

Biztonság már a mobil végpontokon is



Ma már elképzelhetetlen a kommunikáció mobil készülékek nélkül – de vajon biztonságosan használjuk őket?

A világ folyamatosan változik és az információbiztonsággal kapcsolatos munkának valójában soha sincs vége. Ez annak köszönhető, hogy gyakorlatilag fegyverkezési versenyben állunk a számítógépes bűnözőkkel. Folyamatosan változnak az üzleti prioritások és folyamatok, és ezek változásával egyidőben változniuk kell a biztonsági intézkedéseknek is. Az üzleti folyamatok egyik biztonsági környezetét is átformáló változása a mobilitás terjedése. Korábban a cég központjában egy nagyszámítógépen vagy szerveren tárolt adatokat most laptopok ezreire tárolják. A hálózat régen statikus kábelek kötegeit jelentette, most a vezeték nélküli kapcsolatoknak köszönhetően dinamikusan változik. A kiszámítható hálózati útvonalakon áramló adatok a hálózati figyelő- és felügyeleti eszközök számára észrevétlenül most sok gigabájtos, apró méretű USB-meghajtókon cserélnek gazdát.

Ezek a változások azt jelentik, hogy a régi típusú biztonsági megoldások nem elegendőek többé. Szükség van rájuk, de nem jelentenek megfelelő védelmet az új generációs fenyegetések ellen. Amiatt is aggódni kell, hogy megpróbálnak betörni a hálózatba és ellopják a szerverről a kritikus fontosságú adatokat. De mi van ezeknek az adatoknak a vezetők céges gépein található változatával? Mi értelme van egy jól működő peremtűzfalnak, ha a laptopot a taxiban felejtik vagy WiFi hot-spot nem biztonságos hálózatán használják?

> Az új problémákhoz új megoldások kellenek

A hagyományos biztonsági intézkedéseket olyan új megoldásokkal kell kiegészíteni, amelyek közvetlenül az új fenyegetéseket veszik célba. Ezért vásárolta fel a Novell a Senforce Technologies-t, és ezért is jelent meg ZENworks Endpoint Security Management termék.

A ZENworks Endpoint Security Management lehetőséget biztosít a biztonsági rendszergazdáknak a végpontokra (például munkaállomásokra és laptopokra) vonatkozó céges biztonsági irányelvek központi meghatározására, valamint ezek állandó és folyamatos kikényszerítésére. A kikényszerítés kernelszintű illetzőkkel történik, így akkor sem sérül a biztonság, ha a számítógép lekapcsolódik a hálózatról, vagy nem használják. A céges irányelvek kikényszerítésének és a központosított felügyeletnek az előbbieken leírt kombinációja rendkívül fontos a megfelelő kockázatkezeléshez. Abban az esetben, ha a felhasználók maguk hozzák meg a saját biztonságukra vonatkozó döntéseket, jónéhány problémával kell majd

szembesülniük a rendszergazdáknak:

1. Gyakran kell megzavarniuk a felhasználót feladatai teljesítése közben.
2. El kell érni, hogy a felhasználó amatőr biztonsági szakemberré váljon, ami elkerülhetetlenül azt jelenti, hogy rossz döntések is születnek majd.
3. Nem lehet megvalósítani az egységességet a cégen belül, nem biztosítható az előírásoknak való megfelelés.

> A szolgáltatások hatóköre rendkívül fontos

Mivel a mobilitás nem csak műszaki kérdés, hanem alapjaiban változtatja meg a technológia használatát, ezért biztonsági kérdések egész sorát veti fel. A ZENworks Endpoint Security Managementet úgy tervezték, hogy többféle kikényszerítési mechanizmust kínáljon egyetlen integrált felügyeleti keretrendszeren belül, amelyeket egyetlen ügynökprogram hajt végre. Ezek a mechanizmusok az alábbiak:

