DIPLOMAMUNKA

László Attila

Debrecen

2009

DEBRECENI EGYETEM INFORMATIKAI KAR

INFORMÁCIÓ TECHNOLÓGIA

Biztonságos informatikai rendszer kialakítása kis- és középvállalatok számára

Konzulens: Dr. Krausz Tamás
Egyetemi adjunktus

Készítette: László Attila
Programtervező matematikus

Debrecen
2009

1 TARTALOMJEGYZÉK

1 Tartalomjegyzék 2
2 Bevezetés 3
3 Fenyegetések 4
3.1 Általános veszélyek 4
3.1.1 Vírusok 4
3.1.2 Férgek 4
3.1.3 Trójai programok 4
3.1.4 Kémprogramok 5
3.1.5 Script kiddie támadások 5
3.1.6 Hordozható eszköz, mint támadási felület 5
3.2 Célzott támadások 6
3.2.1 Social Engineering 6
3.2.2 WiFi felület 7
3.2.3 IPsec 8
3.2.4 Weboldal felől érkező támadások 8
3.2.5 Autentikáció 9
4 Megvalósítás 10
4.1 Juniper SSG5 Threat Management Gateway 10
4.2 Windows Small Business Server 2008 12
4.2.1 Telepítés 13
4.2.2 SBS 2008 Console 13
4.2.3 Windows Server 2008 újdonságok 21
4.2.3.1 Internet Information Services 21
4.2.3.2 Terminálszolgáltatások 21
4.2.3.3 RODC 22
4.2.3.4 Tűzfal, hálózatba engedés 23
4.2.3.5 Hyper-V 24
4.2.4 Microsoft Exchange Server 26
4.2.4.1 Szerepkörök 26
4.2.4.2 Újdonságok a felhasználóknak 28
4.2.5 Microsoft Forefront Security for Exchange Server 29
4.2.6 Windows Server Updates Services 3.0 32
4.3 Levelezési beállítások 33
4.3.1 Mail relay, ETRN 33
4.3.2 Smarthost 34
4.4 Microsoft Windows Vista 34
4.4.1 Windows Automated Installiation Kit 34
4.4.2 WinPE 35
4.4.3 Windows Imaging, ImageX, SysPrep 35
4.4.4 Windows System Image Manager 36
4.4.5 Távtelepítés 37
4.5 Távoli munkavégzés 37
4.5.1 Remote Web Workspace 38
4.5.2 Outlook Web Access 38
4.5.3 RPC over HTTPS (Outlook Anywhere) 39
5 Összefoglalás 40
6 Köszönetnyilvánítás 41
7 Irodalomjegyzék 42

BEVEZETÉS

Napjainkban nagyon fontos a számítógépes rendszerünk, adataink biztonsága magánszemélyként is, de még inkább jelentkezik ez az üzleti szférában. Ott már nem a nyári kirándulásunk képei, vagy a magánleveleink kerülnek veszélybe (persze ezek sem elhanyagolhatóak), hanem akár üzleti titkok is. De még ha nincsenek is fontos adataink, másik tényező amit védenünk kell, az erőforrások. Senki sem szeretné, hogy számítógépét vírusok, férgek használják fel saját céljaik érdekében. Akár az is előfordulhat, hogy spam[1] küldésére használják gépünket és felkerül az IP címünk feketelistára (ekkor, míg el nem érjük, hogy levegyék onnan, leveleinket automatikusan kiszűrik a spamszűrők). Természetesen a számítógépes hálózatok, az internet térhódításával a biztonság szó új értelmezést nyert. Korábban elég volt fizikailag biztonságban tudni a számítógépeket. Mára ez már nagyon kevés. Sajnos sok kis- és középvállalat nem veszi ezeket elég komolyan. Részben a tudatlanság, részben pedig az anyagiak miatt. Személyes tapasztalatom van egy céggel, ahol a számítógépek vezeték nélküli hálózattal voltak összekötve. Az egyik winchester a könnyebbség kedvéért meg volt osztva. A router-en semmilyen titkosítás nem volt beállítva, tehát bárki, aki leült egy laptoppal az ablak alá hozzá tudott férni a céges adatokhoz. Az is előfordul, hogy egyszerűen sajnálnak költeni ilyesmire, nem ismerik fel a veszélyeket. Ezért is választottam ezt a témát, szeretném felhívni a figyelmet a jelentőségére. Először az általános és célzott támadásokat részletezem bővebben, azután az olyan lehetőségeket mutatom be, amivel egy biztonságos rendszer kiépítése megvalósítható, és alkalmas megoldás lehet azon vállalatok számára, akiknek értékesek adataik illetve erőforrásaik.

[1] Kéretlen, elektronikus reklámüzenet.

2 FENYEGETÉSEK

Ebben a részben felvázolom, hogy melyek lehetnek azok a támadások, amelyekre fel kell készülnie rendszerünknek. Beszélhetünk általános és célzott támadásokról.

2.1 Általános veszélyek

Először essen szó azokról a veszélyekről, amelyekkel valószínűleg már mindenki találkozott: a vírusok, férgek, trójai programok és a kémprogramok.

2.1.1 Vírusok

A vírusok számára szükséges egy gazdaprogram (egy futtatható állomány), amely segítségével aktivizálódik. Emberi beavatkozás nélkül nem képes terjedni. Lehetséges, hogy csak idegesítő hatásai vannak, pl. háttérkép átállítása, de akár komolyabb hardveres hibát is okozhat.

2.1.2 Férgek

A férgek is vírusok, de azok számára nincs szükség gazdaprogramra. Önmagukban is képesek terjedni, legtöbbször email-en keresztül. A legnagyobb veszélye, hogy duplikálni tudja magát a számítógépen belül, így nem egyetlen féreg, hanem akár száz, ezer is keletkezhet. Ha nincs kezelve a probléma, előbb vagy utóbb felemésztik az erőforrásokat (memória, hálózat sávszélessége). Egy rosszul megtervezett rendszer hibáit kihasználva, email-ben, akár a kliens levelezőprogramját igénybe véve tudják továbbküldeni magukat. Ez azért veszélyes, mert így a címzettek számára a feladó ismerős és ez legtöbbjüknek garanciát nyújthat a felől, hogy biztonságos tartalmú a levél. Egyes féregtámadásoknál, akár a számítógép vezérlését is átvehetik.

