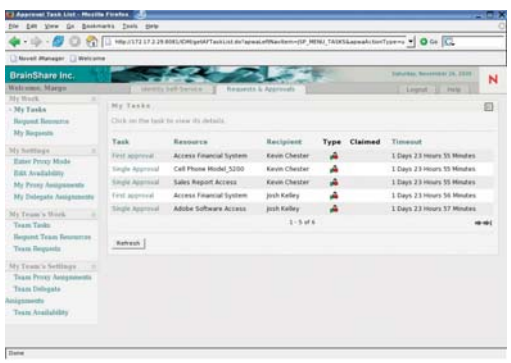
No persze – mondhatja erre valaki – idáig semmi újat nem hallottunk. A személyazonosság-felügyelet mára elengedhetetlenné vált az üzleti szférában. Az újdonság az a technológia, amely lehetővé teszi a személyazonosságok kezelését és hatékony szabályozását mind az automatikus folyamatokra vonatkozóan, mind az olyanok esetében, amelyek emberi beavatkozást igényelnek.

Az új megoldás felgyorsítja a jóváhagyási folyamatokat, lehetővé teszi a felelősség-átruházást; ugyanakkor olyan „önkiszolgáló” funkciókat biztosít, amelyek megkönnyítik a személyzet munkáját. S mindezt úgy teszi, hogy kihasználja a meglévő üzleti folyamatokba és technológiákba fektetett értékeket, nem pedig lecseréli.

> A felhasználók teljes életciklusára kiterjedő személyazonosság-kezelés

A Novell Identity Manager 3 segít a folyamatosan változó felhasználói közösség személyazonosság és hozzáféréseinek biztonságos felügyeletében: teljeskörű felügyeleti rendszert biztosít a felhasználók egész életciklusára kiterjedően, a szervezeti határokon keresztül, minden rendszerben. Az új felhasználók már az első napon elérhetik a szükséges erőforrásokat, szinkronizálhatják a jelszavakat az összekapcsolt rendszerek között, azonnal módosíthatják vagy visszavonhatják a hozzáférési jogokat, valamint kikényszeríthetik a biztonsági és törvényi előírásoknak való megfelelést.

A jóváhagyást igénylő folyamatok esetén a rendszer automatikusan értesíti a jóváhagyókat, akik egyszerűen és gyorsan megadják vagy megtagadják a hozzáférést (lásd 1. ábra). Még azt is megtehetik, hogy szükség esetén átruházzák jogkörüket másra.



1. ÁBRA: A Novell Identity Manager 3 továbbfejlesztett munkafolyamat-kezelő modulja automatizálja a vállalati folyamatot

Attól a pillanattól kezdve, hogy egy új alkalmazott besétált az első munkanapján a céghez, addig, amíg be nem csukta maga mögött az ajtót, amikor kilépett, az Identity Manager 3 felügyeli a folyamatokat. Mindezt az Identity Manager 3 három igen fontos funkciója garantálja: az automatizált, szerep alapú létesítés, a munkafolyamat alapú létesítés és a jelszavak felügyelete.

Nézzük meg egy kicsit közelebbről is, hogyan is működik mindez együtt a gyorsaság és biztonság megvalósítása érdekében.

1. Automatizált, szerep alapú létesítés

Az üzleti szabályok szerint az Identity Manager 3 automatikusan osztja ki az erőforrásokat a felhasználók számára, a szervezetben betöltött szerepeik és kapcsolataik alapján. Az új alkalmazottak már az első munkanapjukon elérhetnek bármit, amire szükségük van anélkül, hogy kézzel kellene felvinniük a felhasználói adatokat az egyes rendszerekre. Ez kevesebb munkaerőt igényel, így amellett, hogy a munkatársak a fontosabb projektekre koncentrálhatnak, költségmegtakarítással is jár.

- Tegyük fel például, hogy a Központi Egészségügyi Szervezet (KESZ) személyzeti vezetője éppen felvitt egy új bejegyzést a szervezet egyik kórházába az újonnan felvett Dr. Bánhidi Dalma számára. Ennek hatására a Novell Identity Manager 3 automatikusan elvégzi az alábbiakat: létrehozza minden egyes alkalmazásban Dr. Bánhidi fiókjait, amelyekbe a pontos, érvényes személyazonossági adatok kerülnek. Ha például a KESZ Microsoft Exchange-et használ a levelezéshez és az e-mail címek tárolásához, akkor az Exchange rendszerben létrehozza a dbanhidi@kesz.hu e-mail címet, és ezt az információt továbbítja a kapcsolódó rendszerekhez.
- Átalakítja az adatokat az egyes rendszereknek megfelelő formátumra. A PeopleSoft például xx-xxx-xxx formátumú telefonszámokat használ, míg a Microsoft Exchange formátuma (xx)xxxxxx. Az Identity Manager automatikusan a helyes formátumokat állítja elő.
- Frissíti az összes lényeges információt az összes kapcsolódó alkalmazásban. Például a PeopleSoft azt mutatja, hogy Dr. Bánhidi a cég debreceni kórházában dolgozik, így az Identity Manager a debreceni konténerben hoz létre számára egy Exchange postafiókot. Ha Dr. Bánhidi később átkerül a pécsi kórházba, akkor az Identity Manager automatikusan módosítja a megfelelő adatokat.

2 Munkafolyamat alapú létesítés

Természetesen előfordulhat, hogy nem lehetséges – vagy nem kívánatos – az összes erőforrás kiosztásának a teljes automatizálása. Néha egyetlen embernek kell döntenie arról, hogy egy adott erőforrás használatára jogosult-e valaki. Ez sem jelent gondot: az Identity Manager új bővítőmodulja integrálja a munkafolyamat alapú létesítést. Amikor egy erőforrást igényelnek, az Identity Manager létesítési modulja elektronikusan, a lehető leggördülékenyebben szolgálja ki a teljes folyamatot, még akkor is, ha emberi beavatkozásra van szükség.

Az Identity Manager 3 ugyanazon része szolgál az automatikus és az emberi felügyeletet igénylő létesítés végrehajtására és egyetlen azonosságtár (Identity Vault) tárolja a létesítéssel, az erőforrások kiosztásával kapcsolatos összes információt. Ennek előnyeit aligha kell magyarázni: nincs szükség papírmunkára, hiszen minden kérés és azok elbírálása elektronikusan történik, az automatizált jóváhagyási folyamat pedig garantálja a lehető leggyorsabb munkát.

Első munkanapján Dr. Bánhidi megnyitja az Identity Manager webes felhasználói alkalmazását, hogy megtekintse, milyen erőforrások állnak rendelkezésre és hogyan kaphat engedélyt a használatukra. A böngészőben megjelenő erőforráslista egyes elemeire egyszerűen csak rá kell kattintania, és máris megindul a hozzájuk tartozó jóváhagyási folyamat.

A nemrégiben megjelentetett Novell Identity Manager 3 segít a folyamatosan változó felhasználói közösség személyazonosságainak és hozzáféréseinek biztonságos felügyeletében: teljeskörű felügyeleti rendszert biztosít minden rendszeren a felhasználók egész életciklusára kiterjedően. Az új felhasználók már az első napon elérhetik a szükséges erőforrásokat, szinkronizálhatják a jelszavaikat az összekapcsolt rendszerek között, azonnal módosíthatják vagy visszavonhatják a hozzáférési jogokat, és minden esetben megfelelnek a biztonsági és törvényi előírásoknak.

Dr. Bánhidi szeretné elérni az Oracle pénzügyi rendszerét, ezért rákattint a megfelelő hivatkozásra, hogy kérje a hozzáférést. A kórház előírja, hogy az ilyen kéréseket Dombó Diánának és Radácsy Tivadarnak a személyzeti osztályról ellen kell jegyeznie. Az Identity Manager 3 automatikusan küld egy e-mailt Dombó Diánának a kérésről. Neki mindössze kattintania kell egy hivatkozásra a jóváhagyási űrlap megjelenítéséhez, majd az űrlap megfelelő gombjára a kérés jóváhagyásához.

Két vizit között Dr. Bánhidi meg tudja nézni a felhasználói alkalmazásban, hogyan is áll a kérése. Látja, hogy az egyik jóváhagyás már megvan, de Radácsy Tivadar jóváhagyása még hiányzik.

Eközben Radácsy – aki éppen Hajdúszoboszlón pihen – megnézi leveleit. A hotel portáján rendelkezésére álló böngészőn keresztül bejelentkezik és látja, hogy számos jóváhagyási feladat vár rá, amelyeket elfelejtett másokhoz rendelni, mielőtt elment. Radácsy e-mailt küld a főnökének, és megkéri, hogy ruházza át ideiglenesen a jóváhagyásokat a listáján egy másik vezetőre. Mivel Kerekes Adrienn helyettes vezető jogosult az Oracle pénzügyi rendszerével kapcsolatban intézkedni, Radácsy főnöke kiosztja neki az összes Oracle-kérés elbírálását Radácsy távollétében. Perceken belül Kerekes megkapja Dr. Bánhidinak az Oracle pénzügyi rendszerre vonatkozó kérését. Mivel az orvosok alapesetben nem jogosultak belelátni a kórház pénzügyeibe, Kerekes megtagadja a kérést. A kórház irányelveit sikerült betartani néhány egérkattintással, még úgy is, hogy a jóváhagyók egyike a Kastély Szállóban üdült.

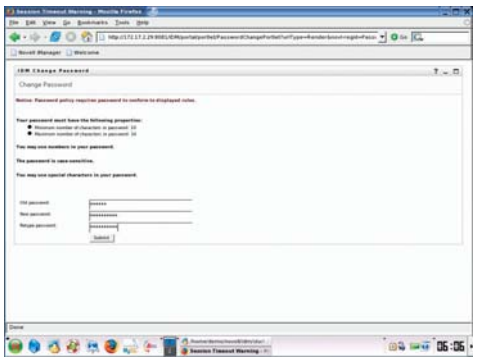
Következő szabadsága előtt Radácsy pedig figyelni fog arra, hogy ne felejtse el átruházni a feladatokat a megfelelő helyettesekre, asszisztensekre vagy akár ideiglenesen kijelölt személyekre. Megteheti ezt máskor is, például jövő hónapban, amikor az éves jelentéseket kell elkészíteni.

Az Identity Manager 3 segít abban, hogy a létesítéssel kapcsolatos jóváhagyási döntéseket mindig a megfelelő, az adott alkalmazottakra vonatkozóan közvetlen döntési jogkörrel rendelkező személyek hozzák meg. Segít továbbá elkerülni a késéseket, ha az emberek távol vannak, vagy mással foglalkoznak.

3. Jelszófelügyelet

Ha egy alkalmazott elfelejti a jelszavát, fel kell hívnia a vállalati helpdesket, hogy állítsa vissza azt – értékes perceket pazarolva ezzel saját idejéből ráadásul ezzel növeli a támogatási költségeket. A Novell Identity Manager 3 használatával azonban a felhasználó szinkronizálhatja jelszavait, így elegendő egyet megjegyeznie az összes rendszerhez. Ha ez nem is sikerülne, kaphatnak segítséget, vagy megváltoztathatják maguk a jelszót a felhasználói alkalmazáson

keresztül. A jelszavak egyébként az egyes rendszerek (például a Microsoft Windows) saját jelszókezelő felületeivel is kezelhetők (lásd 2. ábra).



2. ÁBRA: A Novell Identity Manager 3 leegyszerűsíti a jelszavak menedzselését

Ha például Dr. Bánhidi elfelejtette jelszavát, a felhasználói alkalmazáshoz fordulhat, amely segít neki felidézni, létrehozni, módosítani és visszaállítani jelszavát anélkül, hogy felhívná a helpdesket és feltartana egy informatikust.

A program a rendszergazda által beállíthatóan a következő lehetőségek egyikét kínálja fel Dr. Bánhidinek:

- Súgó a jelszóhoz: a rendszergazda határozza meg, hogy a rendszer a súgót azonnal a képernyőn jelenítse meg, vagy e-mailben küldje el.
- Jelszóvisszaállítás kérdés-válasz alapján: a képernyőn egy vagy több kérdés jelenik meg. Ezek között lehet olyan, amelyet eredetileg Dr. Bánhidi maga adott meg, illetve olyan, amelyet az Identity Manager rendszergazda – sőt, akár a kettő kombinációja is. Ha Dr. Bánhidi helyesen válaszolja meg a kérdéseket, akkor jogosult megváltoztatni jelszavát. A rendszer automatikusan ellenőrzi, hogy az új jelszó megfelel-e a különféle irányelveknek, majd frissítésre kerül és szinkronizálódik az összes csatolt rendszerrel.

A személyazonosság gyakran vitatott téma manapság a vállalati biztonsággal kapcsolatban. Egysége személyazonossági alap nélkül minden egyes új bevezetett megoldás csak egy újabb különálló személyazonosság-halmazt jelent, és csak szaporítja a biztonsági problémákat.

Az Identity Manager használatával garantálható, hogy a felhasználók által beállított jelszavak biztonságosak: az egész rendszerre kiterjedő jelszóirányelvek készíthetők a jelszavak elleni támadások elhárításához.

