

Eltűnnek a hálózati határok?

Az üzleti információkat meg kell védeni

Néhány év alatt a sávszélesség növekedésével, illetve a mobil informatikai eszközök elterjedésével a korábbihoz képest ugrásszerűen megnőtt annak a veszélye, hogy az üzleti információk illetéktelen kezekbe kerülnek akár a vállalaton belül, akár azon kívül. A technikai védelem mellett az üzleti oldal gondolkodásmódját is meg kell változtatni annak érdekében, hogy az információkat sikeresen meg tudják védeni a vállalatok – derül ki a Stratis vezető tanácsadójával, Glász Róberttel folytatott beszélgetésből. [írta: Mozsik Tibor]

Az elmúlt 10-15 évben teljesen megváltozott az informatikai hálózatok természete: a vállalatoknál elsőként bevezetett hálózatok az eltelt időszakban folyamatosan változtak. A hálózatok határainak módosulásával kapcsolatban három fő fázist lehet megkülönböztetni. A több mint tíz évvel ezelőtt általános, úgynevezett „Fortress” hálózatok még nagyon egyszerűek voltak: csak a szervezet saját dolgozói használhatták, azon át csak korlátozott szolgáltatásokat lehetett elérni, és nem kapcsolódott az internethez. A távoli hozzáférés csak dial-up modemeken keresztül kapcsolódott a hálózathoz, így a vírusok sem voltak gyakoriak, mivel az legfeljebb csak egy hajlékonylemezről kerülhetett rá a gépre, és azon át a hálózatra.

Öt-tíz évvel ezelőtt aztán a vállalatoknál is elterjedt lett az internetkapcsolat, amely a belső hálózatra is hatást gyakorolt: a hálózat egyre bonyolultabb lett, de azt többnyire még mindig csak a szervezet saját dolgozói használták. A vállalati hálózat már kapcsolódott az internethez (így e-mailezésre, korlátozott böngészésre is lehetőség nyílt), de a sávszélesség még mindig alacsony volt; ekkoriban jelentek meg az „első”, széles körben pusztító vírusok. A távoli hozzáférés ekkor már virtuális magánhálózaton keresztül vált lehetségessé.

Az utóbbi öt év – többek között a sávszélesség növekedése, illetve a hálózatra kapcsolódó egyre többféle eszköz okán – ismét drámai változásokat hozott: a hálózatok egyre komplexebbé válnak, a sávszélesség is egyre nagyobb, és a belső hálózat már többszörös internetkapcsolaton kommunikál a külvilággal.

A hálózaton nagyszámú „külső” dolgozó végez on-site munkát, illetve csatlakozik távolról internet alapú távoli hozzáféréssel. A vírusok száma és veszélyessége is folyamatosan növekszik, miközben a hálózatokat széles körben hozzáférhető, bonyolult módszerekkel támadják.

Hálózaton belül és kívül

Glász Róbert, a Stratis vezető tanácsadója kérdésünkre elmondta: a vállalati hálózatok az elmúlt évtizedben drámai módon megváltoztak, és ma már rengeteg olyan szolgáltatás van, amelyekről tíz évvel ezelőtt nem is lehetett hallani. A vállalati felhasználók nagy mennyiségben küldenek és fogadnak e-maileket az interneten keresztül, bön-gésznek munkaidőben is a világhálón, emellett hozzáférnek a vállalati hálózati szolgáltatásokhoz és erő-

forrásokhoz. A belső hálózat és erőforrások ma már számos, egymástól különböző, illetve eltérő kockázatot jelentő eszközről érhetők el, például vállalati laptopokról és PC-kről, otthoni számítógépekről, internetkávézók gépeiről, idegen PC-kről, PDA-król, mobiltelefonokról. A szervezetnek emellett – gyakran ugyancsak az interneten át – biztosítania kell a B2B, B2C szolgáltatások közötti kapcsolatot, a szállítók, illetve a vásárlók, fogyasztók rendszereivel is, akiknek elérhetővé kell tenni a webszolgáltatásokat és weboldalakat. A „külsős” vállalkozóknak hozzá kell férniük a vállalati hálózat szolgáltatásaihoz és erőforrásaihoz, mindemellett a saját hálózatukhoz is csatlakozniuk kell.