2.1.3 Trójai programok

A „trójai faló” programok legalább annyira trükkösek, mint a mitológiai történet, amiről a nevét kapta. A felhasználók számára úgy tűnik, hogy egy jó szándékú programot telepít, pedig igencsak kártékonyak tudnak lenni. Ellentétben a vírusokkal, férgekkel, a trójai

programok nem másolják magukat, de ezek is képesek backdoor-t[2], „hátsó ajtót” nyitni a rendszeren.

2.1.4 Kémprogramok

A kémprogramok személyes adatainkat gyűjtik, anélkül hogy beleegyezésünket adtuk volna. Általában internetezési szokásainkat vizsgálják, de a veszélyesebbek akár felhasználóneveinket, jelszavainkat is elmenthetik.

2.1.5 Script kiddie támadások

Ide sorolhatjuk a script kiddie-k (mások által fejlesztett programokat, scripteket használó rosszindulatú személyek) támadásait. Ezek végigpásztázva egy IP tartományt, az interneten fellelhető különböző sérülékenységet kihasználó scriptek segítségével próbálják feltörni a számítógépeket. Az esetek döntő többségében, olyan biztonsági réseket használnak ki, amelyeket már befoltoztak az operációs rendszer fejlesztői. Viszont probléma, hogy sok az olyan számítógép, amelyre nincsenek felrakva a legújabb frissítések.

2.1.6 Hordozható eszköz, mint támadási felület

Napjainkban már fontos tényezőnek számítanak a hordozható eszközök. Az innen érkező támadásokra is fel kell készülnie a rendszernek. Ebből a szempontból három kategóriába sorolhatjuk őket. Egyrészt az egyszerű adathordozók: pendrive-ok, USB-s winchesterek, memóriakártyák, melyeket csatlakoztatva a számítógéphez könnyedén megfertőzheti azt a már említett vírusokkal, férgekkel. Ezeket a biztonság érdekében tiltani kell. Következő csoport a céges laptopok, amiket természetesen nem csak munkahelyi környezetben használnak a felhasználók, így nem biztonságos hálózatra is csatlakoztathatják azokat. A laptopokon egy tűzfal rendszert kell konfigurálni úgy, hogy csak a munkahelyi hálózatot tartsa biztonságos hálózatnak. Minden egyéb hálózaton, a bejövő forgalmat blokkolja, a kimenőt pedig szűrje. Továbbá meg kell még említeni a SmartPhone-okat és a PDA-kat. Ezek esete azért különleges, mert az internet felé a telefonon keresztül is van átjárójuk, így

[2] A felhasználó számára nem látható elem, mely teljes kontrollt adhat a számítógép felett, egy vagy több személynek.

onnan is fertőződhetnek, egy szinkronizálás folyamán pedig máris terjedhetnek tovább a rosszindulatú szoftverek. Ezek elleni védekezés egyedül egy folyamatosan frissülő, jó vírusirtó lehet.

2.2 Célzott támadások

Míg az általános támadásoknál olyan eljárásokról van szó, amelyek például minden Windows XP operációs rendszerrel rendelkező számítógépet megtámadnak, addig célzott támadásnál másról beszélünk. Tegyük fel, hogy cégünktől meg szeretnének szerezni valamilyen gyártási technológiáját. Ekkor a hacker egyrészt használja azokat az eszközöket is, amelyeket az általános veszélyeknél említettünk, illetve olyanokat is, amelyek a mi rendszerünkre vannak kihegyezve.

2.2.1 Social Engineering

A legnagyobb kockázati tényezőt, nem az informatikai rendszer hiányossága jelenti, hanem maga az ember. Hiába teszünk meg minden óvintézkedést, ha az alkalmazottak nem tartanak be bizonyos alapszabályokat. Sokszor az emberi hiszékenységet, a bizalmat használják fel. Erről szól a social engineering. Telefonon, személyesen is megkereshetik a naiv felhasználót, akár még bizonyos személyes adataikkal is a birtokukban, így kizárva minden gyanakvást. Természetesen csökkenthetjük a veszélyt, ha bizonyos szabályzatokat hozunk, amelyet minden felhasználónak be kell tartania. Ezekben olyan szabályok lehetnek például, hogy munkaállomást nem hagyhatnak ott zárolás nélkül, a jelszavakat nem írhatják fel sehova (cédula a monitor szélén), megfelelő bonyolultságú jelszavak használata, amelyeket bizonyos időközönként kötelesek megváltoztatni, illetve hogy ezt soha, senkinek nem adhatják ki e-mailben, telefonon. Fontos, hogy ezek betartására kötelezzük az alkalmazottakat, és megfelelően szankcionálva legyen, ha figyelmen kívül hagyják. Sokan hajlamosak azt hinni, hogy a hálózat hardveres, szoftveres biztonsága önmagában elég, ezért tudatosítanunk kell, hogy nagyon nagy az egyes személyek felelőssége is.

Másik lehetősége a támadónak, ha valamilyen módon hozzáférést szerez a hálózathoz. Ez többféleképpen megtörténhet. Egy szabad végponton, egy nyitott vagy nem megfelelő erősségű jelszóval, illetve titkosítási technológiával védett WiFi hálózaton keresztül.