> Áthelyezés és létesítés

Az Identity Manager 3 funkciói kiterjednek a felhasználó teljes életciklusára. Tegyük fel például, hogy a pécsi áthelyezés után Dr. Bánhidit előléptetik a kórház főorvosává. Az előléptetés természetesen számos változással jár a személyazonossági adatok között – vagyis több rekordot is módosítani kell. A HR-rendszer módosítása után az Identity Manager 3 továbbszinkronizálja a személyazonossági adatokat az egész vállalaton belül. Lássuk, mi történik azután, hogy egy helyen módosultak az adatok:

- Dr.Bánhidi automatikusan megkapja a hozzáférést azokhoz a rendszerekhez, amelyeket főorvosként el kell érnie.
- A hozzáférése azonnal megszűnik azokhoz a rendszerekhez, amelyeket már nem jogosult használni.
- Amikor Dr. Bánhidi átköltözik debreceni irodájából a Pécsi Kórház harmadik emeletére, a főorvosi irodába, akkor a címe automatikusan frissítésre kerül a rendszerben és az új adatok átkerülnek az összes érintett alkalmazásba.
- Dr. Bánhidinek most új főnöke van. Minden rendszer frissül – például a megfelelő főnök-beosztott kapcsolat módosul a költségelszámolási folyamatot kezelő pénzügyi alkalmazásokban.

A Novell Identity Manager automatikusan:

- létrehozza a fiókokat más alkalmazásokban a felhasználó által betöltött szerepek alapján;
- szétosztja a más alkalmazásokból begyűjtött személyazonossági adatokat;
- átalakítja az adatokat az egyes rendszerek saját formátumára;
- frissíti a releváns adatokat az összes kapcsolódó alkalmazásban.

Azon túl, hogy használatával jelentős időmegtakarítás érhető el előléptetések vagy áthelyezések esetén, ez a szolgáltatás jelentős biztonsági funkciót is betölt. Egyetlen módosítással azonnal, az összes rendszeren elvehetők a felhasználó hozzáférési jogai. Ez azt jelenti, hogy a kilépett alkalmazottak és üzleti partnerek mindennemű hozzáférése azonnal megszűnik, ha a céggel való kapcsolatuk megszakad. Gyors és garantált a védelem az esetleg rossz szándékú ex-alkalmazottak ellen, hiszen megszűnik a hozzáférésük a bizalmas adatokhoz és nullára csökkennek a korábbi alkalmazottak felhasználói fiókjaival kapcsolatos szolgáltatási költségek is.

> A megfelelő alap a személyazonosságok kezeléséhez

A személyazonosság gyakran vitatott téma manapság a vállalati biztonsággal kapcsolatban. Egységes személyazonossági alap nélkül minden egyes új bevezetett megoldás csak egy újabb különálló személyazonosság-halmazt jelent, és növeli a biztonsági problémákat.

A Novell Identity Manager 3 áthidalja a gátakat az egyes üzleti rendszerek között és lehetővé teszi, hogy az információ biztonságosan jusson el az arra jogosult felhasználókhoz. A rendszer az üzleti szabályok alkalmazásával azonnal azonosítja és szolgáltatja a megfelelő erőforrásokat az arra jogosultaknak – személyazonosságuk, a betöltött szerepeik és a szervezettel való kapcsolatuk alapján.

A piacvezető technológiákra és a bonyolult személyazonosság-felügyeleti megoldások kialakítása terén szerzett bőséges tapasztalatokra épülő Novell Identity Manager 3 azt a személyazonosság-felügyeleti alapot biztosítja, amellyel a legbonyolultabb üzleti környezetek és a még csak kialakulóban lévő üzleti technikák is kiszolgálhatók. Az Identity Manager 3 innovatív megoldásaival a Novell megteremti a növekedéshez szükséges rugalmasságot, és a Novelltől megszokott és elvárt, világszínvonalú biztonságot. N

Informatika az őrtoronyban

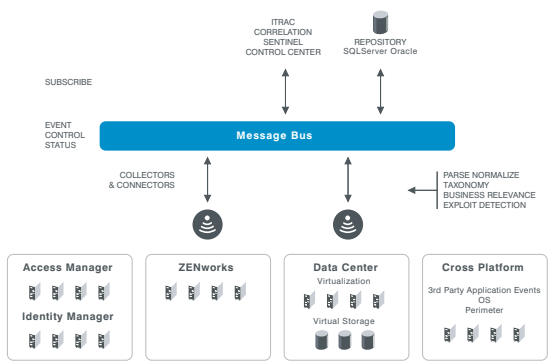
A biztonsági információ felügyelete és a megfelelés folyamatos ellenőrzése a Sentinel 5 által

Sok szervezet csak most kezdi felismerni, hogy milyen fontos szerepet játszik az előírásoknak való megfelelés a szervezeti struktúrában és a biztonság megteremtésében. Fontos az előírt szabályozások ismerete és alkalmazása a szervezeti infrastruktúrán belül. Idővel ezeknek a szabályozásoknak a száma csak nőni fog, vagyis a megfelelés hátterének minél gyorsabb kialakítása nemcsak egy megfontolt üzleti döntés, hanem egyre több esetben törvények által meghatározott előírás is.

Ha a szervezet – másokhoz hasonlóan – arra törekszik, hogy minél jobban eleget tegyen a megfeleléssel kapcsolatos elvárásoknak, jó hírrel szolgálhatunk: a Novell nemrégiben felvásárolta az e-Security-t. A vállalat élen jár a biztonsági információk felügyeletét és a megfelelés folyamatos ellenőrzését biztosító megoldások fejlesztésében. Az e-Security megoldásait a Gartner nemrégiben a biztonsági információk és események felügyeletével kapcsolatos „mágikus négyzeteiben" „vezetőként" emelte ki hozzátéve, hogy ennek a terméknek a legteljesebb a jövőképe.

„A megfelelés területén az ügyfelek olyan egységes megoldásokat igényelnek, amelyek magukban foglalják a rendszer, a személyazonossági adatok, a hozzáférés és a biztonsági események felügyeletét. Az e-Security felvásárlásával jelenleg a Novell az egyetlen olyan szállító, aki kielégíti a felhasználókat, rendszereket és folyamatokat integráló, valós idejű, átfogó megfelelés-kezelési megoldásra vonatkozó üzleti igényeket" – Chris Christiansen, az IDC biztonsági termékekért és szolgáltatásokért felelős alelnöke.

Az e-Security felvásárlásával a Novell ötvözi a valós idejű rendszerfigyelést és -javítást biztonsági, hozzáférés-vezérlési és megfelelésiesemény-felügyeleti funkciókkal. Az e-Security Sentinel termékcsaládjával együtt a Novell elsőként nyújt egyetlen, egységes képet a biztonsági és a megfeleléssel kapcsolatos tevékenységekről a teljes vállalatra kiterjedően, egyesítve a személyazonosság- és rendszerfelügyelet előnyeit a valós idejű megfelelés-ellenőrzéssel (lásd 1. ábra). A felhasználói, hálózati és alkalmazásesemények átfogó megjelenítésével leegyszerűsíthető a korábban munkaigényes és hibázási lehetőségekkel teli folyamat, az automatizálás segítségével pedig csökkenthetőek a költségek és szigorúbb megfelelési program alakítható ki.



1. ÁBRA: A Sentinel csatolói segítségével képes adatokat gyűjteni a Novell biztonsági, felügyeleti és adatközpont megoldásaiból, valamint képes csatlakozni más gyártók termékeihez is

Nézzük meg közelebbről mit tud a Sentinel. A Sentinel elősegíti a kockázatok hatékonyabb kezelését, a biztonsági mérőszámok javítását és a megfeleléssel kapcsolatos kimutatások automatizálását. Emellett csökkenti a biztonsággal és a megfeleléssel kapcsolatos költségeket, miután a manuális folyamatokat egy folyamatos rendszerfigyelési és kimutatáskészítési megoldással váltja fel. A Sentinel lehetővé teszi a biztonsági rendszer és a megfelelés valós idejű, folyamatos figyelését az összes rendszerre és alkalmazásra kiterjedően, a használt platformtól függetlenül. Az egész vállalatra kiterjedően valós idejű képet ad az aktuális helyzetről a biztonsággal és a megfeleléssel foglalkozó csoportok számára.

A Sentinel hozzájárul a másodpercenkénti több ezer eseményből származó adatok begyűjtéséhez, összevetéséhez, megfigyeléséhez és megjelenítéséhez – mindezt valós időben. A szervezet biztonsági és megfelelési állapotára vonatkozó kimutatások állandóan naprakészek: nem kell a legutóbbi biztonsági vagy megfelelési felülvizsgálat jelentéseire támaszkodni.

A Sentinel az alábbi modulokból épül fel:

- Sentinel Control Center (irányítóközpont)
- Sentinel Reports (kimutatások)
- Sentinel Wizard (varázsló)
- Sentinel Advisor (tanácsadó, opcionális modul)
- Sentinel Mainframe Connect (nagygépes kapcsolat, opcionális modul)

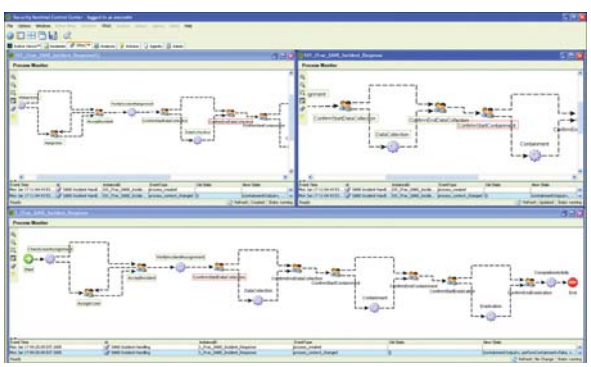
A Sentinel Control Center központi konzolt biztosít a valós idejű rendszerfigyeléshez, az események összevetéséhez, az incidensek kezeléséhez és a jelentések készítéséhez.

Az Active Views (aktív nézetek) számos valós idejű megjelenítési és elemzési funkciót kínál a fenyegetések és az irányelvsértések azonosításához és elemzéséhez – mindezt egyetlen integrált, nagyteljesítményű biztonság- és megfelelésfigyelő irányítóközpont formájában (lásd a 2. ábrát). Az intuitív képernyőkön az elemzők gyorsan azonosíthatják az új trendeket, támadásokat vagy irányelvsértéseket. Valós időben, grafikusan kezelhetik az adatokat; és visszatérhetnek a régebbi adatok részleteihez, legyenek azok néhány másodperccel vagy több órával korábbiak. A gyakorlatban tulajdonképpen egy valós idejű hiteles elemzési eszköztárként működik.

2. ÁBRA: A Sentinel „aktív nézet" képernyő az események valós idejű megjelenítéséhez

Az átfogó incidenskezelési funkciókkal manuálisan (a megfelelő adatok és dokumentumok hozzácsatolásával) és automatikusan (bővíthető korrelációs szabályok átfogó halmaza alapján) is létrehozhatók incidensek.

Az iTRAC munkafolyamattal előre lehet reagálni az incidensekre, automatizálva és kikényszerítve ezzel az incidensek azonosítási és megoldási folyamatát. Így a biztonsági szervezet meghatározott „rögzítési rendszert" használhat a biztonsággal vagy a megfeleléssel kapcsolatos incidensek nyomon követésére és kimutatására (lásd a 3. ábrát).



3. ÁBRA: Az iTRAC modul segítségével automatizálhatók a biztonsági eseményre adandó reakciók

A Sentinel Reports – a Sentinel 5 egyik fő modulja – segítségével az alábbi feladatok végezhetők el:

- bizonyítható, hogy folyamatosan figyelik a felhasználók tevékenységét a kritikus informatikai erőforrásokkal kapcsolatban, valamint az, hogy a biztonsági és megfelelési incidensek azonosításra kerülnek;
- igazolható, hogy a szervezet nyomon követi, valamint megoldja az incidenseket és az irányelvek megsértését a még robusztusabb megfelelési tanúsítás érdekében;
- megszerezhető a biztonsági állapot hatékony figyeléséhez, méréséhez és javításához szükséges tudás;
- felderíthetők azok a trendek és rendellenességek, amelyeket manuálisan nem lehetne azonosítani.

A Sentinel Reports segítségével nyomon követhető és kimutatható minden, a biztonsággal kapcsolatos tevékenység a Sarbanes-Oxley, HIPAA, FISMA, PCI és más törvények által szabályozott eszközökre vonatkozóan: például a felhasználók tevékenysége, az incidensek és az irányelvek megsértései.

A Sentinel Reports értékes megállapításokat ad az irányelvek betartásáról, megsértéseiről és a korrekciós tevékenységekről a felső vezetés, a belső és a külső auditorok számára. Továbbá beszámol arról is, hogyan befolyásolja a felhasználók tevékenysége a kritikus eszközöket. A rendszernaplók és más fontos adatforrások kézi átvizsgálásának időigényes gyakorlatának megszüntetésével a ráfordított idő és a költségek mellett csökkenthető a működési kockázat is, mindaz, amit egy felülvizsgálatra való felkészülésre és annak áttekintésére kellene fordítani.