A hálózati határ ott fordul elő, ahol a belső hálózat csatlakozik a külső hálózathoz. Az „új” üzleti igények megjelenése következtében úgy tűnik, mintha a hálózati határok eltűnnének, és a határ egy idejeműlt, korszerűtlen hipotézissé vált volna – vélekednek egyes szakemberek. A valóság ennél összetettebb; a tisztánlátáshoz először is le kell szögezni, mit jelent a hálózatok

határa. A „hálózaton kívül” és „hálózaton belül” fogalmakat ugyanakkor úgy definiálhatjuk, hogy a belső hálózatot a szervezet kontrollálni tudja, míg a hálózaton kívül a szervezet nem tudja szavatolni a felügyeletet.

Az információt védeni kell

A legújabb hálózatok határai azonban nem statikusak: a határok elhelyezkedése folyamatosan változik,

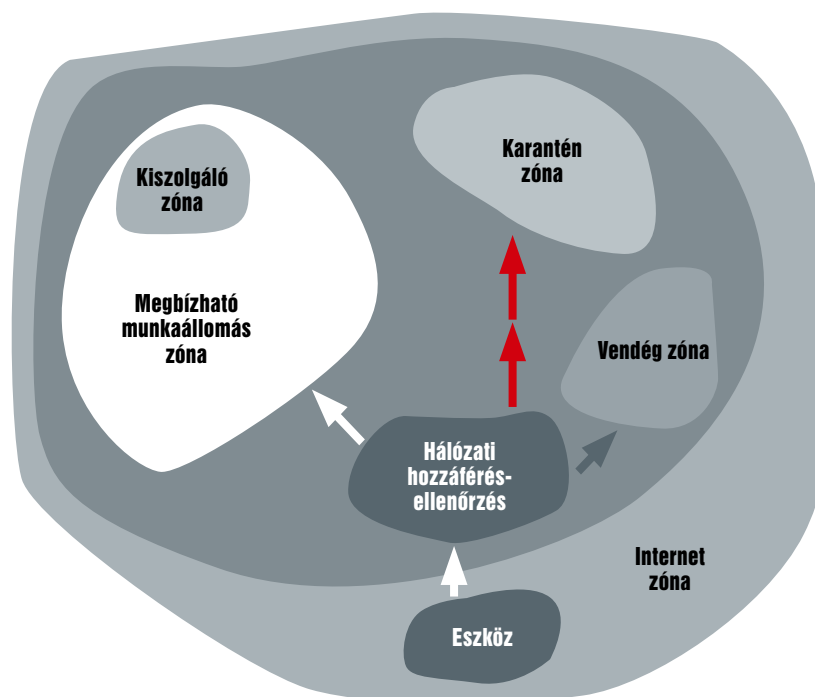
amint egy felhasználó vagy eszköz kapcsolódik a hálózathoz, vagy lekapcsolódik a hálózatról. A változásra két elméleti megközelítés született: a növekvő határ elmélet szerint, amint egy új eszköz csatlakozik a hálózathoz, azonnal megváltozik, növekszik az elméleti határ, és magában foglalja az eszközt; mikor egy felhasználó csatlakozik az otthoni PC-vel a vállalati hálózathoz, az is a hálózat részévé válik. E megközelítés szerint a hálózati határ magában foglalja a

szervezet összes eszközét, továbbá az összes külső eszközt, amely csatlakozott a vállalati hálózathoz. Ha ezt a megközelítést elfogadjuk, akkor a hálózati határok csaknem teljesen kikerülnek a szervezeti kontrollok alól. Az ellentábor véleménye szerint ugyanakkor a standardizálás révén a hálózati határok folyamatosan szűkülnek.

Glász Róbert hangsúlyozta: a hálózati határok változásával együtt a vállalatok biztonsági megközelítésének is módosulnia kell, a nyílt hálózatok terjedésével ugyanis folyamatosan csökken a biztonsági kontrollok és technológiák hatékonysága, a korábban alkalmazott hálózati biztonsági modellek egyre kevésbé alkalmazhatók, miközben a fenyegetettség kritikus mértékben növekszik a belső támadások, illetve a sérülékenységek kihasználása következtében. A szervezeteknek rövid távú célokat kell kitűzniük a menedzsment és a technológia területein, hogy kezelni tudják a hálózati határok lehetséges változásával, „megszűnésével” kialakuló nehézségeket. Sajnos a vállalatok többsége



Glász Róbert
vezető tanácsadó,
Stratis



ma inkább csak a technológiai megoldásra koncentrál, pedig az információbiztonság elsősorban nem informatikai, hanem üzleti kérdés – hangsúlyozta a Stratis tanácsadója. Pedig a technológiát „el kell felejtetni”, és az információt kell megvédeni. A határok ott vannak, ahol az információ van: éppen ezért azonosítani kell az információcsoportokat, és megfelelően kell védeni azokat.