2.2.2 WiFi felület

A WiFi hálózatra sok helyen nem fordítanak elég figyelmet, pedig igen nagy kockázata lehet, ha hanyagul van beállítva. Kezdetekben a használt titkosítási protokoll a WEP[3] volt, de idővel sok hibájára fény derült, könnyen feltörhetővé vált, így kialakították a WPA-t (WiFi Protected Access). Ez már sokkal biztonságosabb volt, de csak egy átmeneti megoldásnak szánták, míg az IEEE 802.11i szabványt véglegesítették. Ezután adták ki a WPA2-t, ez jelenleg a legbiztonságosabb technológia, feltörési lehetősége nem ismert. 2006. március 13-tól kezdődően minden vezeték nélküli eszköz, kötelezően ezzel a szabvánnyal készül. Tehát ha vezeték nélküli hálózatot szeretnénk kiépíteni, akkor mindenképpen a WPA2 az ajánlatos titkosítás. Vállalati környezetben fontos még, hogy a WPA2-t ne Pre-Shared Key módban használjuk. Ez azt jelenti, hogy a hitelesítés, egy előre beállított jelszóval történik, amit becsatlakozáskor kell megadnunk. Helyette RADIUS alapú hitelesítő szervert használjunk. Segítségével megoldható a többszintű felhasználói jogosultság kezelés, azaz meghatározható hogy ki milyen erőforráshoz férhet hozzá. Ha mégis szükségünk van arra, hogy idegenek is becsatlakozhassanak a hálózathoz (például vendégek számára biztosított internetelérés), akkor ezt egy szeparált zónába tegyük úgy, hogy ne tudjon kommunikálni a hálózat többi részével egyik irányban sem és természetesen legyen levédve tűzfallal.

Esélyt adhat egy hanyagul védett switch is, illetve ha lehetőség van VPN[4] kapcsolódásra és a felhasználók a laptopoknál szeretik menteni a jelszavakat. Ekkor egy ellopott számítógép is veszélyt jelenthet. Természetesen ebben az esetben, minden account-ot valamilyen módon védeni kell, amelyről információt tárolhat. Ha sikerül csatlakoznia a betörőnek a hálózathoz, máris elkezdhet „hallgatózni”, azaz figyelni az adatforgalmat. Így

[3] Wired Equivalent Privacy – vezetékessel egyenértékű, biztonságos hálózat, elég optimista elnevezés.

[4] Virtual Private Network – virtuális magánhálózat. Az interneten keresztül alakítható ki vele biztonságos kapcsolat a vállalati hálózattal.

könnyedén szerezhet jelszó hash-eket. De ha például egy felhasználó megnyit egy Microsoft Word dokumentumot, és pont erre van szüksége a hackernek, akkor könnyedén meg is tudta szerezni a tartalmat jelszótörés nélkül. Megteheti azt is, hogy különböző túlterheléses támadásoknak teszi ki a szervert, amikre az internet felől fel van készítve, de a belső hálózat oldaláról nem feltétlenül.

2.2.3 IPsec

Érdemes tehát a hálózati forgalmat védeni. Erre a legalkalmasabb megoldás az IPsec kommunikáció, amely megakadályozza a „lehallgatást". Az IPsec egy protokoll készlet az Internet Protocol kommunikáció biztonságosabbá tételéhez. Működése során az adatfolyam minden egyes IP csomagját autentikálja és titkosítja. Tartalmaz eszközöket a kétirányú autentikációhoz is. Segítségével megvédhetjük az adatfolyamunkat hosztok közötti (pl. kliens-szerver, kliens-kliens), gateway-ek közötti (router-ek, tűzfalak), vagy akár egy gateway és hoszt közötti kommunikációk során. Az IPsec az OSI modell 3. rétegében van jelen, ezért nagyobb flexibilitást nyújt, mint például az SSL, SSH, amelyek felsőbb rétegekben működnek.

2.2.4 Weboldal felől érkező támadások

Ha elég jó a védelmünk, és nem tudnak közvetlen hozzáférést szerezni a hálózathoz, akkor is próbálkozhatnak az internet felől. A cégünknek természetesen van weboldala is, ami tipikusan egy nyitott felület ahol próbálkozhatnak, a kipublikált szolgáltatások biztonsági hibáit kihasználva. Alapvetően háromféle dolgot tehet a hacker. Ha tudomása van egy „zero-day exploit"-ról[5] akkor sajnos nem sok mindent tehetünk. Előfordulhat az is, hogy egy régebbi hibát használ ki, amihez már van is kiadott patch, csak nincs feltelepítve. Ekkor sem sok mindent tehetünk, de ezért nagyon fontos a frissítések azonnali telepítése. Ha egy olyan oldal van publikálva, amely saját fejlesztés, akkor maga a kód is tartalmazhat biztonsági réseket, amely kinyitja a rendszert az internet felé. Erre legjobb példa az SQL injection, amely az adatbázis réteg sebezhetőségén alapul. Legegyszerűbb esete az, amikor kihasználja, hogyha nincsenek megfelelően szűrve a nyitó/záró karakterek, vagy nincs

[5] Olyan biztonsági rés, amelyhez a gyártó még nem adott ki frissítést, adott esetben még az is elképzelhető, hogy a résről magáról sincs tudomása.

típusellenőrzés az adatbeviteli mezőkben. Ekkor egy felhasználónév bekéréskor akár egy tábla törlésének utasítását is megadhatja a támadó.

2.2.5 Autentikáció

Nagyon fontos hogy az autentikációs szintet megemeljük. Hogy is néz ki ez mélyszinten? A szerver megkéri a klienst, hogy küldjön neki egy jelszó hash-t. Nyilván a hash algoritmus meg fogja határozni az autentikáció erősségét. A legelemibb algoritmus, a Lan Manager (LM) hash. Ezt még az MS-DOS idején alakították ki. Nem tesz különbséget kis- és nagybetűk között, összesen 7 karaktert tud egyszerre hash-elni, az ennél hosszabb jelszavakat, ilyen hosszúságú darabokra bontja. Mivel elég korai technológia, könnyen visszafejthető, a mai modern számítógépek még a nehéz jelszavakat is képesek órákon belül feltörni. A Microsoft Windows NT 3.1-el jelent meg az NT LAN Manager v1 (NTLMv1) ez már case-sensitive (megkülönbözteti a kis- és nagybetűket) és nem tördeli a jelszavakat. A szótáras támadásokra gyenge jelszavak esetén még igen érzékeny. A Microsoft szerint 100 db 2Ghz-es számítógéppel, Brute Force[6] támadással 5 és fél év alatt törhető. Az NT LAN Manager v2-t (NTLMv2) a Microsoft Windows NT 4.0 SP4 után mutatták be. Ennek kulcstere már 128 bites, kölcsönös azonosítást végez és létrehoz egy biztonságos csatornát, melyen folyhat a kommunikáció. A legmodernebb Microsoft által használt hash algoritmus a Kerberos, amely a Microsoft Windows 2000-el jelent meg. Ennek működése már bonyolultabb. Ami fontos, hogy időbélyeget használ, így nem lehet 5 percnél nagyobb időeltérés a kliens és a szerver között. A LM-t és az NTLMv1-et érdemes kitiltani a rendszerből. Igaz, így egyes kliensek nem tudnak csatlakozni a hálózathoz, de a biztonság megköveteli és jó esetben olyan régi operációs rendszert már nem használunk. Természetesen lehet bármilyen erős az autentikáció, ha rövid, könnyű jelszót adunk meg, percek alatt törhetővé válik.