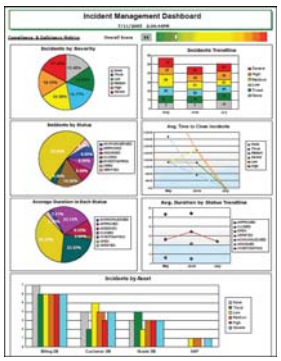
A Sentinel 5 azonnal használható jelentéskészítési funkcióival a szervezet gyorsan és hatékonyan juthat hozzá a kritikus biztonsági és megfelelési adatokhoz, amely jelentős előnynek számít, amikor az előírt felülvizsgálati dátumok, a törvényi előírások határidejei és más szorító tényezők határozzák meg a projektek ütemezését. A Sentinel Reports számos egyszerűen beállítható kimutatást és műszerfalat tartalmaz. (Lásd a 4. ábrát.) Emellett készíthetők saját, a szervezet saját igényeinek megfelelő jelentések is az ipari szabvány jelentéskészítővel. A vállalat összes osztálya hozzájuthat a szervezet megfelelési és biztonsági helyzetével kapcsolatos friss adatokhoz. A hatékony működést segíti elő, hogy a jelentéskészítő megoldás rugalmasan, többféle formátumban készít jelentéseket, így például előre ütemezett módon jeleníti meg az adatokat a belső, vállalati intranetes portálokon.

> Legyen a szabályozás célszerű, betartható és ellenőrizhető

Legyen a szabályozás célszerű

A szabályozásnak és a mögöttük rejlő irányelveknek nemcsak az információval, hanem a szervezettel és magukkal az előírásokkal szemben támasztott biztonsági igényeknek is meg kell felelniük. Ez azt jelenti, hogy a bizalmas adatok esetében célszerű a lehető legmagasabb szintű védelem biztosítása. Ha azonban egy ilyen védelmi rendszer kialakításának költségei, előírásai vagy összetettsége

meghaladja a szervezet lehetőségeit, akkor az irányelvet többféle módon fogják megkerülni a szervezeten belül.



4. ÁBRA: Átfogó biztonsági riportok készítése

Legyen a szabályozás betartható

Az irányelveknek és a szabályozásnak együtt kell működniük, és segíteniük kell egymást. Az irányelv kijelenthet valamit, mellyel meghatározza a vezetőség felfogását valamilyen irányba. Ha azonban nincs lehetőség az irányelv implementálására és betartatására, akkor komoly szakadék alakul ki a felfogás és a valóság között. Ez a szakadék pedig csak tágulni fog minden egyes felülvizsgálatnál, amikor az irányelv alapján mérik a biztonsági gyakorlatot. Sok esetben az irányelv lassan valósítható meg és tartható be, de ahogy nőnek és fejlődnek a rendszerek, használatuk egyre fontosabbá válik és egyre nehezebben tarthatóak be. Jó példa erre az események megfigyelése. A legtöbb cégnél van valamilyen irányelv vagy szabályzat, ami előírja az eseménynaplók időről időre történő átnézését a problémák azonosítása érdekében. A valóságban azonban a legtöbb eseménynaplót többször is felülírják, mire valaki megnézi őket.

Legyen a szabályozás ellenőrizhető

Egy irányelv semmit sem ér, ha működik és ellenőrzik, azonban semmi nyoma annak, hogy létezik. Az irányelveknek és a szabályozásnak együtt kell működniük. Minden biztonsági irányelvhez tartoznia kell felülvizsgálati naplóknak, amelyek jelzik és igazolják, hogy az irányelv létezik és következetesen, folyamatosan be van tartva. Ha pedig megvan az elfogadható információbiztonsági irányelv, akkor létrejönnek a belső szabványok és a szabályozás is.

A Sentinel Wizard kibővíti az eseményfolyamot: a vállalat számára releváns adatokat szúr be az események összevetése és elemzése előtt. (Lásd az 5. ábrát.) A sok esemény azt jelenti, hogy a Sentinel összeveti az adatokat a belső vagy külső fenyegetések és az irányelvsértések azonosításához és kijavításához szükséges üzleti kontextussal. A Sentinel Wizard egyszerűen, egérműveletekkel kezelhető felületén az adatok gyűjtéséhez, szűréséhez, normalizálásához, illetve a lényeges információ Sentinel Control Center felé történő biztonságos továbbításához bármely forrásból szabályalapú gyűjtők (collectors) készíthetők. Használatával bármely forrás figyeléséhez gyorsan és hatékonyan elkészíthetők és beállíthatók gyűjtők, valamint:

- gyűjtők létrehozásához, felügyeletéhez és alkalmazásához az összes vállalati rendszeren;
- bármely informatikai eszköz csatlakoztatásához a Sentinel Control Centerhez;
- szabályok menet közbeni kialakításához és testreszabásához;
- a legjobb gyakorlatok és az üzleti szabályok felhasználásához az egyedi biztonságfelügyeleti és megfelelés-ellenőrzési igények kiszolgálásához.

A maximális rugalmasság és gyors telepíthetőség érdekében a Sentinel 5 eredetileg is tartalmaz több azonnal használható, paraméterezhető és bővíthető gyűjtőt. (Lásd a 6. ábrát.)

A Sentinel Advisor központosított biztonsági intelligenciát biztosít az új sérülékenységek elleni proaktív védekezéshez. A Sentinel Advisor az ismert fenyegetésekről és sérülékenységekről átfogó, naprakész ismeretekkel rendelkezik. A Sentinel Advisor és az iTRAC páratlan funkcionalitást nyújtanak a fenyegetések valós időben történő csökkentéséhez és az irányelvek megsértésének megakadályozásához.

A Sentinel Advisor összeveti a Sentinel valós idejű riasztási adatait az ismert sérülékenységekkel, és automatikusan elvégzi a javítást, leegyszerűsítve ezzel az incidensek felderítését és a rájuk való reagálást. A Sentinel Advisorral megállapítható, hogy az események egy adott sérülékenység kiaknázását jelzik-e, és hogy a támadások milyen mértékben érintik az eszközöket.

Az informatikai szabályozás automatizálása – védekezés, észlelés és javítás

Az informatikai szabályozás automatizálása munkaigényes folyamatnak tűnhet, de nem kell, hogy az is legyen. Az átállás a kézi jelentésekről az automatizáltakra könnyen és gyorsan elvégezhető az alábbi lépésekkel:

- A szervezettség kialakítása.
- A szabályozás céljainak megértése.
- Terv kialakítása a sikerhez.
- Megfelelő szabályozási szintek meghatározása a szervezet számára.

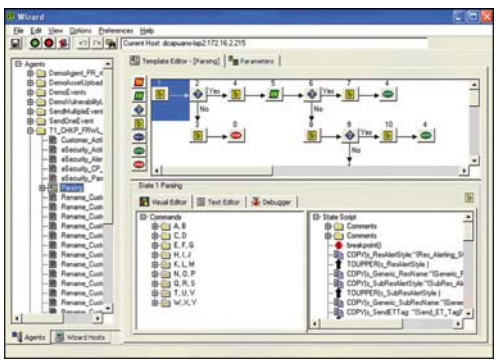
A szervezet számára megfelelő szabályozási szintek meghatározása függ a szervezetre vonatkozó előírásoktól, a szervezet típusától és az üzleti követelményektől.

A megfelelő szabályozás háromféle formában jelentkezik: védekezés, észlelés és javítás.

Minden vállalatnál vannak értékes, védelmet igénylő információs erőforrások. Sok vállalat készít irányelveket, amelyben meghatározza, milyen igényeket támaszt a vállalat információs eszközeinek védelmével kapcsolatban. Így az adott információ vélt értékének megfelelő védelmi eszközöket telepítik az irányelv megvalósítása érdekében. A biztonsági elemek típusainak megismerése segíthet a szervezetek informatikai biztonsági csapatainak a legmegfelelőbb típus kiválasztásában.

Eszközök a megfelelő védelemhez

A védőeszközök megelőző intézkedések az információ értékének elvesztése ellen. Az ilyen eszközök, határozott közbelépéssel és irányítással megakadályozzák a támadásokat. Gondoskodni kell az engedélyek naprakészségéről és felügyeletéről. A legtöbb védőeszköz bevezetése és fenntartása drágább, mint az észlelő és javító eszközöké. Később azonban, ha a megfelelő módon használják megakadályozza az értékes információ elvesztését. Néhány példa védekező eszközökre: hitelesítési rendszer, hozzáférés-vezérlési rendszerek, titkosítás és tűzfalak (amelyek mind-mind a megfelelés fontos elemei).



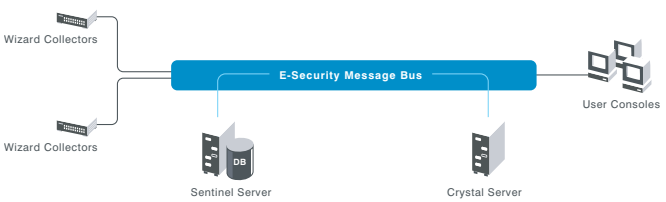
5. ÁBRA: A Sentinel csatolók testreszabása

Eszközök az azonosításhoz

Az azonosításra szolgáló eszközök már az eseményt követően szerephez jutnak. Ezek az eszközök a veszteséget enyhítő rendszerek, amelyek – hasonlóan egy riasztóhoz – jelzik, ha valami történt és lehetséges, hogy elvesztek értékes információk. Ez a fajta eszköz a már meglévő megelőző eszközöket támogatja. Ezeket kiegészítve költsége általában jóval alacsonyabb, mint a védekező eszközöké. Ezeket az eszközöket passzív/reaktív jellegüknél fogva azok a vállalatok használják, amelyek kizárólag észlelő eszközökre támaszkodnak, nagyobb kockázatot vállalva ezzel az értékes információk elvesztésére.

Eszközök javításhoz

A harmadik típus, a javításra szolgáló eszközök szinte minden szervezetnél megtalálhatók. Gyakran ezeket az eszközöket telepítik, ha elegendő egy jól működő biztonsági mentési/visszaállítási rendszer. A legtöbb szervezet esetében ez az alkalmazott stratégia a nyilvánosan elérhető rendszerek, például a webhelyek és az anonim FTP helyek esetében. Az információ értéke jellemzően az elérhetőségben rejlik és ha valaki módosítja vagy törli is az információs erőforrást, akkor elegendő egy korábbi állapot visszaállítása. Az ilyen eszközök telepítése olcsó, ezért nem ajánlatos kizárólag ezekre támaszkodni a valóban értékes információs erőforrások védelme esetén. A javító eszközök költsége azonnal megtérül, ha történik egy incidens és egy értékes adat megsérül vagy elveszik.



6. ÁBRA: A nagyteljesítményű e-Security Massage Bus biztosítja a Sentinel skálázhatóságát

A Sentinel Mainframe Connect közvetlenül a nagyszámítógépekről gyűjti be a biztonsági és megfelelési tevékenységekkel kapcsolatos adatokat és veti össze ezt az információt a cég más informatikai biztonsági és megfelelési eseményeivel – páratlan megoldást nyújtva ezzel az iparágban. A Sentinel Mainframe Connect használata az összköltségek mellett csökkenti a karbantartás szükségességét, hiszen ezáltal nem kell más cégek termékeit használni a nagygépes biztonsági adatok eléréséhez.

A Sentinel termékekről, valamint a Novell-környezetben történő működésükről további információt a novell.com/sentinel weboldalon talál. N

Novell Sentinel 5, az elektronikus világ testőre

Folyamatos megfelelőség-kezelés
A törvényektől kezdve a külső és belső előírásokig egyre összetettebbek a betartandó szabályok (Sarbanes Oxley/BASEL II/PSZÁF előírások,...). Gyakrabban fordul elő, hogy a szervezeteknek különböző információforrásokra és eszközökre kell támaszkodniuk az ún. megfelelőség kezelése során. A Sentinel 5 valós időben, és teljes körűen jeleníti meg a biztonsági és megfelelőségi adatokat, emellett biztosítja a vállalat hálózati eseményeinek automatikus monitorozását, jelentések készítését és az eseményekre történő azonnali reagálást.

Valós idejű eseménykezelés
A Sentinel 5-tel az egész IT infrastruktúrán belüli váltások, változások könnyen követhetőek az üzleti folyamatoktól a definiált szabályokig és előírásokig bezárólag. A rendszer használata lehetőséget kínál továbbá arra is, hogy a szervezet csökkentse a biztonság és a szabályoknak történő hatékony megfelelés költségeit, eredményesen kézben tartsa a biztonsági kockázatokat.

Nagy teljesítményű valós idejű adatgyűjtés, feldolgozás
A rendszer nagy teljesítménye elősegíti az azonnali adatgyűjtést és összevetést akár másodpercenként több ezer legyűjtött 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.

Biztonsági rés felismerése, megelőző megoldások
A rendszer tartalmaz egy munkafolyamat támogató mechanizmust a biztonsággal kapcsolatos váratlan események figyelemmel kísérésére, nyomkövetésére a felmerülésétől kezdve a probléma megoldásáig. Valósidejű riasztáskor, a Sentinel 5 a felmerült problémát összeveti a tárolt, centralizált szabályok és megoldási utak adataival és akár automatikusan beavatkozik. Ez jelentősen csökkenti a reakció időt.

Standard jelentések és a biztonság mérhetősége
A jelentések előre definiált mintái standard jelentés készítő alkalmazások (pl. Business Objects'Crystal Reports) alapján lettek kialakítva. Használatukkal könnyen elkészíthetőek a tendenciákkal, vizsgálatokkal és a megfelelőséggel kapcsolatos reportok, amelyek nem a legutóbbi biztonsági és előírásoknak történő megfelelőségi auditokból, hanem a rendszerből jövő valós idejű a hálózat állapotával kapcsolatos azonnali információkból származnak és így mindig naprakészek.