1. rendkívül részletesen ellenőrzik a bejövő és kimenő csomagok áramlását egy végponti tűzfal használatával,
2. mindenre kiterjedő felügyeletet látnak el a vezeték nélküli használat fölött, például lehetőséget adnak a rendszergazdák számára:
 - a vezeték nélküli használat teljes letiltására
 - a hozzáférési pontokról szóló fehér lista készítésére (hogy ne véletlenszerűen történjen a felkapcsolódás), vagy
 - minimális titkosítási normák kikényszerítésére (például hogy elfogadható minimumként követelje meg a WPA használatát és utasítsa el a WEP-et),
3. biztosítják a hordozható eszközök átfogó felügyeletét, így a rendszergazdáknak lehetősége nyílik az ilyen eszközök teljes tiltására, az engedélyezett fehér listába sorolására, illetve csak az olvasási használat engedélyezésére,
4. úgyszintén lehetőséget adnak a hordozható eszközre kiírt adatok automatikus titkosításának kikényszerítésére és/vagy a merevlemezen tárolt adatok titkosítására a fájl-/könyvtárinformációk alapján,
5. a rendszergazdák kikényszeríthetik a felhasználóktól a vállalati VPN használatát,
6. a rendszergazdák lehetőséget kapnak arra, hogy kézben tartsák, mely alkalmazásokat lehet végrehajtani a végpontokon,
7. lehetőség nyílik a ZENworks Security Client használatára annak érdekében, hogy a biztonsági eseményekre automatikus válaszokat adhasson a rendszer, hogy rendszergazdai beavatkozás nélkül valós idejű, parancsfájlokkal meghatározott műveleteket hajthasson végre válaszul,

**Mindezek a változások azt jelentik,
 hogy a régi típusú biztonsági megoldások
 (mint például a peremtűzfalak és a peremhálózati vírusellenőrzők) nem elegendőek többé.
 Még mindig szükség van rájuk,
 de nem jelentenek megfelelő védelmet az új generációs fenyegetések ellen.**

8. irányelvekkel vezérelhető lesz az összes fizikai port és protokoll működése (Bluetooth, IrDA, soros és párhuzamos port, modemek stb.)

Ezek a szolgáltatások valós időben működnek és nincs szükségük a felhasználó beavatkozására.

> **Hogy működik mindez?**

Az architektúra

A megoldás több különböző elemet tartalmaz. Amint az 1. ábrán is látható, ezek az alábbiak:

ZENworks Security Client: A ZENworks biztonsági kliens az az ügynökprogram, amely a végpontokon kikényszeríti a biztonsági intézkedéseket. Ez a biztonság „karja”, míg a központilag létrehozott irányelvek alkotják az „agyat”.

Policy Distribution Service: Az irányelv-szétosztási szolgáltatás felelős a biztonsági irányelvek eljuttatásáért a ZENworks Security Client-ekhez, és ez fogadja a kliensek jelentési adatait is. Az irányelv-szétosztási szolgáltatás telepíthető a demilitarizált zónában (DMZ), a vállalati tűzfalon kívül a mobil végpont rendszeres irányelv-frissítéseinek biztosításához. Ez azt jelenti, hogy a kliensek LAN-kapcsolat nélkül is frissíthetők.

Management Service: A felügyeleti szolgáltatás a hálózat egy biztonságos pontján található. Felelős a felhasználói irányelvek társításáért, az összetevők hitelesítéséért, a jelentési adatok beolvasásáért, a jelentések készítéséért, illetve a tárolási és biztonsági irányelvek létrehozásáért.

Management Console: A felügyeleti konzol a rendszergazdák által használt felhasználói felület, amely vagy közvetlenül a felügyeleti szolgáltatást futtató szerveren fut, vagy egy másik munkaállomáson, amely biztonságos hozzáféréssel rendelkezik a felügyeleti szolgáltatás szerveréhez. A felügyeleti konzolt a felügyeleti szolgáltatás beállításához, a felhasználói és csoportirányelvek létrehozásához és felügyeletéhez használják. Az irányelvek létrehozhatók, másolhatók, szerkeszthetők, szétoszthatók vagy törölhetők.

Client Location Assurance Service: A kliens helyét ellenőrző szolgáltatás – melynek használata nem kötelező – titkosított módon garantálja, hogy a ZENworks Security Client valóban a megadott helyen található. További részletek a későbbi Hely, hely, hely bekezdésben.

Irányelvek létrehozása és szétosztása

Az irányelvek létrehozására a felügyeleti konzol használható. Ez egy egyszerű grafikus felület a rendszergazdák biztonsági igényeinek megadásához. Ha például el szeretné kerülni azokat a fenyegetéseket, amelyek abból származnak, hogy a felhasználók egyidőben csatlakoznak vezeték és valamilyen más – esetleg veszélyes – vezeték nélküli hálózatra, egyszerűen jelölje meg a „no wireless when wired” (vezeték nélküli hálózat letiltása, ha van vezeték) lehetőséget. Az irányelv-szétosztási szolgáltatás igénybevételevel történő felügyelet során, az irányelvek egy XML BLOB állományban gyűlnek össze, amit a rendszer tömörít, AES-256 kódolással titkosít és digitálisan aláír, mielőtt szétküldené a végpontokra.