Kockázatok tekintetében...

A menedzsment terület legfontosabb feladata az információ azonosítása – milyen adatok bírnak információval, illetve hol van az információ –, ezt követően pedig egy kockázatanalízist kell végezniük. A kockázatelemzés célja az alap kockázati kategóriák meghatározása és az információk-adatok ezekbe való besorolása. Az elemzés segít azonosítani az információt, és a vállalat ez alapján képes meghatározni a szükséges biztonsági szintet és kontrollokat az információk védelme érdekében. A kockázatelemzés alapján áttekinthetőbb, általánosabb és kezelhetőbb biztonsági szintek, kategóriák építhetők fel. Emellett fontos a munkatársak oktatása, hogy ennek révén növeljék a biztonsági tudatosságot. Ez ahhoz elengedhetetlen, hogy a felhasználók megértsék, milyen fontos a biztonság; így megfelelő, biztonságos módon végezhetik feladataikat, azonosítani tudják a gyanús eseteket, illetve felismerik az ellenőrizhetetlen, ismeretlen hálózatokhoz való csatlakozás veszélyeit.

Emellett azonban technológiai oldalról is kezelni kell a hálózati határvonalak eltűnésével járó kockázatokat, amihez a szervezet által meghatározott standard eszközök, operációs rendszerek használata adhatja a legnagyobb segítséget a szervezetnek. A standardizáció segíti a biztonsággal kapcsolatos konfigurációs követelmények betartását és menedzsmentjét (antivírus-beállítások, patchek, biztonsági konfiguráció stb.). Emellett szükség van még a hitelesített eszközök használatára, a hagyományos hálózati irányításra, valamint a távoli hozzáférési megoldások szigorítására, illetve korlátozására.

A biztonsági beállításokat ki is kell kényszeríteni, ehhez pedig elengedhetetlen a szervezet által üzemeltetett eszközök megfelelő biztonsági ellenőrzése, emellett a vállalati PC-ken és a laptopokon

egyenként korlátozni kell a fontos átlományokhoz való hozzáférési jogosultságot, valamint az adminisztrátori privilégiumokat. A hálózati biztonsághoz szükség van még a kötelező patchelésre és antivirus-frissítésre, a personal firewall használatára, a titkosítás használatára a tárolóeszközökön – laptop, PDA, USB-kulcs esetében is. Amennyiben az eszköz beállításai nem felelnek meg a szervezet által meghatározott követelményeknek, úgy automatikus és megkerülhetetlen biztonsági korrekcióra van szükség, amely a nem megbízható eszközök biztonsági karanténba helyezését jelenti.

A vállalati hálózatoknál egyre égetőbb probléma, hogy a munkatársak ellenőrizetlen, sokszor nem is titkosított vezeték nélküli (Wi-Fi) hálózatokat használnak.

Éppen ezért az adatszivárgás megakadályozása érdekében a vállalatoknak szigorítaniuk vagy korlátozniuk kell a vezeték nélküli hálózatok használatát, megfelelő titkosítást (WEP) kell használniuk, vagy korlátozniuk kell akár az erőforrások használatát is, ha a Wi-Fi-n keresztül kapcsolódnak a hálózathoz. A folyamatos biztonság érdekében a hálózatot monitorozni kell, és az idegen, nem jóváhagyott vezeték nélküli hálózatok azonnali tiltása is indokolt.

Lenni, vagy nem lenni?

A szervezeteknek hosszú távon át kell gondolniuk a teljes eddigi működésüket. A statisztikák szerint a szervezetek informatikai döntéshozói körében kétfajta álláspont és megközelítési mód alakult ki. Az egyik megközelítés azt mondja, hogy nincs hálózati határ, míg a másik megközelítés szerint viszont igenis létezik hálózati határ. E megközelítési módok alapján alakítják ki a határvédelmi rendszerek terveit és egyéb biztonsági politikákat, továbbá az elfogadott megközelítési mód alapján készülnek el a szükséges eljárásstervek.

Ha elfogadjuk, hogy nem tudjuk biztosítani egy szervezet hálózatának megfelelő kontrollját, akkor meg kell valósítani, hogy minden egyes eszközt és alkalmazást egyedileg védjünk és vonjunk ellenőrzés alá. Ahhoz, hogy ezt a szervezet

megvalósíthassa, a következő szempontokat kell fontolóra vennie: terveket kell létrehozni minden egyes eszköz védelme érdekében, hálózati kontrollokat kell implementálnia a kapcsolódó rendszerek között, és a teljes hálózati forgalmát titkosítania kell.