Novell Access Manager 3

Hogy biztosan csak a megfelelő emberek férhessenek hozzá az adatokhoz

Kovács Úr gyomra görcsbe rándult, ahogy befejezte a hívást és az autópályán előtte tornyosuló tömegre meredt. A hírek finoman szólva is rosszak voltak. Az egyik versenytárs cégnek sikerült kilopnia bizalmas kutatási fájlokat az egyik partner rendszeréből. Egy forradalmian új gyógyszer kifejlesztésére irányuló több hónapnyi úttörő kutatás kapott léket. A megbízható forrásokra is a gyanú árnyéka vetült. Fontos adatok váltak elérhetetlenné mindenki számára, amíg a partnercég a károkat mérte fel. A gyógyszer fejlesztése pedig megállt.

Ha ez megtörténhetett a partnercéggel, akkor Kovács Úr gyanította, megtörténhetett volna saját gyógyszercégükön belül is. Mint operatív igazgató, a lehető leggyorsabban gondoskodnia kellett arról, hogy biztonságba helyezze szervezete legértékesebb erőforrásait. Ez azonban nem is olyan egyszerű. Az épületeket leszámítva szinte minden vállalati eszköz valamilyen módon a hálózatra kapcsolódik. Az alkalmazottak, partnerek és vásárlók elvárják az egyszerű hozzáférést mindenhonnan, minden pillanatban. És mégis, a konkurenciát – és a bűnözőket – hatékonyan távol kell tartani.

Kovács Úr fő problémája az volt, hogyan valósítsa meg egyszerre és a lehető leggyorsabban a biztonságot és a hozzáférhetőséget. Mindezt tovább nehezítette, hogy a költségvetésen sem szeretett volna változtatni. A „biztonság” fogalma első látásra meglehetősen egyszerű: az ember vagy beenged valakit, vagy kizárja. Kovács Úr azonban egy labirintussal találta magát szemben: az egész világra kiterjedő cég nemrégiben vásárolt fel két másik vállalatot és egy sor partnerre támaszkodott. A dolgok bonyolultabbak voltak annál, mint ahogyan azt először gondolta volna.

Kovács Úr olyan modern megoldást keresett, amellyel megakadályozhatja az információlopást, védheti az infrastruktúrát, és a munkatársak személyes adatait a cégen belül és kívül egyaránt. A rendszernek légmentesen kellett zárnia – hibának vagy kompromisszumoknak nem volt helye.

A biztonság mellett ugyanakkor azt is szem előtt kellett tartania, hogy a megoldást bármely alkalmazott tartózkodási helyétől, illetve a használt operációs rendszertől és platformtól függetlenül, problémamentesen tudja használni. Olyan felhasználóbarát megoldásra volt szükség, amellyel a partnerek gyorsan és egyszerűen hozzáférhetnek a számukra szükséges információkhoz. S végül segítenie kellett a céget abban, hogy egyszerű, átlátható módon feleljen meg a szigorú törvényi előírásoknak, anélkül, hogy a rendszergazdák értékes idejét rabolná.

Kovács Úr tudta, hogy egyes megoldások kiváló biztonságot nyújtanak. Tisztában volt azzal is, hogy más rendszerek meg a hozzáférés terén jeleskednek, de kevésbé biztonságosak, különösen a szervezetre és a partnerekre leselkedő meglévő veszélyek tekintetében. Kovács Úr olyan megoldást keresett, amelyik egyszerre szolgálja ki a biztonsággal és a hozzáféréssel kapcsolatos igényeket – és költséghatékonyan vezethető be a vállalatnál a használt platformok sokszínűsége ellenére.

> A megoldás: Novell Access Manager 3

Ez a megoldás a Novell Access Manager 3. Három fő ok, amiért érdemes a Novell Access Manager 3-at választani:

- A Novell Access Manager 3 segítségével az alkalmazottak, partnerek és vásárlók egyszerűen és biztonságosan érhetik el a szükséges információt, ugyanakkor a rendszer hatékonyan megakadályozza, hogy bárki más hozzáférjen az értékes adatokhoz. Pontosan meghatározható, hogy kik jogosultak az erőforrások elérésére, ők pedig mindent, amihez joguk van, egyetlen jelszóval érhetnek el. Természetesen a még jobban védeni kívánt erőforrások esetében egyéb kifinomult módszerek is használhatók, mint például tokenek vagy X.509 tanúsítványok.
- A Novell Access Manager 3-mal szabályozható mind a webes, mind a hagyományos üzleti alkalmazások hozzáférése. Egyetlen jelszóval adhatják fel a megbízható partnerek a rendeléseiket az interneten keresztül, ellenőrizhetik a fontos projektek állapotát, vagy éppen chatelhetnek a vállalat fejlesztőivel.
- A Novell Access Manager 3-mal lehetővé válik az interneten keresztüli biztonságos üzletvitel, mivel minden egyes esetben pontosan azonosítható és ellenőrizhető, hogy kivel állunk kapcsolatban.

Lássuk, hogyan is működik mindez: önnek kell meghatároznia, hogy ki milyen adatokhoz férhet hozzá. Ezek alapján az adatok elérését szabályozó irányelvek készülnek, és a Novell Access Manager 3 ezen irányelvek alkalmazását kényszeríti ki minden alkalommal. Ha valaki megpróbálja elérni az adatokat, akkor a rendszer az alapján engedélyezi a hozzáférést, hogy az illető milyen szerepet tölt be a szervezetben, vagy milyen kapcsolatban áll a szervezettel.

A Gartner Inc. a 2006 második félévére vonatkozó, a webes hozzáférés-kezelést vizsgáló Magic Quadrant jelentésében a Novellt a hozzáférés-kezelés egyik vezető szállítójának minősítette.

Kovács Úr készített például egy irányelvet, amelynek értelmében minden kutató, aki egy bizonyos rákellenes projekten dolgozik, elérheti az adott projekt adatait. Ezeknek az adatoknak az elérését egy másik partner számára is engedélyezheti, ilyenkor egy egyszerű irányelv gondoskodik arról, hogy a partner elérheti a számára engedélyezett adatokat, minden más hozzáférés azonban tiltott számára.

Az irányelvek módosítása egyszerű, és a változások azonnal életbe lépnek a teljes cégre kiterjedően. Vagyis ahogy változnak az üzleti igények, úgy lehet gyorsan módosítani az irányelveket – és alkalmazni különféle irányelveket a különböző felhasználók esetében. Kovács Úr például minden vezető számára engedélyezi, hogy elérje az általuk irányított dolgozók személyi adatait, de védi mindenki mástól, aki nem vezető.

Mi a helyzet a kompatibilitási problémákkal? Szemben más hozzáférés-vezérlési megoldással, a Novell Access Manager 3 platformok és címtárszolgáltatások széles körét támogatja. Hatékonyan működik olyan összetett, többgyártós környezetekben is, amelyek AIX, HP-UX, Linux, NetWare, Solaris és Windows platformokat tartalmaznak. A Kovács Úréhoz hasonló vállalatoknál ez kritikus szempont, hiszen a felvásárolt cégek más és más rendszereket használtak. A Novell Access Manager 3 lehetővé teszi, hogy megbízható biztonsági rendszert építsen ki egyszerű hozzáférés mellett anélkül, hogy szembesülnie kéne a költségekkel és nehézségekkel, amit egy frissen felvásárolt cég rendszerének lecserélése jelentene. Így nem kell külön foglalkoznia azokkal a partnerekkel, akik eltérő rendszereket vagy alkalmazásokat használnak.

> A Novell Access Manager 3 elősegíti a törvényi előírások betartását

Nem elhanyagolandó kérdéskör a törvényi előírásoknak való megfelelés sem: számos más vezetőhöz hasonlóan Kovács Úrnak is egyre szigorúbb kormányzati és törvényi előírásokat kell betartania. A Novell Access Manager 3 segít a cégeknek az információ és személyazonosságok megosztásában – a cégen belül és kívül egyaránt –, és automatikusan jelentéseket készít, amelyek segítenek a Sarbanes-Oxley, HIPAA és hasonló törvényi előírások betartásában.

> A biztonságos hozzáférést garantáló komponensek

A Novell Access Manager 3 kínálta különleges funkciók megismeréséhez tekintsük át, hogy a megoldás milyen régi és új összetevőkből épül fel.

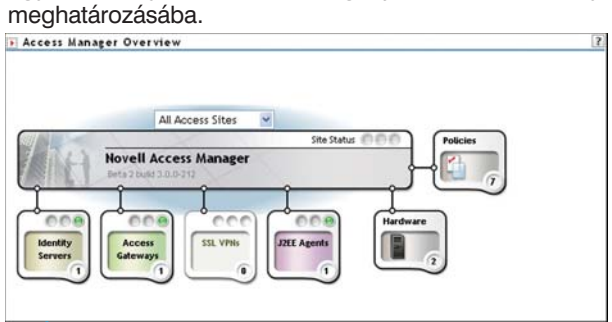
Szabványalapú egypontos bejelentkezés

Ma a számítástechnika világában nélkülözhetetlenek a jelszavak: nélkülük egyszerűen nem beszélhetünk biztonságról. A sors iróniája, hogy az utóbbi időben a jelszavak saját maguk is egy fontos biztonsági problémává váltak, mivel az embereknek túl sok jelszót kell megjegyezniük a munkájuk elvégzéséhez. Ennek eredménye, hogy a jelszavakat felírják és felragasztják a monitorokra, a billentyűzetekre és az iroda más, túlságosan is nyilvánvaló helyeire.

A Novell Access Manager 3 egypontos bejelentkezési technológiát használ. Ez azt jelenti, hogy az alkalmazottaknak és a partnereknek csak egyetlen jelszót kell megjegyezniük ahhoz, hogy elérjék a számukra engedélyezett adatokat – függetlenül attól, hogy azok pontosan hol is találhatóak, és ha szükség van rá, a Novell Access Manager 3 a hitelesítés kifinomultabb módszereit is támogatja.

Access Manager irányelvek

A Novell Access Manager 3 legnagyobb előnye az irányelvek felügyeletében és betartatásában rejlik. Ön az, aki meghatározza az irányelveket – azt, hogy az egyes felhasználók hogyan érhetik el az adott információt. A Novell Access Manager 3 ezután betartatja ezen irányelveket és naplózza az alkalmazásukat a későbbi megfelelési kimutatások számára. Arra is van lehetőség, hogy külső fejlesztők egyedi folyamatokat integráljanak az irányelvek meghatározásába.



1. ÁBRA: Az új menedzsment konzol központi helyet biztosít az összes komponens és irányelv konfigurálására és felügyeletére

Identity Server

A Novell Access Manager 3 „agya” – a személyazonosság-kezelő kiszolgáló – a kialakított irányelveket használja a felhasználók hitelesítéséhez és a jogosultság megadásának eldöntéséhez. Ez a kiszolgáló biztosítja a hitelesítési szolgáltatásokat a Novell Access Manager 3 összes komponensének, valamint állítja elő a szolgáltatásokat a Liberty Alliance és SAML (Security Assertion Markup Language) kérések számára. Ellentétben a korábbi változattal, a személyazonosság-kezelő kiszolgáló most már támogatja a SAML 1.1 és 2.0 verzióját is.

Egy másik technológia, amelyet a személyazonosság-kezelő kiszolgáló biztosít, az ún. egyesített létesítés (federated provisioning). Egyesíteni két vagy több, egymásban megbízó üzleti partner tudja rendszereit, megfelelő üzleti és műszaki megállapodások birtokában. E megállapodások alapján megoldható, hogy az egyik partner egy felhasználója problémamentesen elérhesse egy másik partner erőforrásait – szigorúan biztonságos, ellenőrzött módon.

Más megoldások megkövetelik, hogy ebben az esetben mind a két félnél – a személyazonosság szolgáltatójánál és a szolgáltatást biztosító félnél – már létezzen egy felhasználói fiók még azelőtt, hogy az egyesítés létrejönne. A Novell Access Manager 3 személyazonosság-kezelő kiszolgálója azonban képes automatikusan létrehozni a felhasználói fiókokat az egyesítési szolgáltatás kérései alapján. Ez azt jelenti, hogy a felhasználóknak nem kell regisztrálni magukat – azaz előre létrehozni egy felhasználói fiókot – a szolgáltatást biztosító félnél ahhoz, hogy átvihessék azonosságaikat.

Példaképpen képzeljük el légitársaságok az egész világra kiterjedő, egyesített rendszerét, amelyben utasok millióit szolgálják ki a világ több száz országában. Amikor Ténagy János csatlakozik a szövetséghez, a Novell Access Manager 3 automatikusan létrehoz egy fiókot János számára a Liberty használatát támogató szolgáltatásokat alkalmazó tag-légitársaságok mindegyikénél. A Novell Access Manager 3 ezután elvégzi János fiókjainak egyesítését. Az eredmény? János egyetlen jelszóval képes elérni a megfelelő utasadatokat a légitársaságok bármelyikénél. Ugyanazzal a jelszóval és ugyanazon egyszerű folyamat használatával János képes ellenőrizni, hogy mikor is indul a Lufthansa-járata, lefoglalni egy utat az ünnepekre a United Airlinesnál és bejelölni az ülésekre vonatkozó preferenciáit a jövő hónapi útján az Air New Zealanddal.