Hogy működik az ügynökprogram?

A végpontokon a kikényszerítést első sorban kernelszinten működő illesztők végzik. A végpont tűzfala például egy hálózati illesztőfelület-specifikációs (Network Driver Interface Specification, NDIS), köztes miniport-illesztőt használ arra, hogy a csomagokat egy alacsony hálózati réteg szintjén szűrje. A ZENworks Security Client hatékony, biztonságos csomagszűrést biztosít azzal, hogy a csomagokat azonnal elfogja, amint feljebb érnek a hardverabsztrakciós rétegből. Az architektúra kliensen belüli előnye az is, hogy a kernelszintű illesztők a felhasználó által generált forgalmon kívül látják azt a belső felügyeleti forgalmat is, amit az operációs rendszer használ az alapvető szolgáltatásokhoz. Az olyan vezetékek nélküli funkciók, mint a látható hozzáférési pontok „bejárás táblája” keresztülhalad a kernel ZENworks Security Client által felügyelt részein, és az ügynök szűrheti ezeket az irányelvben található fehérlista szerint. Ezzel a rendszergazdák könnyen kézben tarthatják, hogy a felhasználók melyik hozzáférési pontokhoz csatlakozhatnak, amely jelentősen csökkenti a véletlen kapcsolódások okozta veszélyeket. Mivel a szűrés kernelszinten, nem pedig alkalmazásszinten történik, a szűrés minden vezeték nélküli felügyeleti alkalmazásnál működik (lásd 1. ábra).



1. ÁBRA: A ZENworks Endpoint Security Management központilag meghatározott irányelveket szállít és aktívan betartatja azokat a végpontokon – függetlenül azok helyétől

A hálózati szinten működő illesztők nem tudnak a korábbiakban leírt összes biztonsági kényszerítő intézkedést végrehajtani. A ZENworks Security Client számos más illesztőt is használ, amelyek a fájlrendszer szintjén fejtik ki tevékenységüket, például adattitkosítást végeznek, vagy ellenőrzik a hordozható eszközök titkosítását. A ZENworks Endpoint Security Management terméknek is vannak mobil adathordozókra vonatkozó biztonsági funkciói.

Nagyvállalati működés

A ZENworks Endpoint Security Management a nagyvállalati piacra készült termék számos olyan funkciójával rendelkezik, amely növeli a hatékonyságot és teljesítményt. Ilyen funkciók például az alábbiak:

1. Felhasználókra vagy gépekre vonatkozó irányelvek. Nem lehet olyan „konfekció”-irányelveket készíteni, amelyek

Fontos, hogy a biztonsági beállításokat központilag lehessen megadni és felügyelni.

Ellenkező esetben még csak nem is állíthatja, hogy vannak biztonsági irányelvek: csak néhány jó cél van és néhány rosszul használt biztonsági eszköz.

minden cégnek egyformán megfelelőek. A vezetők munkaprofilja (és fenyegetési profilja) alapjaiban eltér a támogatási csoport munkatársaitól, mint ahogy a kereskedőké is a belső informatikai rendszert biztosítókétól. Amire szükség van – és amire a ZENworks Endpoint Security Management lehetőséget ad – az az, hogy különböző irányelveket lehessen létrehozni az egyes felhasználóknak, majd ezeket az irányelveket a megfelelő szereplőkhöz lehessen hozzá rendelni. Ehhez a ZENworks Endpoint Security Management hozzákapcsolódik a vállalati címtárhoz (akár eDirectoryról, Active Directoryről vagy bármilyen más LDAP-kompatibilis személyazonosság-tárról van szó) és lehetőséget ad az irányelvek megfelelő célokhoz rendelésére, az egyedi felhasználók, a csoportok vagy szervezeti egységek, illetve a személyazonosság-konténerek bármilyen más szintjén. Az irányelvek akár gépekre is irányulhatnak a felhasználók helyett, így könnyebben megvalósítható a biztonsági felügyelet a megosztott gépeken.

2. Kiforrott jelentéskészítési és felülvizsgálati szolgáltatások. Fontos, hogy a biztonsági kikényszerítést ne lehessen „beállítani majd elfelejteni”. A kényszerítő intézkedéseket magas szinten méretezhető jelentéskészítési és felülvizsgálati mechanizmusokkal kell támogatni.

Megadható, hogy melyik jelentéseket szeretné látni, ekkor a ZENworks Security Client a Distribution Service eszközt használva létrehozza a megfelelő jelentési adatokat és visszaküldi ezeket a felügyeleti szerverre. Az adatokat ezután a felügyeleti szerver összegyűjti, elemzi, és összeállítja belőlük a kívánt jelentéseket.