A biztonsági rések kihasználása ellen növelheti védelmünket egy jó proxy is, mert megakadályozhatja, hogy nem szabványos kérések érkezzenek a web szerver, ftp szerver felé.

[6] Működésének lényege, hogy a titkosító rendszer ismeretében az összes lehetséges kulcsot kipróbálva határozza meg az alkalmazott kulcsot.

3 MEGVALÓSÍTÁS

Ebben a részben rátérek a konkrét eszközökre, amelyek a megvalósításhoz szükségesek. Először is kell egy megfelelő tűzfal, erre a Juniper SSG5 Threat Management Gateway eszköz lesz alkalmas. A szerverre, a Microsoft Small Business Server 2008 termékét telepítjük. Feltételezzük, hogy az egész rendszer kiépítését ránk bízzák, így a kliens számítógépeket is, azokra Microsoft Windows Vista-t telepítünk.

3.1 Juniper SSG5 Threat Management Gateway

Juniper SSG 5

A Juniper Networks integrált biztonsági eszközei azzal a céllal készültek, hogy ellássák az alapvető hálózati biztonsági funkciókat. A teljesítmény optimalizálása és a bővítmények integrálása érdekében egy real-time operációs rendszer a lelke a tűzfalnak, ez a ScreenOs. Mivel ez az alapoktól kezdve céltudatosan lett kialakítva, ezért nem tartalmazza azokat a sérülékenységeket, hibákat, mint az általános célú operációs rendszerek.

A hálózati szintű támadások ellen dinamikus csomagszűrést használ, amely segítségével felfedi a rosszindulatú forgalmat. A módszerrel a tűzfal a csomagok fejlécében információkat gyűjt a különböző komponensekről, így a cél és forrás IP címről, port számokról, és a csomagok sorszámáról. Amikor válaszcsomag érkezik, a tűzfal összehasonlítja a fejlécében lévő információt és a hozzátartozó folyamat állapotát, ha nem egyeznek meg akkor a csomagot eldobja. Ez, az állapotot is tartalmazó vizsgálat, nagyobb biztonságot nyújt, mint például a nem dinamikus csomagszűrés, mert a kapcsolattal összefüggésben vizsgálódik, nem pedig csak csomagok egy kollekcióját látja. Alapbeállításban mindenirányú forgalom tiltva van, később a központi, házirend (policy)

alapú management felületen van lehetőség különböző policy-kat definiálni, amelyben beállíthatjuk, hogy melyik forrásból melyik célállomásba engedélyezett a forgalom.

Az SSG család nyújt egy beépített fájl-alapú vírusvédelmet, a Kaspersky Lab közreműködésével. Így tehát a tűzfal képességeit kombinálták egy víruskeresővel, amely tartalmaz adathalászat, kémprogramok, reklámprogramok elleni védelmet. Ezek az integrált eszközök keresnek mind az e-mail, mind a webes forgalomban úgy, hogy alaposan átvizsgálják az IMAP, SMTP, FTP, POP3, IM és a HTTP protokollokat is. Így a legnagyobb biztonságot tudja nyújtani már gateway szinten, a manapság gyorsan terjedő férgek, vírusok, trójaiak, kémprogramok és más rosszindulatú programok ellen, akár a tömörített fájlokat kicsomagolva is.

Lehetőségünk van kiszűrni a rosszindulatú weboldalakat is az eszköz segítségével. Kétféleképpen oldható meg: belső illetve külső szűréssel. Utóbbi esetén, átirányítja a forgalmat egy dedikált Websense Web Filtering szerverre, amely alkalmazza a Web használati házirendet. Az SSG 5 tartalmaz integrált szűrőt is, melynek segítségével kiépíthetjük saját házirendünket is. Természetesen már tartalmaz egy saját adatbázist is, amely frissességéről a Websense (a webtartalom-szűrés piacvezetője) gondoskodik. Ez több mint 20 millió URL-t tartalmaz, 54 kategóriába sorolva.

A Juniper Networks összefogott a Symantec-el (az anti-spam szolgáltatásokat nyújtó cégek piacvezetője), hogy csökkentse már gateway szinten a spam-ek rendszerbe érkezését, ezzel egy első szintű védelmet kiépítve. Mikor egy ismert kéretlen levél érkezik, ezt blokkolja, vagy megjelöli (beállításfüggő), így az mail szerver dolgát megkönnyíti.

A Juniper virtualizációs technológiáinak segítségével könnyedén szegmensekre bonthatjuk hálózatunkat, melyek mindegyikére külön tűzfalat, külön biztonsági házirendet alkalmazhatunk. Nézzük, milyen virtualizációs megoldásai vannak.

- Létrehozhatunk biztonsági zónákat (Security Zones). Virtuális részekre oszthatjuk vele hálózatunkat, amelyek külön logikai egységként működnek. Egy-egy részt akár fizikai interfészhez is rendelhetünk.
- Virtuális routereket (Virtual Router – VR) alakíthatunk ki az eszközön belül, így az úgy tud működni, mint több fizikailag létező router. Mindegyik VR kiszolgálhatja saját tartományát, biztosítva azt, hogy nem kavarodnak a route információk. Így akár több vevő igényét is kiszolgálhatja ugyanaz az SSG 5 eszköz.

- Virtuális hálózatok (Virtual LANs – VLAN) segítségével logikai alhálózatokat lehet kiépíteni, mely képessé tesz minket, hogy elkülönítsük a forgalmat alacsony szinten. Biztonsági házirendek segítségével leírhatjuk, hogy a forgalom az egyes VLAN-okból melyik biztonsági zónába, vagy fizikai interfészhez kerüljön, ezáltal könnyűvé téve annak eldöntését, hogy melyik erőforrásnak mihez van hozzáférése.