Access Gateway (hozzáférési átjáró)

Az Access Gateway a Novell Access Manager HTTP proxy komponense. Ez biztosítja azokat a díjnyertes biztonsági és proxyszolgáltatásokat, amelyekről a Novell méltán híres: vagyis az engedélyezést, az egypontos bejelentkezést és az adatok titkosítását. Ezenfelül összekapcsolódik a Novell Access Manager 3 új személyazonosság- és irányelv-kezelési szolgáltatásaival is. Az Access Gateway NetWare és Linux platformokon egyaránt elérhető, vagyis az informatikusok szabadon választhatják meg preferált platformjukat.

SSLVPN

Az SSLVPN biztonságos hozzáférést valósít meg a nem HTTP alapú alkalmazások felé. Az Access Gateway kiegészítőjeként biztonságos hozzáférést nyújt a vállalati erőforrásokhoz. Linuxos szolgáltatásként felgyorsítja az Access Gateway-t, amellyel meg is osztja adatait. A sikeres hitelesítés után egy Active-X bővítőmodult vagy Java kisalkalmazást tölt le a kliens.

A felhasználó szervezetben betöltött szerepe határozza meg, hogy a felhasználó jogosult-e elérni egy adott erőforrást. Ugyanez a szerep határozza meg, hogy hogyan reagálnak a háttéralkalmazások. Egy SSLVPN munkamenet kezdeményezése előtt az SSLVPN szolgáltatás ellenőrzi a kliens integritását és a szükséges szoftverek (például tűzfal és vírusvédelmi program) meglétét.

Java alkalmazásügynökök

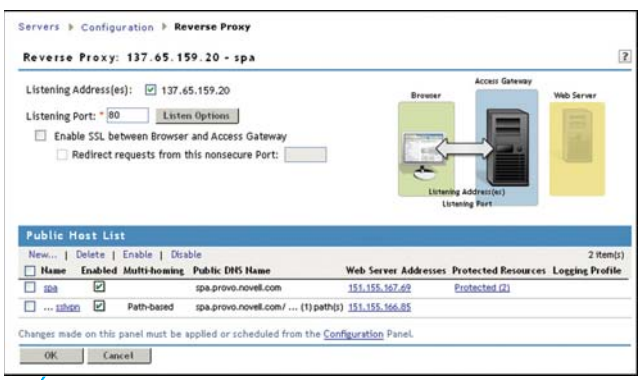
A NAM 3 három Java alkalmazáskiszolgáló ügynököt – IBM WebSphere, BEA Weblogic és JBoss – használ a hitelesítés elvégzésére. Ez a három ügynökprogram a JAAS és JACC mechanizmusokat, valamint belső webkiszolgáló API-kat alkalmaz. A működésük során a servletek és EJB-k hozzáférését szabályozó irányelveket is figyelembe veszik. Egyes esetekben a platformspecifikus API-k még szorosabb, még robusztusabb integrációt tesznek lehetővé.

SP ügynök

Az SP ügynök egy megosztott komponens, amely egységes implementációt biztosít a személyazonosság-kezelő protokollokhoz és az egyesítési szabványokhoz. Amikor beérkezik egy hitelesítési kérés, az SP ügynök automatikusan átirányítja a kérést a személyazonosság-kezelő kiszolgálóhoz. A személyazonosságkezelő kiszolgáló ezután visszaad egy SAML nyilatkozatot (assertion) a komponensnek. A bizalmas adatok védettek, hiszen a komponensek között nincs szükség a felhasználó hitelesítési adatainak cseréjére.

Felügyeleti konzol

A Novell Access Manager 3 felügyeleti felületén a rendszergazdák beállíthatják és felügyelhetik a termék összes komponensét és az általa kezelt irányelveket. Az egyes eszközök, ügynökök és irányelvek adminisztrációs felelősségei átruházhatók. Az új felügyeleti konzol képes csoportosítani is a hozzáférési átjárókat, vagyis a konfiguráció bármely módosítása teljesen egyidőben kerül továbbításra az összes átjáróhoz (lásd az 1. és a 2. ábrákat).



2. ÁBRA: A menedzsment konzol komponensei lehetővé teszik a Web böngészők és Web szerverek irányelveinek meghatározását, és a nyilvános listákhoz való hozzáférések menedzselését

> Összefoglalás

A Novell Access Manager 3 bevezetésével Kovács Úr képes volt megoldani a cég legkritikusabb eszközeinek és erőforrásainak védelmét. Ezzel egyidőben azt is tudja garantálni, hogy akinek szüksége van valamilyen információra, valóban elérhesse – függetlenül attól, hogy hol van, vagy milyen platformot használ. Sőt, a felhasználók számára egyszerűsítette a hozzáférést, az adminisztrátorok számára pedig megkönnyítette a felügyeletet.

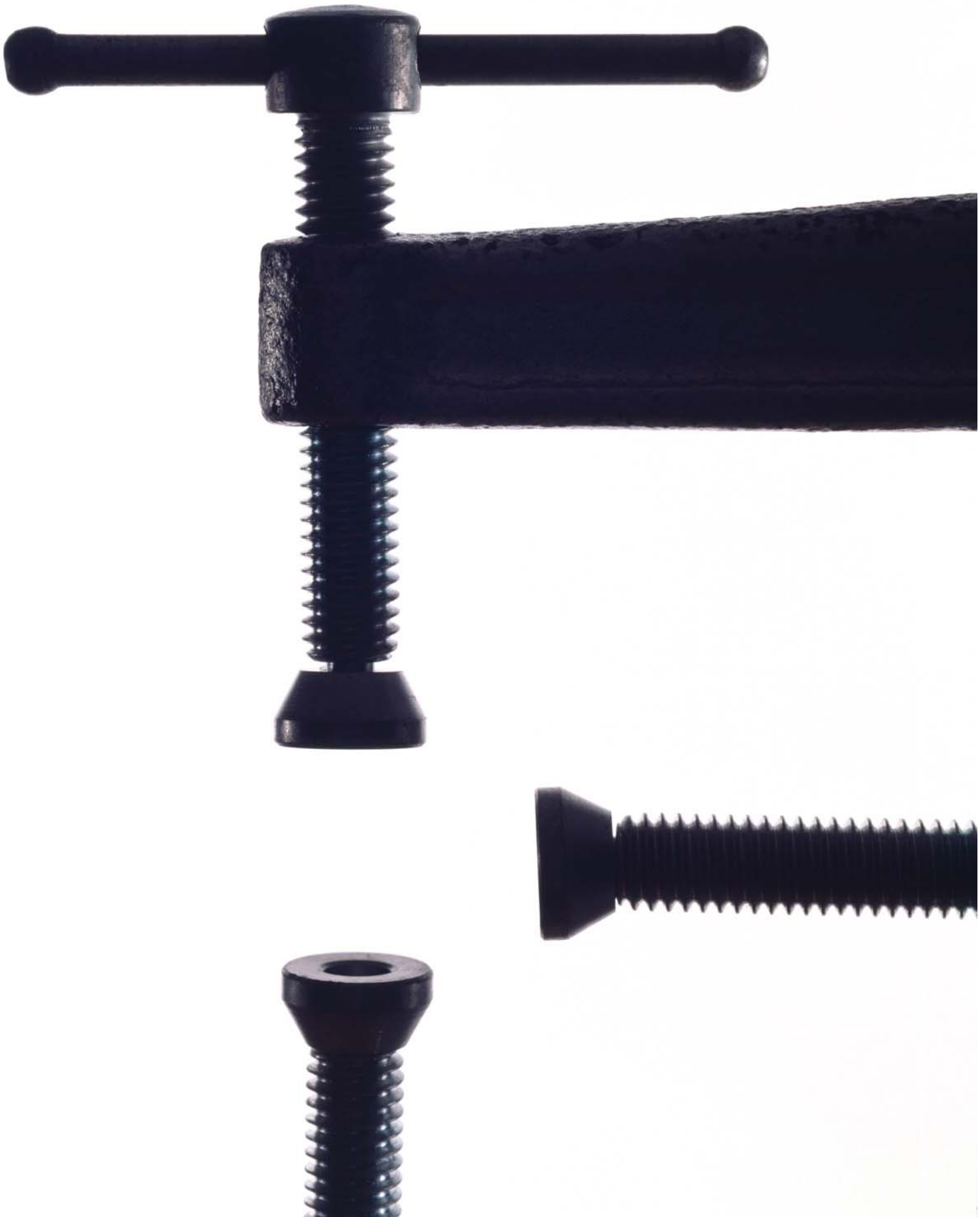
A Novell Access Manager 3 gyors és egyszerű hozzáférést biztosít az illetékesek számára, ugyanakkor távol tartja az arra nem jogosultakat. A számos új funkciót és csúcstechnológiás komponenst felvonultató új változat olyan kifinomult megoldás, amely hatékonyan biztosítja az infrastruktúra védelmét, megakadályozza az értékes információ eltulajdonítását és védi a felhasználók személyes adatait mind a szervezeten belül, mind azon kívül. A mai rohanó, kompetitív üzleti környezetekben nagy fontossággal bír egy ilyen biztonsági megoldás. N

TECHNOLÓGIA

„Aki mások nyomában jár, sohasem kerülhet elébük.”
–Michelangelo–

Az adatvédelmi partner
PC-biztonsági megoldás a SecureWave Sanctuary Suite segítségével

Novell Secure Login 6.0
Kiút a jelszavak és biztonsági előírások útvesztőjéből



Az adatvédelmi partner

PC-biztonsági megoldás a SecureWave Sanctuary Suite segítségével

A Sanctuary Suite egy olyan megoldás, amelylyel teljesen kézben tartható, hogy ki melyik I/O-eszközhöz férhet hozzá és milyen kódot/alkalmazást futtathat a számítógépén. A Sanctuary Suite pozitív modellt alkalmaz, nem fekete-listákkal dolgozik: alapértelmezésben megtiltja a hozzáférést minden eszközhöz és alkalmazáshoz, amíg azok használatára kifejezetten engedélyt nem adnak.

> Sanctuary Suite: A biztonság „fehérlistás” megközelítése

A mai cégek biztonsági és támogatási problémáinak elsődleges, legjelentősebb forrása a végfelhasználók valamint a személyi számítógépeik. A rosszindulatú szoftverek, a mobil adathordozók és kémszoftverek által okozott adatszivárgás, valamint a törvényi előírások betartatásával járó nehézségek aggasztják leginkább a vállalatok informatikai részlegeinek munkatársait.

A legtöbb meglévő biztonsági megoldás azonban képtelen gátat vetni a biztonsági fenyegetések egyre növekvő áradatának, elsősorban azért, mert a vállalati végpontok rendkívül sérülékenyek és még inkább azok lesznek, ahogy az új hardvertechnológiák és az egyenrangú hálózati (P2P-) alkalmazások elszaporodnak a piacon. Néhány évvel ezelőtt kevesen gondolták volna, hogy egy iPod biztonsági kockázatot jelenthet majd, és az egyes szervezeteket célba vevő üzleti kémszoftverek hulláma sem volt előre látható – mára azonban mindkét veszély napi realitássá vált.

A hagyományos biztonsági megoldások nem úgy készültek, hogy képesek lennének enyhíteni ezeket a kockázatokat – egyszerűen azért, mert negatív mintákra támaszkodnak, amelyekkel csak a fenyegetés megjelenése után reagálnak a tünetekre. A SecureWave Sanctuary Suite 3.2 azt a két legfontosabb összetevőt kínálja, az eszközfelügyeleti és alkalmazás felügyelet programmal, amelyre a vállalatoknak szükségük van a munkaállomások végrehajtható állományainak és mobil eszközeinek biztonságos kezeléséhez. A „fehérlistás” megközelítésnek köszönhetően hátat lehet fordítani a nemkívánatos alkalmazások, rosszindulatú szoftverek és jogosulatlan eszközök tömegeinek, helyette az ellenőrzésre és engedélyezésekre kell csupán koncentrálni.

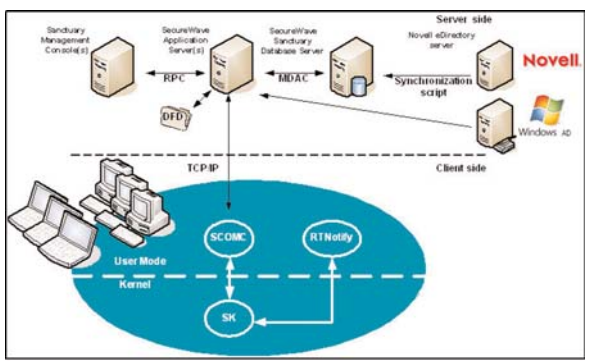
A Sanctuary Suite a Novell eDirectory-ban, vagy Microsoft Active Directory-ban tárolt felhasználói és felhasználócsoport-adatokhoz köti az alkalmazás- és eszközirányelveket, nagymértékben leegyszerűsítve a végponti alkalmazások és eszközerőforrások vállalati környezetben történő kezelését.