3. Erős kliens-önvédelmi funkciók. Ha a vállalat komolyan gondolja az előírások betartását, akkor fontos, hogy a felhasználók ne tudják azt megkerülni vagy kikapcsolni a kényszerítést. Az ezzel kapcsolatos problémákat a ZENworks Security Client úgy előzi meg, hogy hatékonyan hárítja el a felhasználók támadásait, még akkor is, ha a kérdéses gépen adminisztrátori jogosultságokkal rendelkező felhasználókról van szó. A rendszer valós időben észleli a folyamatok leállítására, az illesztők eltávolítására vagy a rendszerleíró adatbázis megváltoztatására tett összes kísérletet, így védelmet nyújt az adminisztrátori műveletek ellen és naplózza azokat.

Kiforrott technológia

Az emberek méltán lesznek idegesek, ha az „új kernelszintű illesztőtechnológiáról” hallanak. Ez olyan, mint amikor az orvos azt mondja: „Ez a LEGELSŐ alkalom, hogy ezt a műtetet valakin elvégzik”. Az új technológia előnyeinek kihasználása egy dolog, kísérleti nyúltnak lenni egy másik. Ne felejtse el azonban, hogy a ZENworks Endpoint Security Management egy már beérett, a piac által kipróbált technológia, amely a Senforce Technologies felvásárlásával került a Novell portfóliójába. A termék négy éve van a piacon, és széles körben használják.

> Hely, hely, hely

Folytatjuk azt a gondolatmenetet, hogy nincs olyan alapértelmezett irányelv, amely a cég összes dolgozójának megfelelne. A biztonság maximalizálása és a termelési költségek csökkentése érdekében sokszor nincs más alternatíva, mint hogy számos különféle irányelvet kell létrehozni és ezeket különféle csoportokhoz kell rendelni.

Mivel mobil világban élünk, a helyzet még ennél is összetettebb. Még egy adott személy esetében sincs igazán olyan irányelv, amely mindig megfelelne. A ZENworks Endpoint Security Managementet a mobil munkaerő igényeinek megfelelően fejlesztették ki, emiatt a termék irányelvei (és irányelv-kikényszerítése) helytudatos módon épülnek fel. A rendszergazdák készíthetnek olyan irányelveket, amelyeknek a végponton egy adott hálózati helyen kell érvényre jutniuk. A hálózati paraméterekre (például IP-címekre, alapértelmezett átjárókra, DHCP-szerver címekre stb.) teljes rálátással rendelkező ügynökprogram azonosítja, hogy jelenleg melyik hely használható és alkalmazza az adott környezetre érvényes biztonsági irányelveket. Így a rendszergazdák egyszerűen készíthetnek olyan irányelveket, amelyek azt mondják, hogy „ha a felhasználóim a céges helyi hálózatot használják, akkor engedélyezem a hálózati forgalmat, de ha egy internetkávézóban ülnek, akkor ezeknek a portoknak az állapota inkább legyen 'stateful' (állapotfigyelő), ne 'open' (nyitott)”. A helytudatos működés teljes egészében automatikus, nem igényli a felhasználó beavatkozását.

> Összefoglalás

A világ megváltozott, és a régi típusú biztonsági intézkedések, mint például a peremtűzfalak és a peremhálózati vírusszűrés már nem elegendőek. Ma már a mobilkészülékek is közvetlenül ki kell kényszeríteni a biztonsági intézkedéseket. Miközben ezt a kikényszerítést elosztottan kell végezni, rendkívül fontos, hogy a biztonsági irányelvek felügyelete és meghatározása központilag történjen. A ZENworks Endpoint Security Managementet a mobil munkaerő igényeinek megfelelően fejlesztették ki. Használatával a biztonsági rendszergazdák a konzol előtt ülve kijelenthetik hogy a „céges irányelvek azok, amelyeket a felhasználóknak be KELL tartaniuk”, és hogy az irányelveket biztonságosan szétosztották az összes felhasználónak és valóban ki is kényszerítették ezek használatát. Nem számít, hogy a problémát a csomagok hálózaton keresztül történő áramlása jelenti, mert a vezeték nélküli használat biztonságossá tétele, a hordozható média-felügyelet vagy az érzékeny adatok titkosítása – melyeket a rendszergazdák mind-mind ellenőrzésük alatt tarthatnak – egyetlen egységes felügyeleti és jelentéskészítési keretrendszerből megoldhatók. 