3.2 Windows Small Business Server 2008

A Windows Small Business Server 2008 (SBS 2008) egy ideális „all-in-one” megoldás kis- és középvállalatok számára. Magában foglalja azokat a Microsoft technológiákat, amelyekre egy ekkora méretű cégnek szüksége lehet. Nézzük pár szóban, milyen eszközöket foglal magában, amiket ebben a fejezetben később részletezek is.

- A **Windows Server 2008** a Microsoft szerverre írt operációs rendszereinek legfrissebb kiadása. Legtöbb verziója elérhető 32 és 64 bites formában is, de az SBS 2008 csak 64 bites architektúrájú gépre telepíthető,
- a **Microsoft Exchange Server 2007** miatt. Ez egy, a levelezést és csoportmunkát támogató Active Directory integrált, szerverszoftver. Főbb funkciói közé tartozik az e-mail, naptárak, feladatok, névjegyek kezelése, a mobil és web alapú hozzáférés támogatása és az összes adat központosított tárolása. Magyar nyelvű változata nincsen, kivéve a webes és Outlook-kliens alapú hozzáférést.
- Ehhez kapcsolódóan nyújt egy fokozott védelmet az e-mailen keresztüli támadásokhoz, a **Microsoft ForeFront Security for Exchange Server**-t (külön licenc nélkül csak 120 napos próbaverzió), ami egy vállalati szintű vírus és spam-szűrő technológia.
- A **Windows Live OneCare for Server** (szintén 120 napos próbaverzió) szolgáltatás megfelelő a vírusokkal, kémprogramokkal, a hackerekkel és más nem kívánatos behatolókkal szemben.
- Mint már említettem, nagyon fontos a naprakészség a frissítések tekintetében. Erre kínál megoldást a **Windows Server Updates Services 3.0** technológia, mely központi irányítás alá helyezi a telepítéseket.

- A **Windows SharePoint Services 3.0** segítségével lehetőségünk nyílik, akár utazás közben is belső dokumentumok megosztására, naptárak egyeztetésére, problémák megoldására.
- Említést érdemel a **Microsoft Office Live Small Business**, mely szolgáltatás integrációjával biztosítja a cég internetes jelenlétéhezés népszerűsítéséhez szükséges valamennyi eszközt.

Az eddigi eszközök megtalálhatóak mind a Standard, mind az Premium Edition kiadásokban. A Premium Edition-hoz jár egy plusz Windows Server 2008 és SQL Server 2008 licenc is. Így ha a vállalat számára adatbázis-elérés szükséges, könnyedén megoldható ez is. Sőt, mivel nem mindenhol használnak még SQL Server 2008-at, egy korábbi kiadás, az SQL Server 2005 is jár a kiadáshoz, hogy a legújabb verzióval nem kompatibilis alkalmazásokat is ki tudja szolgálni.

3.2.1 Telepítés

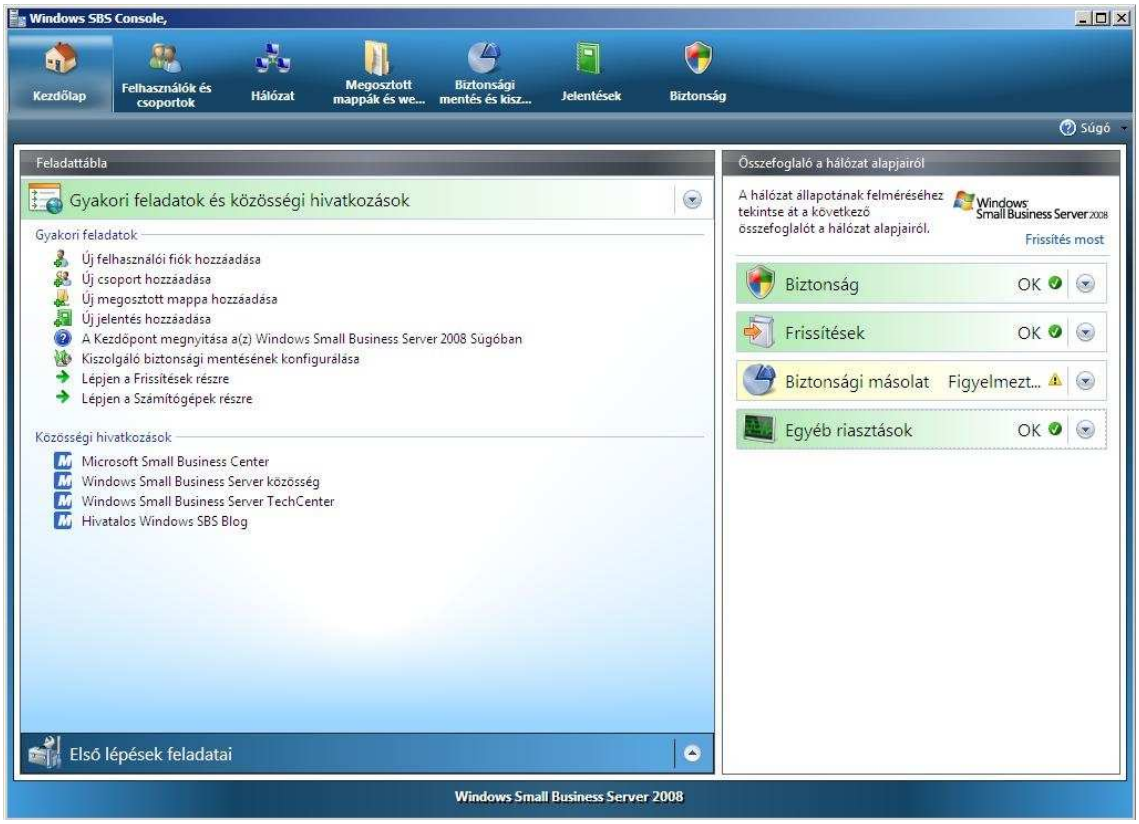
Az operációs rendszer telepítése nagyon egyszerűen történik. Mindössze pár adat kitöltését kell elvégeznünk, így a cégadatok (opcionális), kiszolgálónév és belső tartománynév, itt fontos megjegyezni, hogy ez a későbbiekben nem módosítható. Illetve egy hálózati rendszergazda fiókot kell létrehoznunk. Ezek után már használatba is vehetjük szerverünk új operációs rendszerét.