> A Sanctuary csomag felépítése

A Sanctuary csomag által használt architektúra a következő részekből áll:

- Alkalmazáskiszolgáló(k)
- Adatbázis (Microsoft SQL Server)
- Sanctuary felügyeleti konzol(ok)
- Sanctuary kliens(ek)

Az 1. ábra az architektúrát, valamint a kliens- és szerveroldali komponensek által használt kommunikációs útvonalakat és protokollokat mutatja be. Minden egyes Sanctuary-infrastruktúra saját adatbázist használ, ahol a felhasználói házirendeket és engedélyeket tárolja. Az adatbázis Microsoft SQL Server 2000/2005, vagy az ingyenes MSDE2000/SQL 2005 Express lehet. A hibatűrés érdekében az SQL Server adatbázis clusterbe is telepíthető. A kliensek és az alkalmazás-kiszolgáló közötti forgalom privát és nyilvános kulcsú titkosítási technológiákra épül, mely az elküldés előtt az adatokat is tömöríti.



1. ÁBRA: Kommunikáció a Sanctuary komponensek között

A hozzáférés felügyelete több helyről is elvégezhető. Nem kell fizikailag ott lenni egy számítógépnél egy adott felhasználó és/vagy gép engedélyeinek beállításához és módosításához.

A kliensekre egy kernelszintű illesztőprogramot (Sanctuary kliens), egy kommunikációs szolgáltatást (SCOMC) és egy értesítési szolgáltatást (RTNotify) telepítünk – ezek együttese

alkotja a tényleges Sanctuary klienst. A Sanctuary kliensoldali illesztőprogramja egy alacsony szintű kernel-illesztőprogram, amely Windows 2000/XP/2003/XPe munkaállomásokon fut, és akkor is kikényszeríti a házirendek alkalmazását, ha a többi szolgáltatás nem áll rendelkezésre. A kliens telepíthető a gépekre felügyelet nélküli telepítéssel is, például a Novell ZENworks Desktop Management használatával, a SecureWave saját klienstelepítő eszközével, bejelentkezési parancssorozatokkal és csoportházirendekkel, vagy bármely más telepítőeszközzel, amely támogatja a Microsoft System Installer (MSI) használatát. A Sanctuary kliens biztosítja, hogy az adott számítógépen csak a felhasználó számára engedélyezett eszközöket és alkalmazásokat használhassák. A tiltott eszközökhöz és alkalmazásokhoz való hozzáférést opcionálisan naplózza és blokkolja a program, függetlenül attól, hogy a felhasználó milyen számítógépről jelentkezett be.

A Sanctuary alkalmazáskiszolgáló (Application Server)

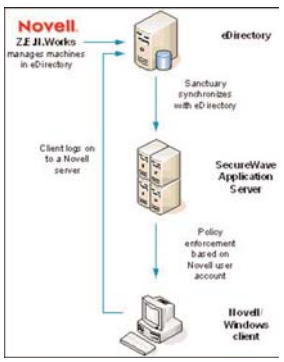
Egy Windows 2000/2003 szolgáltatás, amely a Sanctuary kliensekkel kommunikál és szétosztja az eszközökre és alkalmazásokra vonatkozó engedélyeket az egyes kliensgépeknek, illetve felhasználóknak vagy csoportoknak. Több alkalmazáskiszolgálóval kiegyensúlyozható a hálózati és hardverterhelés, illetve megoldható az átterhelés, ha az egyik valamiért kiesik.
A Sanctuary felügyeleti konzol az alkalmazáskiszolgáló(k)hoz csatlakozik az adminisztráció elvégzéséhez. Az adatbázissal folytatott kommunikációt az alkalmazásszerver(ek) végzi(k), kivéve a Novell eDirectory objektumokat, amelyeket egy parancsfájl szinkronizál.

Minden egyes alkalommal, amikor a felhasználó bejelentkezik, vagy a gép elindul, a kliensgép kernel-illesztőprogramja felveszi a kapcsolatot a SecureWave alkalmazáskiszolgálóval és lekéri a végrehajtásra engedélyezett fájlok listáját, valamint az eszközök hozzáférés-vezérlési listáját (Access Control List, ACL). Ezt követően (ha a gyorsítótárja üres) az alkalmazáskiszolgáló letölti a felhasználó számára futtatásra engedélyezett fájlok kivonatainak (hash) kriptográfiai technikákkal aláírt listáját, valamint az eszközök ACL-jét. A listákat tömörítés után továbbítja a kliensgépre. A végrehajtható fájlok engedélyezése egy biztonságos „ujjlenyomat” (kivonat) funkció (a FIPS szabvány SHA-1 algoritmusa) alapján történik.

A hozzáférés engedélyezése vagy megtagadása menet közben történik, a végfelhasználónak semmi teendője nincs ezzel kapcsolatban: a kliens illesztőprogramnak nincs is felhasználói felülete és a végfelhasználó sem avatkozhat be a működésébe. A Sanctuary folyamatosan védi az összes számítógépet, akkor is, ha éppen nem csatlakoznak a vállalati hálózathoz, például ha a noteszgépét a felhasználó lekapcsolta a hálózatról. Ha a kliens illesztőprogram bármely okból nem tudja letölteni a kivonatlistát, akkor a helyben tárolt listát használja egészen addig, amíg nem tud újra csatlakozni a kiszolgálók valamelyikéhez, vagy az engedélyeket nem tudja importálni egy biztonságos házirendfájlból.

> Eszközfelügyelet

A Sanctuary Device Control (eszközfelügyeleti program) az I/O-eszközök kezelését felügyeli úgy, hogy a felhasználók csak az engedélyezett eszközökhöz férhetnek hozzá. A program egy hozzáférés-felügyeleti listát (ACL-t) hoz létre. A jogosultságok megadásához csak hozzá kell rendelnie a szervezeti egységeket, felhasználókat vagy csoportokat az elérendő eszközökhöz és/vagy eszközosztályokhoz.



2. ÁBRA: eDirectory integráció

Eszközadminisztráció: egyszerű, gyors és rugalmas

A Sanctuary Device Control telepítése után az adminisztrátor azonosítja a szükséges akár szabványos vagy akár specifikus eszközöket és adathordozókat.

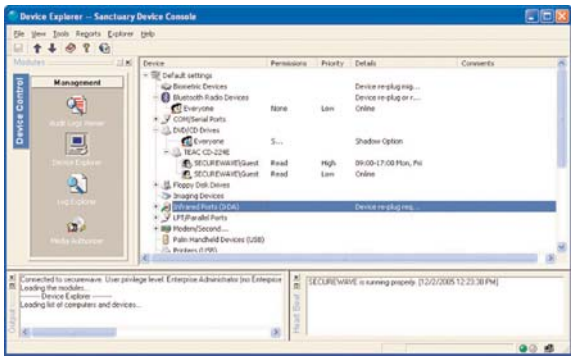
A következő lépésben az eszközök automatikusan hozzárendelésre kerülnek az előre meghatározott eszközosztályokhoz. Az adminisztrátor speciális eszközöket is megadhat típus vagy márkanév szerint. Végül pedig az egyes adathordozók (például a CD- és DVD-lemezek) kerülnek besorolásra a adathordozó listába. Az adminisztrátorok az eszközosztályok alapján oszthatják ki a jogosultságokat és hozzáférési attribútumokat; amikor az egyes eszközöket egy adott számítógéphez rendelik. A módosítások és a további felügyelet központilag, egy egyszerű grafikus felületen végezhető el.

Eszközök hozzáférés-vezérlése

Ha egy felhasználó el szeretne érni egy eszközt, akkor a Sanctuary Device Control illesztőprogramja kernelszinten érzékeli az operációs rendszertől jövő kérést. Ha az eszköz nincs benne az engedélyezettek listájában, a program megtagadja annak használatát. Ha az eszköz ismert (például benne van a listában), az illesztőprogram ellenőrzi a felhasználói jogosultságokat a hozzáférés-vezérlési listában. A jogosultság megléte esetén a felhasználó megkapja az eszköz használati jogát. Ha egy felhasználó nem jogosult egy eszköz elérésére, akkor „hozzáférés letiltva” üzenetet kap. A rendszer opcionálisan beállíthatóan, visszakereshető módon naplózza az eszköz elérésekkel kapcsolatos eseményeket is.

Támogatott eszköztípusok

A SecureWave Sanctuary Suite 3.2 használata során támogatott eszköztípusok az USB memóriák, a ZIP-meghajtók, a PDA-k, a szalagos, a merev- és hajlékonylemez-meghajtók, a biometrikus eszközök (pl. ujjlenyomatolvasó), a modemek, a vezeték nélküli hálózati adapterek, a digitális kamerák, a CD/DVD-lejátszók és írók, a lapolvasók, a chipkártyaolvasók és az USB nyomtatók.



3. ÁBRA: Jogosultságok és eszközök kezelése a Sanctuary Device Control Device Explorer segítségével

Támogatott kapcsolódási módok

A Sanctuary Device Control használatával az eszközök kapcsolódási módtól függetlenül felügyelhetők, legyen az USB, LPT, FireWire, Bluetooth, WiFi, IrDA, PCMCIA, COM, IDE, S-ATA vagy PS/2.

> Adathordozók engedélyezése és titkosítása

A Sanctuary-vel napi adatmásolási korlátok is beállíthatók a mobil adathordozókhoz és/vagy floppy-meghajtókhoz. Az összes engedélytípus egyszerre is alkalmazható. Akár „gyökérszintű" engedélyek is megadhatók. Az ilyen engedélyek az eszközböngésző gyökérobjektumához vannak rendelve és minden eszközosztályra egyformán érvényesek. Az ütemezett eszközhozzáféréssel az engedélyek meghatározott időtartamokhoz, illetve meghatározott ütemezéshez köthetők. Ezzel a funkcióval kifinomult biztonsági házirendek készíthetők, szabályozva például, hogy bizonyos eszközök csak hétfő és péntek között, reggel 9-től délután 5-ig használhatók. Az egyes felhasználókhoz online/offline engedélyek is rendelhetők, amelyben engedélyezik (vagy tiltják) számukra bizonyos eszközök használatát. Más eszközházirend vonatkozik rájuk amikor Internetet használnak, és más amikor nem.

A még nagyobb biztonság érdekében a Sanctuary Device Controllal megadható az is, hogy egy adott felhasználó csak bizonyos engedélyezett DVD-khez, CD-khez vagy más mobil adathordozókhoz férhessen hozzá. A vállalati DVD-k/CD-k használatát korlátozhatják azokra, akiknek ez kifejezetten engedélyezett és megtilthatják mások számára. A mobil adathordozókon tárolt adatok titkosíthatók is, így biztonságosan szállíthatók anélkül, hogy aggódni kellene amiatt, hogy a bizalmas adatokat arra jogusalatlan személyek is láthatják. A felhasználók olyan számítógépeken is hozzáférhetnek a titkosított adatokhoz, amelyeken nincsen telepítve a kliensszoftver, ha a Sanctuary Device Control önálló visszafejtő (Stand-Alone Decryption) eszközét vagy a Sanctuary Easy Exchange titkosítási módját használják. Az első esetben a felhasználónak rendelkeznie kell a Sanctuary önálló visszafejtő eszközével, a megfelelő jelszóval és titkosítási kulccsal. A második esetben csak egy jelszóra van szükség az adathordozó olvasásához.

> Hatékony auditálási és jelentéskészítési funkciók

A SecureWave nagyteljesítményű auditálási és jelentéskészítési funkcióival egyszerűbben követhető, hogy mit is használnak – vagy helytelenül használnak – a felhasználók és a rendszergazdák:

- A SecureWave szabadalmaztatásra benyújtott I/O-árnyékolási technológiájával kézben tarthatók az adatok (teljes fájlok, csak fájlnevek vagy adatfolyamok), amikor írható DVD-kre vagy CD-kre, mobil adathordozókra, hajlékonylemezekre, vagy éppen COM, LPT vagy modemportokra írják őket. Még az olyan műveleteket is naplózza a rendszer, ha például valaki egy másodpéldányt akar menteni az éppen lemásolt adatokról. A megfelelő jogosultsággal rendelkező személyek később megtekinthetik és megnyithatják ezeket az árnyék- vagy adatfolyam-másolatokat.
- Követhetők a felhasználók tevékenységei: az illegális hozzáférési próbálkozások a tiltott eszközökön, különféle eszközök csatlakoztatása és eltávolítása a számítógépeikről, megtekinthetők a kliens hibajelentései, valamint ha a felhasználó megpróbál az engedélyezettnél több adatot másolni.

Alkalmazások engedélyezése

Az ellenőrző összeg kiszámítása után az illesztőprogram ellenőrzi, hogy az aktuális felhasználó jogosult-e végrehajtani az alkalmazást. A hitelesítés akkor történik meg, amikor a fájl betöltődik a memóriába – tehát nem akkor, amikor a lemezről olvassák, vagy kiírják. Pozitív eredmény esetén engedélyezi a rendszer a végrehajtást; ellenkező esetben megtagadja, kivéve, ha az opcionális "helyi engedélyezés" (Local Authorization) funkció be van kapcsolva a felhasználó számára. A Sanctuary ezen kívül még véd a parancsfájlok (VBS, VBA, JScript) végrehajtása ellen is.

> Alkalmazásfelügyelet

A Sanctuary Application Control (az alkalmazásfelügyeleti program) az alkalmazások végrehajtását felügyeli: teljes ellenőrzést gyakorol a hálózat összes alkalmazásának végrehajtása felett.

A Sanctuary Application Control arra az elvre épül, hogy kifejezett engedély hiányában minden futtatható állomány használata tiltott. A feketelistás megközelítéstől eltérően, amely csak az ismert rosszindulatú szoftverek végrehajtását gátolja meg, az alkalmazott pozitív modell felsorolja az összes engedélyezett futtatható állományt, és tiltja az ismeretlen végrehajtható állományokra épülő vírusokat, trójai programokat, férgeket, kémszoftvereket és rendszerfigyelőket, és véd a nem kívánatos (illegális vagy licenc nélküli) szoftverek használatával szemben.