Az előbbieket mellett robusztusabb, szigorúbb hitelesítési és jogosultsági megközelítési módokat és eljárásokat kell alkalmaznia, az alkalmazások jelenlegi biztonsági funkcionálisánál magasabb és megbízhatóbb funkcionálisokat kell fejlesztenie, továbbá szigorú patchmenedzsmentet kell kialakítania. Ez a működés azonban a legtöbb vállalatnak nem járható út, mivel egyfelől a hálózat működtetésének költségei ilyen esetben az egekbe szöknek, másfelől nehéz garantálni, hogy minden veszélyesnek tartott eszközt a hálózaton kívül tudnak tartani.

A másik megközelítés alapján, ameddig létezik hálózat, addig mindig is lesznek hálózati határok. E megközelítési mód támogatói szerint, amint egy eszköz csatlakozik a hálózathoz, abban a pillanatban a szervezet hálózatának részévé válik, ezáltal a szervezet teljes, direkt kontrollt gyakorolhat fölötte. A megfelelő szinten monitorozható, vizsgálható, szabályozható. Ezáltal a szervezet ellenőrizni tudja a hálózatát kiterjesztő eszközöket, így minden esetben képes megtartani a saját hálózata feletti kontrollt. Ebben az esetben a szervezet hosszú távú terveket dolgozhat ki arra vonatkozóan, hogy milyen „bizalmas-

sági” kategóriákat, szinteket implementál a szervezet hálózatának biztonságához.

Hozzáférésszintek szerint

Az alábbi kiinduló információk alapján fel lehet állítani a bizalmassági mátrixot és eljárásokat, amelyekben azt kell megválaszolni, hogy milyen eszköz kerül kapcsolatba a hálózattal, ki az eszköz tulajdonosa – szervezet, vállalkozó, otthoni felhasználó –, a biztonsági konfigurálás kinek a felelőssége, és hogy az előbbi szempontok alapján az eszköz milyen bizalmassági szintre kerül (megbízható, részben megbízható vagy megbízhatatlan). A bizalmassági szint megállapítása attól függ, hogy a kapcsolódó eszközről milyen információkat állapít meg a rendszer. Amennyiben megállapítható, hogy hitelesített felhasználóról van szó, aki beazonosítható, az utolsó patchek is installálva vannak, a gépen fut a friss vírus-softver, személyi tűzfal és a szervezet által specifikált egyéb biztonsági szoftver telepítve van és működik, továbbá a meghatározott biztonsági konfigurációt érvényesíteni tudják, úgy a felhasználó beléphet a hálózatba, egyébként pedig karanténba kerül, vagy csak korlátozott jogosultságokat kap.

Persze minél mélyebbek a szükséges információk, annál pontosabb, és finomabb szabályozást lehet megoldani a hálózat védelmének kialakítása érdekében. A szervezetnek biztosítani kell a szükséges egyezőséget, hogy folyamatos kontrollt gyakorolhasson a hálózathoz permanensen vagy ideiglenesen kapcsolódó eszközök felett, ezáltal külön és hatékonyan tudja majd kezelni a különféle eszközöket, felhasználókat és kapcsolódó helyszíneket – tette hozzá Glász Róbert. ▀

Amint egy eszköz csatlakozik a hálózathoz, abban a pillanatban a szervezet hálózatának részévé válik, ezáltal a szervezet teljes, direkt kontrollt gyakorolhat fölötte...

PLUSZINFÓ
computerworld.hu/linkek

ISYS-ON Informatikai Tanácsadó Kft. keres

ERP SUPPORT MÉRNÖKÖT.

Feladat:

ERP-rendszerek telepítése, adminisztrációja, működés támogatása.

Elvárások:

- közép- és kisvállalat szintű hálózati ismeretek (tűzfal, biztonság, távoli elérés),
- Windows, Windows-Server, Linux, Unix operációs rendszerek adminisztrátori szintű ismerete (telepítés, támogatás),
- adminisztrátori szintű adatbázis-kezelői ismeretek (telepítés, támogatás, előny: a Progress ismerete, hasonló munkaköri tapasztalat),
- több éves üzemeltetői tapasztalat.

Amit kínálunk:

- piacképes jövedelem és rugalmas munkaidő,
- továbbképzési és továbblépési lehetőség,
- fiatalos csapatszellem,
- jó munkakörnyezet.

Ha hirdetésünk felkeltette érdeklődését, küldje el fényképes önéletrajzát az info@isys-on.hu e-mail címre.

isys on