3.2.2 SBS 2008 Console

Az SBS konzol lesz az első, amivel találkozunk, mint a menedzselés legfontosabb eszköze. Ismerkedjünk is meg vele kicsit közelebbről. Általában ha egy operációs rendszer ennyi komponenst foglal magában, akkor komplex menedzsment felületet nyújt mindehhez. Ezzel szemben az SBS 2008 egy könnyen kiismerhető konzolt biztosít számunkra, amelyben releváns rendszerinformációkat tartalmaz, és a fontosabb beállításokat, különböző csoportokba osztva. Például egy felhasználó hozzáadása, pár adat megadásával és három kattintással meg is történik, az SBS 2008 elvégzi a további teendőket (email alias létrehozása, szerver erőforrásainak hozzáféréséről gondoskodik, felépíti a felhasználó gyökér könyvtárát stb.). Telepítés utáni első indításkor automatikusan

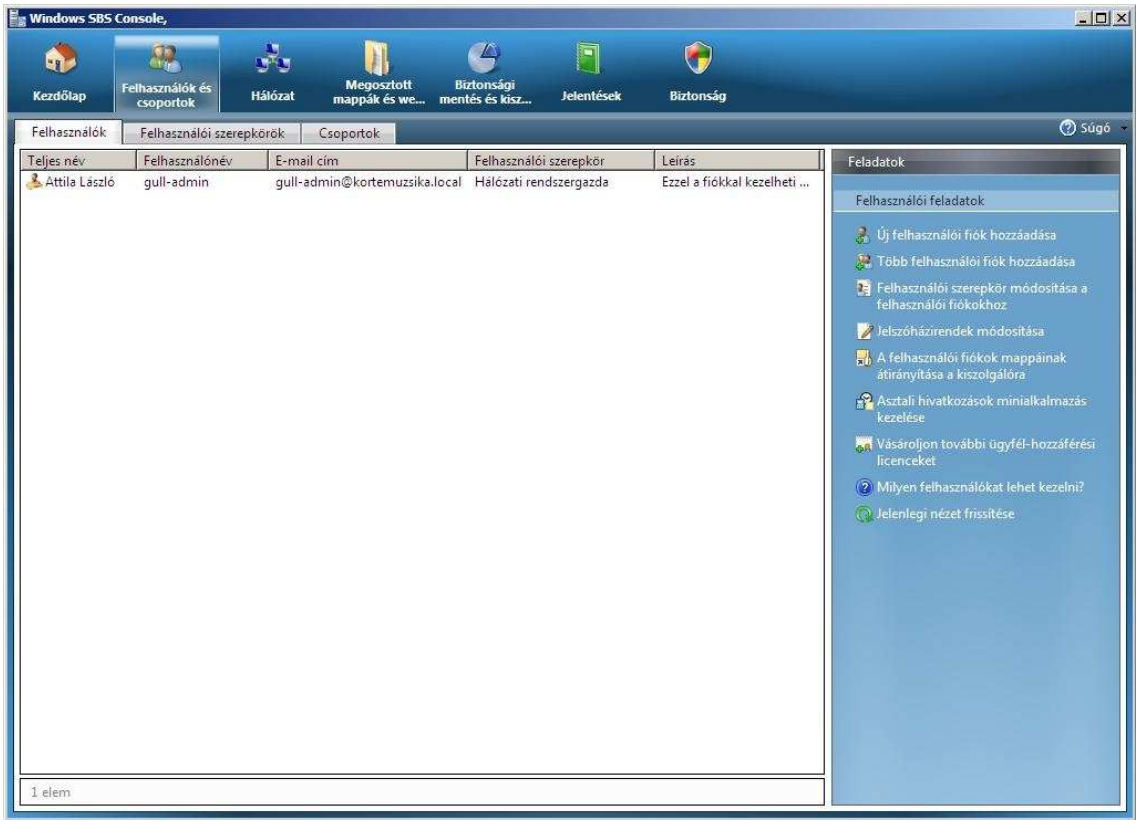
elindul, de Start menüből, vagy az asztalról magunk is elindíthatjuk. Hét fülre vannak csoportosítva a különböző eszközök, státusz információk:

Kezdőlap: a kezdeti lépéseket és a leggyakrabban használt eszközöket találhatjuk. A jobb oldalon egy összefoglalót találhatunk az alap hálózati állapotról, mely folyamatosan frissül.