Egyszerű és rugalmas adminisztráció

A Sanctuary Application Control telepítése után az adminisztrátor azonosítja a felhasználók számára a munkavégzéshez szükséges alkalmazások (vagy más futtatható állományok) különféle forrásait, amelyek általános, vagy akár a szervezet szempontjából specifikus állományok is lehetnek. A Sanctuary Application Control által biztosított funkciók használatával egyszerűen összegyűjthető az összes azonosított futtatható fájl mintája.

A Sanctuary Application Control minden végrehajtható állományt megvizsgál és a beépített SHA-1 algoritmus használatával kiszámít egy egyedi digitális fájl lenyomatot

(ellenőrző összeget). A SecureWave tartalmaz előre kiszámított ellenőrző összegeket is a legtöbb Windows operációs rendszerhez (többféle nyelvűhöz is), valamint a rendelkezésre álló javítócsomagokhoz kapcsolódóan.

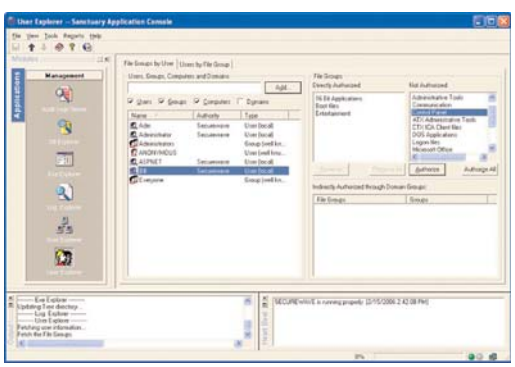
E lépés végrehajtása után a fájlok logikai úton fájlcsoportokba rendezhetők. Néhány fájlcsoport előre definiált, ezeket a Sanctuary Application Control felajánlja a konfiguráció megkönnyítésére, de létrehozhatók a szervezet igényeihez teljesen illeszkedő fájlcsoportok is.

A legutolsó fázis a fájlcsoportok hozzárendelése a különféle felhasználókhoz. Ez egyénenként vagy az eDirectoryban megadott felhasználói csoportok alapján is történhet, de a Windows hálózat és az Active Directory is támogatott a rendszerben.

> A Sanctuary alkalmazásvezérlés adminisztrációjának részletei

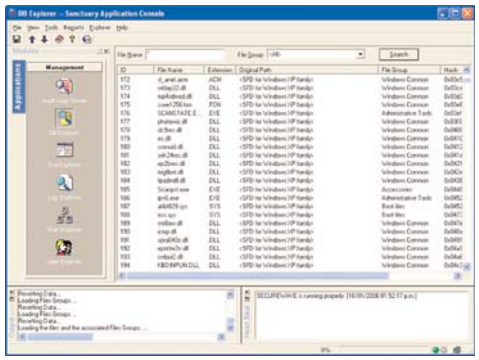
Azon túl, hogy számos eszköz megegyezik a Sanctuary eszközvezérlés adminisztrációjával, az alkalmazásvezérlés (Application Control) az alábbi funkciókat is biztosítja a Sanctuary felügyeleti konzolban:

- A felügyelendő végrehajtható fájlok listájának elkészítése a Scan Explorerrel: Egyszerűen használható megoldás teljes merevlemezek vagy azok részeinek átvizsgálására, új, vagy ismeretlen alkalmazásokat keresve. Különböző időpontokban pillanatfelvételek készíthetők a számítógépről, melynek segítségével megvizsgálható, hogy mely fájlok különböznek.
- A végrehajtható fájlok logikai fájlcsoportokba szervezhetők: a meglévő fájlcsoportok közül a Sanctuary javaslatot ad az újonnan felderített alkalmazásokhoz.
- SecureWave fájldefiníciók importálása: előre definiált aláírásliták a támogatott Microsoft operációs rendszerek többnyelvű változataihoz és szolgáltatáscsomagjaikhoz.
- Fájlcsoportok felhasználókhoz és felhasználócsoportokhoz rendelése a User Explorer eszközzel (lásd 4. ábra).



4. ÁBRA: Felhasználói jogosultságok beállítása

- Az Exe Explorer eszközzel választható ki, hogy a felhasználók mely végrehajtható fájlokat jogosultak futtatni.
- A Database Explorer a végrehajtható fájlok, illetve a hozzájuk tartozó, a Sanctuary adatbázisában tárolt listájának megtekintésére és karbantartására szolgál (lásd 5. ábra).



5. ÁBRA: Engedélyezett alkalmazások felügyelete

- Az engedélyezési varázslóval (Authorization Wizard) gyorsan azonosíthatók és engedélyezhetők a végrehajtható fájlok a hálózati mappákban, CD-ken és DVD-ken, vagy bármely más adatforráson. A felderítő alrendszer a népszerűbb tömörített fájlformátumokat (CAB, MSI, ZIP, RAR) is kezeli. A Windows Server frissítési szolgáltatásai is integrálhatók a Sanctuaryvel, megszüntetve a sűrű Microsoft-frissítések okozta problémákat.
- A Log Explorerrel részletekbe menően megvizsgálhatók a naplók. Minden egyes alkalommal, amikor egy kliensgép egy végrehajtható fájlt kér, létrejön egy naplóbejegyzés. A hozzárendelés részletei szükség esetén megtekinthetők és kezelhetők a megfelelő naplófájlokból. Az ismeretlen végrehajtható fájlok felügyelete is egyszerű, hiszen a Log Explorerrel egyetlen jobb egérkattintással engedélyezhetők.
- Beállíthatók a paraméterek, hogy a kliensgépek hogyan használják a Sanctuaryt.

> Közös jövőkép és kiforrott technológiák

A SecureWave egyetért a Novell személyazonosság-alapú szabályozásáról szóló stragtégiájával, hiszen napjainkban a blokkoló, korlátozó technológiák helyett az új technológiák kiaknázása az elsődleges cél, melyek segítségével minimálisra csökkenthető a kockázat. A Novell és SecureWave partnerkapcsolatának eredménye a hálózati végpontokon az alkalmazások és eszközök szabályozására kínált megoldás.

A SecureWave Sanctuary Suite a legjobb elsővonalas védekezés a rosszindulatú programok, nem kívánt alkalmazások, licenc nélküli programok és a jogosulatlan eszközhasználat ellen. N

Novell Secure Login 6.0

Kiút a jelszavak és biztonsági előírások útvesztőjéből

Egy átlagos hálózati felhasználó egy átlagos napon… megérkezik a munkahelyére és azon aggódik, hogy vajon ez lesz-e az a nap. Félve közeledik a számítógéphez, bekapcsolja. A bejelentkező képernyőn beírja a jelszavát és rákattint az OK gombra. Néhány másodperc múlva kiderül, hogy valóra váltak félelmei: a rendszer értesíti, hogy már csak 14 napja van egy új jelszó kitalálására. Felfordítja az egéralátétet, leszedi róla az éppen aktuális jelszót és kétségbeesetten próbál kitalálni valami olyat, amit még nem használt.

Ahogy beírta kedvenc papagája nevét, a rendszer közli, hogy a jelszónak még meg kell felelnie bizonyos biztonsági előírásoknak. Ilyen előírás például, hogy szerepelnie kell benne speciális karakternek, nagybetűnek, számnak, és persze nem lehet a jelszó túl rövid sem. Szomorúan néz körbe az íróasztalon, hátha eszébe jut valami jó... de semmi.

Így gondolkozik egy átlagos hálózati felhasználó. A legutolsó dolog, ami hiányzik neki, hogy még a jelszavakkal is foglalkoznia kelljen. Az ilyen felhasználó nem fog mindenféle, a hálózat biztonságát maximalizáló, matematikai alapú jelszósémát használni. Semmi mást nem akar, csak gyorsan megváltoztatni a jelszavát valami olyanra, amire még 10 perc múlva is emlékezni fog. Ha a rendszer jelszaván túl használnia kell egy hálózati alkalmazást, amelyhez meg kell adnia a felhasználói adatokat is a hitelesítéshez a lehető legegyszerűbb módszert fogja választani.

A felhasználó számára az a legegyszerűbb, ha ugyanazt a jelszót használja az alkalmazásokhoz, mint amelyikkel a rendszerbe jelentkezik be. Tekinthetjük ezt ún. „közös nevezőnek”, ahol a felhasználó egyetlen közös, könnyen megjegyezhető jelszót használ. Nem furcsa, hogy a hálózatot védő szigorú biztonsági irányelvek pontosan az ellenkező hatást érik el?

Érdemes figyelembe venni azt is, hogy a felhasználónak hány hálózati vagy internetes alkalmazást kell elérnie. Sok szervezetnél a felhasználóknak akár nyolc különböző rendszerrel vagy alkalmazással is kell dolgozniuk. Ilyen alkalmazás lehet például a vállalati CRM-rendszer (például SAP), az egyedi, belsőleg fejlesztett webes alkalmazások, vagy egy terminálemulátor a régebbi nagygépes alkalmazások eléréséhez.

Minden egyes alkalmazás saját jelszómódosítási irányelveket használ, és saját formázást követel meg. Jelen esetben az „egyforma jelszó minden alkalmazáshoz” nirvánája csak néhány napig tart, utána a jelszókövetelmények miatt kialakított kombinációk exponenciálisan nőnek – pokoli kínokat okozva ezzel a rendszergazdáknak és a felhasználóknak.

> A jelszófelügyelet látható és láthatatlan költségei

Szinte minden elemző különböző becsléssel rendelkezik ezen a téren, de átlagosan 25 és 50 dollár közé esik a nem megfelelően kezelt személyazonosságok és az elszabadult jelszófelügyelet tarifája – minden egyes alkalommal, amikor egy felhasználó betelefonál a helpdeskhez. Egy 10 000 felhasználós szervezet esetében például évi 100 000 dollárról beszélünk. Ez az éves, direkt költség ráadásul figyelmen kívül hagyja, hogy milyen egyéb járulékos költségeket jelent a termelékenység kiesése, amíg a felhasználók a jelszavaik visszaállítására várnak.

> Barát vagy ellenség a JAEA módszer?

A felhasználók annak érdekében, hogy áthidalják a jelszavak okozta problémát, gyakran alkalmazzák a JAEA módszert. A JAEA módszer – vagyis „Jelszó Az Egéralátét Alatt” – sokat segít a felhasználóknak abban, hogy megjegyezzék jelszólistáikat anélkül, hogy feljegyeznék azokat a táblázatkezelő programban, vagy memóriatréningre járnának. Ez azonban csak az adott hálózati felhasználó problémáit csökkenti, viszont megnöveli azokét, akik a hálózat védelmével foglalkoznak. A legtöbb szervezetnél évek óta harcolnak a JAEA módszer ellen. Minél nagyobb erővel próbálják kikényszeríteni a biztonságot a hálózaton belül, annál kevésbé sikerül megvalósítani a gyakorlatban. A Novell SecureLogin legújabb verziója azonban segít eligazodni a jelszavak bonyolult rendszerében.

> A megoldás: Novell SecureLogin 6.0

A Novell SecureLogin 6.0 gyors és egyszerű hozzáférést biztosít a vállalati erőforrásokhoz, egyetlen, biztonságos bejelentkezéssel. A felhasználóknak csak egyszer kell bejelentkezniük a hálózatba, utána a SecureLogin automatizálja a hozzáférést a többi alkalmazáshoz és erőforráshoz. A SecureLogin 6.0 a rendszergazdák számára lehetővé teszi a hitelesítési adatok felügyeletét, mivel automatikusan kezeli a jelszavakat az összes hálózati alkalmazás és az összes végfelhasználó számára. Biztonságos jelszókezelési irányelvek kialakításával, majd a felhasználókhoz és a hálózati

A felhasználó számára az a legegyszerűbb, ha ugyanazt a jelszót használja az alkalmazáshoz, mint amelyikkel a rendszerbe bejelentkezik. Tekinthetjük ezt ún. „közös nevezőnek”, ahol a felhasználó egyetlen közös, könnyen megjegyezhető jelszót használ. Hát nem furcsa, hogy a hálózatot védő szigorú biztonsági irányelvek pontosan az ellenkező hatást érik el?

alkalmazásokhoz rendelésével számos előnyt biztosít a szervezet számára:

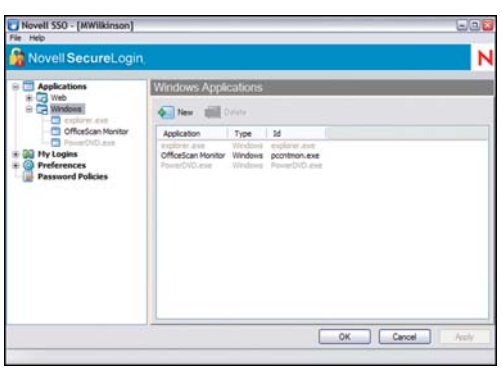
- növelhető a hálózati adatok és alkalmazások biztonsága a szigorú jelszókezelési előírások és irányelvek révén, anélkül, hogy a felhasználókat hátráltatná a munkavégzésben;
- csökkenthetők a helpdesk költségei a jelszavakkal kapcsolatos problémák számának csökkentésével;
- növelhető a felhasználók termelékenysége, mivel egyszerűbben elérhetik a szükséges hálózati alkalmazásokat, és kevesebb időt kell tölteniük a jelszavakkal kapcsolatos problémáik megoldásával (hátráltatva ezzel a helpdesket is);
- betarthatók a személyazonosság nyilvántartására, a személyes adatok kezelésére, az irányelvek betartására, valamint az auditálásra és a hitelesítési szolgáltatásokra vonatkozó új törvényi előírások.

> Újdonságok a SecureLogin 6.0 -ban

A Novell SecureLogin 6.0 számos újdonságot tartalmaz, például megújult felhasználói kezelőfelületet, továbbfejlesztett felügyeleti funkciókat, ezen belül integrációt az iManagerrel. Az iManager folyamatosan átveszi a ConsoleOne helyét, és ez az integráció segít abban, hogy az összes felügyeleti segédprogram elérhető legyen a webről. További újdonság még a Mozilla Firefox támogatása, egy új webes varázsló, gyárilag sokkal több alkalmazás támogatása, valamint speciális biztonsági eljárások, például intelligens kártyák és biometriai eszközök kezelése.

> Új felhasználói kezelőfelület

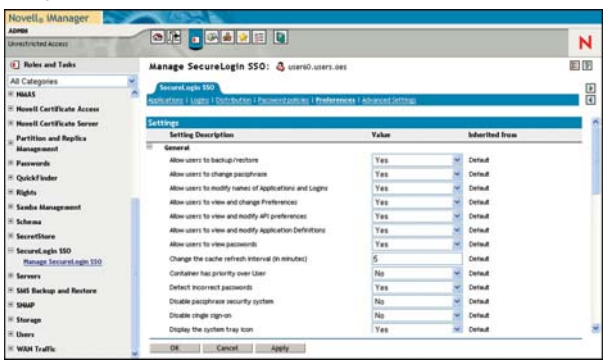
A SecureLogin 6.0 kezelőfelülete átalakult az egyszerűbb kezelés érdekében. Az új felület egy két részre osztott képernyőből áll, a bal oldalán egy tallózható faszerkezettel, a jobb oldalon pedig a felhasználó beállításaival és lehetőségeivel (lásd 1. ábra). A Novell ábrákkal színesítette a felületet az eszközök, beállítások és a felhasználói adatok jobb azonosításához. Az ügyfelek visszajelzései alapján a program intuitívabban is működik, például új alkalmazásdefiníciók vagy hitelesítési adatok létrehozásakor és módosításakor.



1. ÁBRA: A SecureLogin 6.0 új felhasználói felülete

> Továbbfejlesztett felügyeleti funkciók

A SecureLogin 6.0 integrálható – és felügyelhető – az iManagerrel, a Novell webes felügyeleti segédprogramjával. A 6.0 változat immár lehetővé teszi csoportos irányelvek (Group Policies) használatát is, leegyszerűsítve az alkalmazások hozzáférésének és a hitelesítési adatoknak a felügyeletét. A csoportos irányelvek kibővítik a jelenlegi felhasználói és konténer alapú felügyelet lehetőségeit: nagyobb rugalmassággal alakíthatók ki és szabályozhatók a biztonsági irányelvek (lásd 2. ábra).



2. ÁBRA: A SecureLogin 6.0 integrált az iManager-rel, a Novell webes felületi konzoljával

Ha címtárként LDAP-t használ, vagy több címtár is van a cégnél a felvásárlások és fúziók miatt, akkor egy új eszköz segít a hozzáférési jogok kezelésének leegyszerűsítésében. Az LDAP módban használható eszköz egy faszerű segédprogrammal teszi lehetővé az LDAP objektumok böngészését, valamint a jogok hozzárendelését. Korábban fejből kellett tudni (és kézzel be kellett írni) az objektum teljes minősített nevét a helykontextussal együtt. Emiatt könnyű volt hibát véteni, de az új segédprogram segít a hibák kiküszöbölésében.

> A Mozilla Firefox támogatása

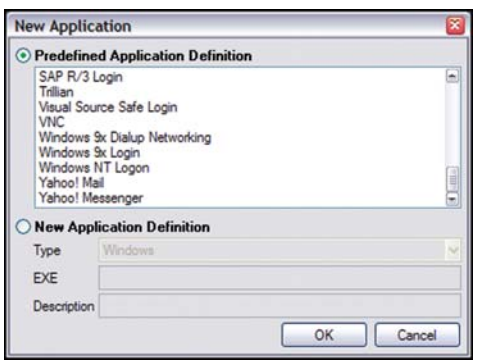
Az új verzió kiemelkedő újdonsága, hogy a webes varázsló már támogatja a Mozilla Firefox használatát is. A Mozilla szerint mára már több mint 100 millióan töltötték le a Firefoxot. Az Internet Explorernél biztonságosabb böngészőt ma már sok vállalat használja és vezette be céges szabványként. Az új Firefox-támogatás egyik előnye, hogy a Firefox alatt elkészített parancsfájlok és alkalmazásdefiníciók Internet Explorer alatt is működnek, és fordítva. Kevés olyan hely van, ahol csak az egyik böngésző van telepítve. A Firefox-támogatás révén hatékonyabbá válik a belső elérés, főleg akkor, ha új biztonsági irányelveket vezetnek be a szervezetben.

Egyes speciális funkciókkal lerövidíthető a bejelentkezés ideje egy alkalmazásba, és leegyszerűsíthető a bejelentkezés folyamata. Lehet például, hogy be kell jelentkezni egy távoli rendszerbe, ott el kell indítani egy alkalmazást, abba megfelelően be kell jelentkezni, esetleg meg kell válaszolni

kérdéseket vagy reagálni kell felugró ablakokra, majd ezek után még el kell érni az alkalmazáson belül a kívánt részt. A SecureLogin a teljes folyamatot automatizálja: mindössze egyetlen alkalmazásikonra kell csak kattintani.

> Még több alkalmazás támogatása

Kibővült a SecureLogin alkalmazásdefiníciós könyvtára is, amely már számos windowsos alkalmazást támogat: például az SAP-t, az SQL Servert, a Novell GroupWise-t; egy sor terminálalkalmazást; valamint számos népszerű webhely, mint a Yahoo!Mail vagy a Hotmail konfigurációit (lásd 3. ábra). A SecureLogin már támogatja a Java alapú alkalmazásokat is és olyan speciális funkciókat tartalmaz, amelyekkel az összetett webes alkalmazások speciális követelményei is teljesíthetők. Beállítható akár úgy is, hogy keresse a SecureLogin előtt betöltődő alkalmazásokat, mint például az iFoldert, és átadja a szükséges adatokat a hitelesítésre várakozó alkalmazásoknak.



3. ÁBRA: A SecureLogin 6.0 azonnali támogatást nyújt számos Windows alkalmazáshoz, terminál-alapú alkalmazáshoz és számos népszerű weboldal konfigurációjához

> Továbbfejlesztett webes varázsló

A továbbfejlesztett webes varázsló a 6-os verzióban az egypontos webes bejelentkezési folyamatot gyorsabbá és egyszerűbbé teszi mindenki számára. Amikor a felhasználó első alkalommal jár egy olyan weboldalon, ahol hitelesítési adatokat kell megadnia, megjelenik a SecureLogin webes varázslója. A felhasználónak be kell írnia a szükséges hitelesítési adatokat, amelyeket a program rögzít a későbbi felhasználáshoz. Ezzel az egyszerű, egylépéses folyamattal kényelmesen, akadálymentesen – és mégis biztonságosan – tekinthető meg legközelebb a weboldal (lásd 4. ábra).

4. ÁBRA: Az egypontos bejelentésen keresztül a SecureLogin automatizálja a felhasználók bejelentkezési folyamatát az olyan oldalak újralátogatása során, ahol hitelesítésre vagy azonosításra van szükség

Egyes speciális funkciókkal lerövidíthető a bejelentkezés ideje egy alkalmazásba és leegyszerűsíthető a bejelentkezés folyamata. Előfordulhat például, hogy be kell jelentkezni egy távoli rendszerbe, ott el kell indítani egy alkalmazást, abba megfelelően be kell jelentkezni, esetleg meg kell válaszolni

kérdéseket vagy reagálni felugró ablakokra, majd ezek után még el kell érni az alkalmazáson belül a kívánt részt. A SecureLogin a teljes folyamatot automatizálja: mindössze egyetlen alkalmazásikonra kell csak kattintani.

> Speciális hitelesítési módszerek

A SecureLogin már beállítható a Novell Modular Authentication Services használatához, tovább fokozva a biztonságot a kulcsfontosságú helyeken. Az emelt szintű biztonsági lehetőségek közé tartozik az intelligens kártyák, tokenek és biometriai eszközök használata.

Az intelligens kártyák általában hitelkártya méretűek, és található rajtuk egy programozható lapka, amely nemcsak adatok tárolására, hanem kriptográfiai funkciók elvégzésére is alkalmas.

A tokenek kis, kulcstartó méretű eszközök, amelyek egyszer használatos jelszavakat generálnak a hitelesítéshez. Többféle elven is működhetnek, de a leggyakoribb az, amikor a felhasználó megadja hitelesítési adatait, és kap egy véletlenszerűen hozzárendelt számot. Ezt kell beírnia a tokenbe, amely erre kiad egy, a hitelesítéshez használható választ.

A biometriai eszközök olyan berendezések, amelyek az emberi test egyedi jellemzőit vizsgálják és hasonlítják össze ezek tárolt változatával. Ilyen jellemző lehet például egy ujjlenyomat, a retina mintázata, vagy éppen az arc jellegzetességei. A bizalmas adatokhoz vagy alkalmazásokhoz való hozzáférés engedélyezés előtt az intelligens kártyák, tokenek és biometriai eszközök használata kombinálható a stratégiai területek védelme érdekében. A Novell Modular Authentication Services e speciális biztonsági eszközeinek használatával teljesen kézben tartható a hozzáférés az adatokhoz. A SecureLogin nyomon követi és rögzíti a hálózati hitelesítési és a hozzáféréssel kapcsolatos eseményeket, amely adatokból később a Novell Audit segítségével auditálható jelentések készíthetők.

> Összefoglalás

A jelszókezelés és a személyazonossági adatok felügyelete fontos területek, amelyekre komolyan oda kell figyelni, különösen a nagy szervezetek esetében. Manapság a legtöbb szervezetnél ezekkel a kérdésekkel sajnos úgy foglalkoznak, hogy a tüneteket kezelik a valódi problémák megoldása helyett. A SecureLogin 6.0 minden olyan funkciót tartalmaz, amellyel kézben tarthatók a hálózatok a költségek csökkentése és a rendszerek biztonságának növelése mellett úgy, hogy közben még a felhasználók termelékenysége is növekszik. Emellett elősegíti és megkönnyíti a törvényi és egyéb iparági előírásoknak való megfelelést. Leegyszerűsíti mind a rendszergazdák, mind a JAEA jelszókezelési módszert alkalmazó felhasználók munkáját. A nem megfelelően kezelt személyazonosságok és az elszabadult jelszófelügyelet tarifájának lecsökkentésére pedig szintén a SecureLogin 6.0 a megoldás. N

SUSE Linux Enterprise Server + IBM software + IBM hardware = AVNET

A Novell új SUSE megoldását az Avnet Partner Solutions ajánlata egészíti ki: a SUSE Linux IBM System x szerverhez a cég az alábbi szoftvereket kínálja Önnek csomagárban:

- Novell SUSE, Linux Enterprise Server 1 éves előfizetéssel
- IBM WebSphere, Application Server Community Edition
- IBM DB2 Express-C
- Centeris Likewise, Management Suite 1 éves előfizetéssel (Windows környezeti integrációs szoftver)

Az Avnet Technology Solutions Kft. **a fenti szoftvercsomagokhoz a következő IBM System x szervereket ajánlja Önnek**:

System x 226 + az Avnet szoftvercsomagja,

Intel Xeon 3.0 Ghz, 1GB RAM, 2x73 GB SCSI,
RAID 0,1, torony kivitel, 3 év helyszíni garancia
319.900 Ft + áfa

System x 3400 + az Avnet szoftvercsomagja,

Intel Xeon 1.86 GHz dual core (Woodcrest), 1 GB RAM,
2x160 GB SATA II, RAID0,1,10, 2x835 W redundáns táp,
torony kivitel, 3 év helyszíni garancia
439.900 Ft + áfa

System x 3650 + az Avnet szoftvercsomagja,

Intel Xeon 2.33 GHz dual core (Woodcrest), 1 GB RAM,
3x146 GB SAS, ServreRAID 8k, 2x835 W redundáns táp,
rack 2U kivitel, 3 év helyszíni garancia
769.900 Ft + áfa

Ha ajánlatunk felkeltette érdeklődését, kollégáink szívesen állnak rendelkezésére.
További információkat és részleteket Timár Tibor IBM termékmenedzsertől kaphat a következő elérhetőségeken:
e-mail: **tibor.timar@avnet.com**
telefon: **06-1-888-2-333**
Szoftver és hardver ajánlatunk a készlet erejéig tart.

Avnet Partner Solutions - www.avnet.hu

Várja nyugodtan a BSA ellenőreit!

ZENworks Asset Management, a Novell által kínált piacvezető megoldás szoftver-gazdálkodásra, amely a BSA által is elfogadott szoftveraudit eszköz.