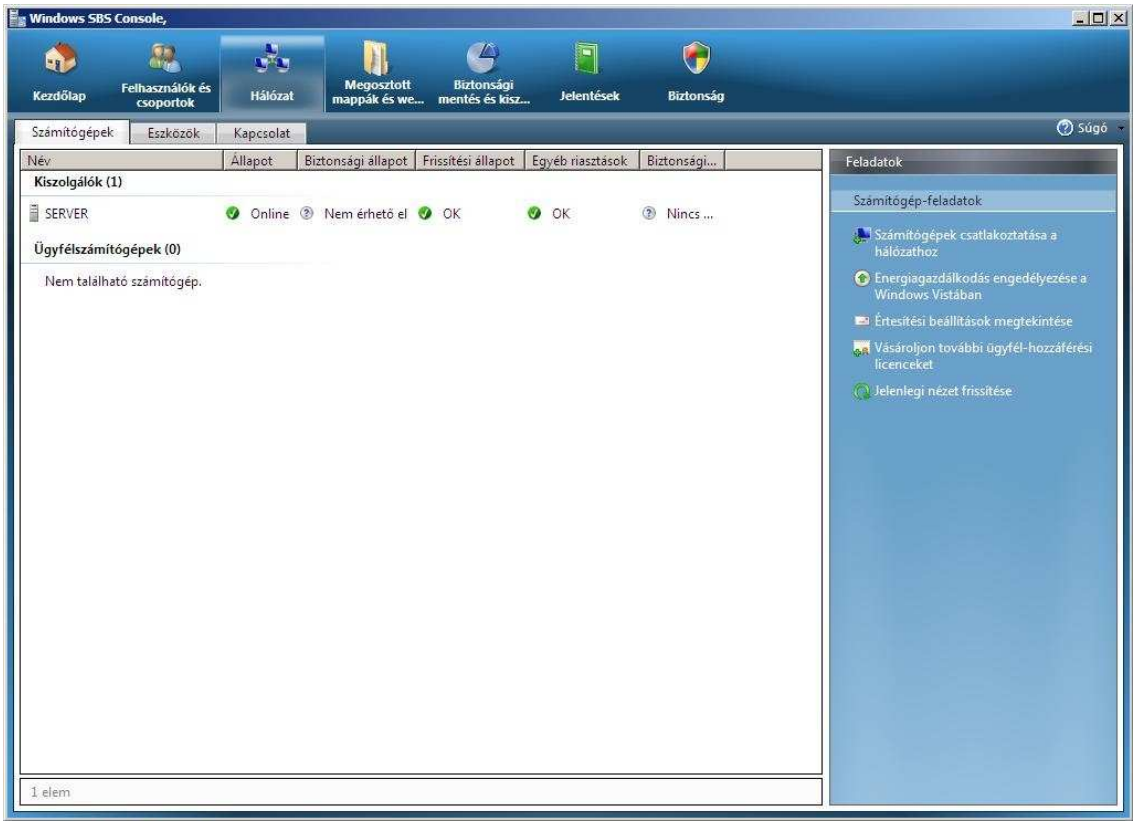
Windows SBS Console: Kezdőlap

Felhasználók és csoportok: itt tudjuk kezelni a felhasználókat, különböző szabályokat, csoportokat (külön-külön fül). Egy összefoglaló szolgáltatás, ami több eszköz adatait is felhasználja, mint például az Active Directory. Részletes beállításokhoz előfordulhat, hogy az adott eszköz kezelőfelületén kell dolgoznunk.



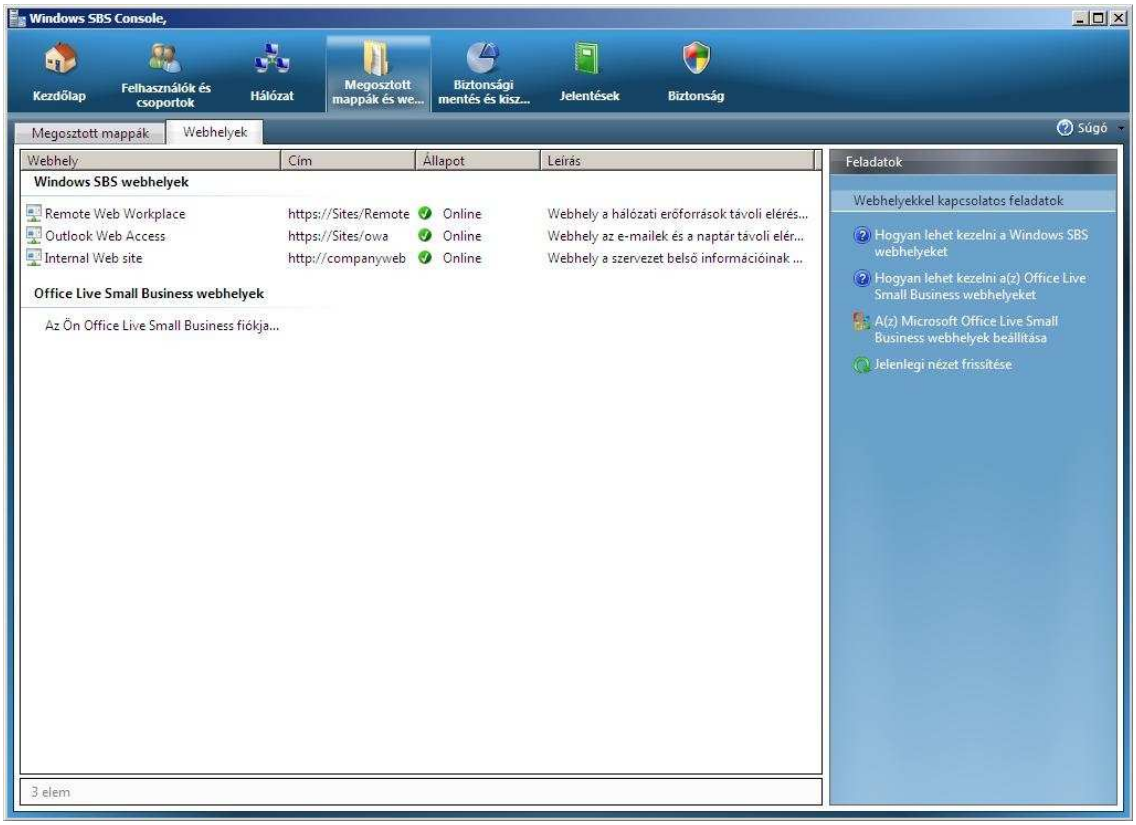
Winsows SBS Console: Felhasználók és csoportok

Hálózat: elsődleges hely ahonnan menedzselhetjük a hálózaton található fizikai eszközöket (számítógépek, faxok nyomtatók, mobil eszközök). Továbbá minden hálózati szolgáltatás beállításait is itt tudjuk végrehajtani.



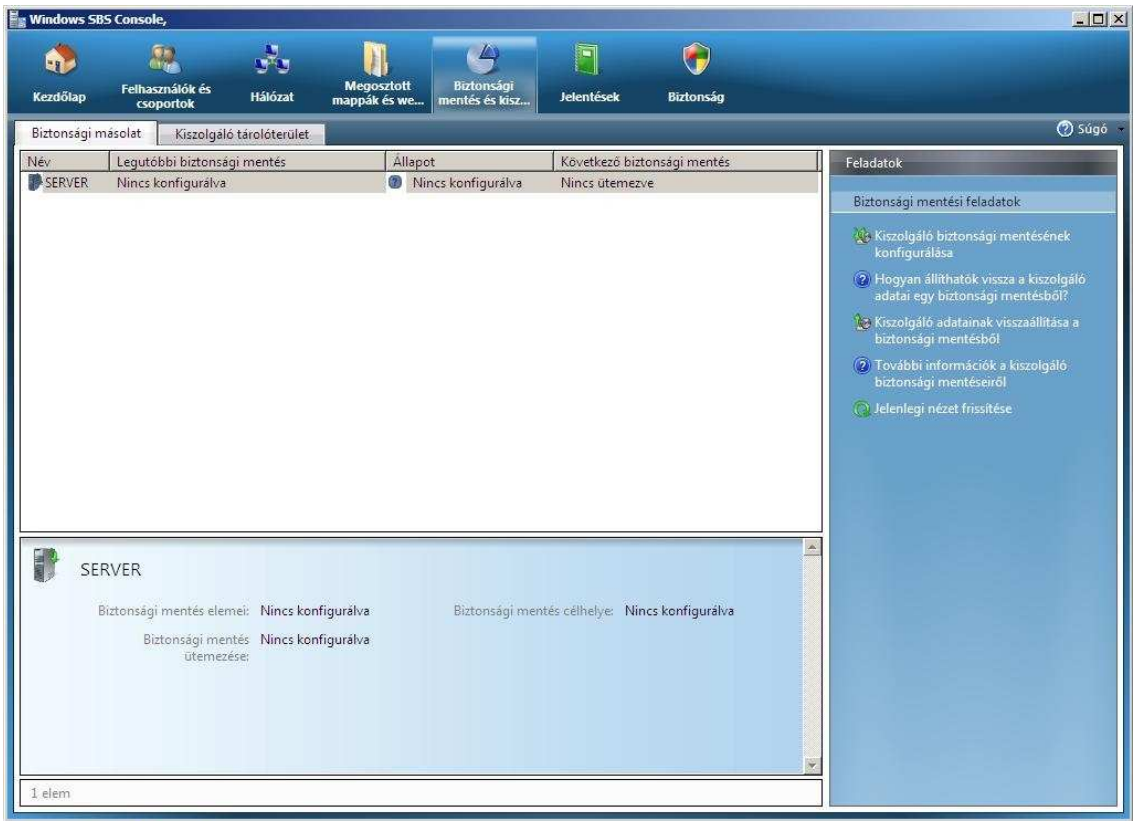
Windows SBS Console Hálózat

Megosztott mappák és webhelyek: egy modern felületet biztosít számunkra, a megosztott mappák és a webhelyek kezelésére. Nagyon egyszerűen hozhatunk létre új megosztást varázsló segítségével, egy kattintással kikapcsolhatjuk weboldalunk használatát stb.



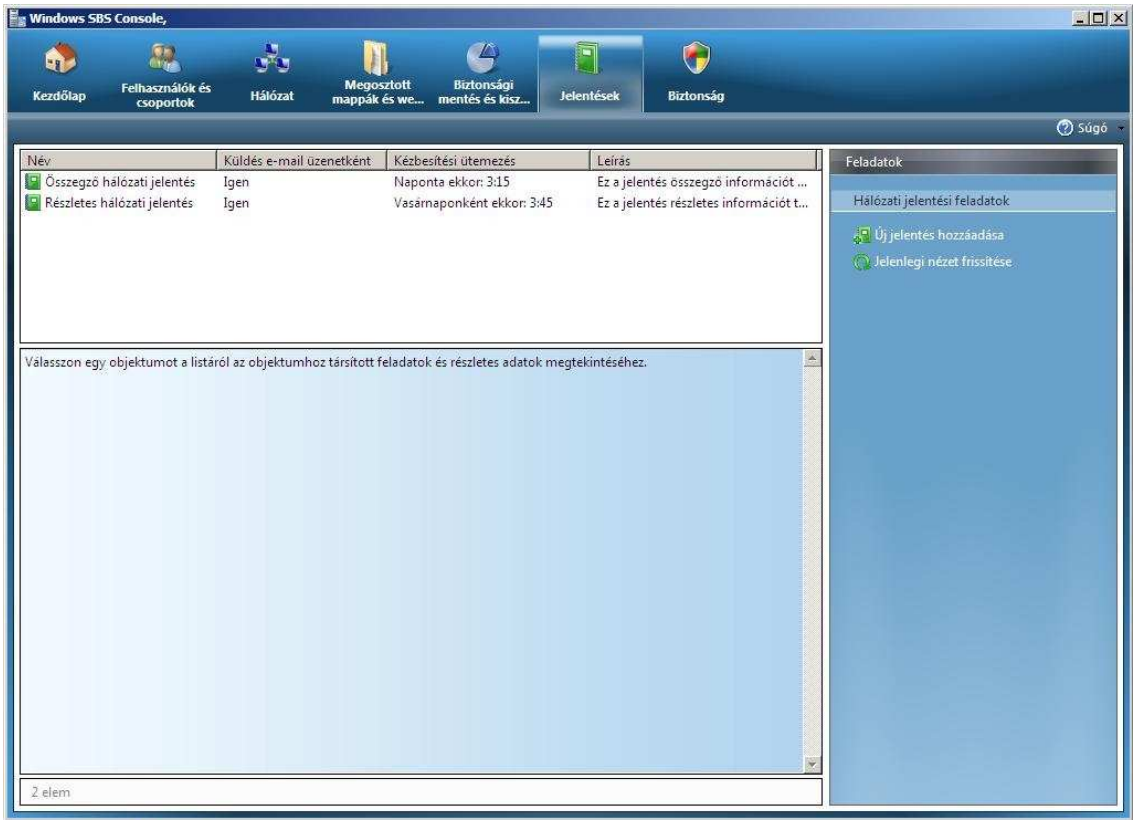
Windows SBS Console: Megosztott mappák és webhelyek

Biztonsági mentés és kiszolgáló tárterület: könnyen átlátható eszközkészlet, aminek segítségével létrehozhatunk biztonsági másolatot, illetve menedzselhetjük ezeket (pl. ütemezés beállítás). Fontos megemlíteni, hogy dedikált partíció kell a biztonsági másolat készítésére. Itt láthatjuk egy helyen, a szerverben rendelkezésre álló tárolók részletes adatait is, illetve mozgathatjuk az adatainkat, mint például az Exchange, a SharePoint, Microsoft Update-hez tartozó adatok.



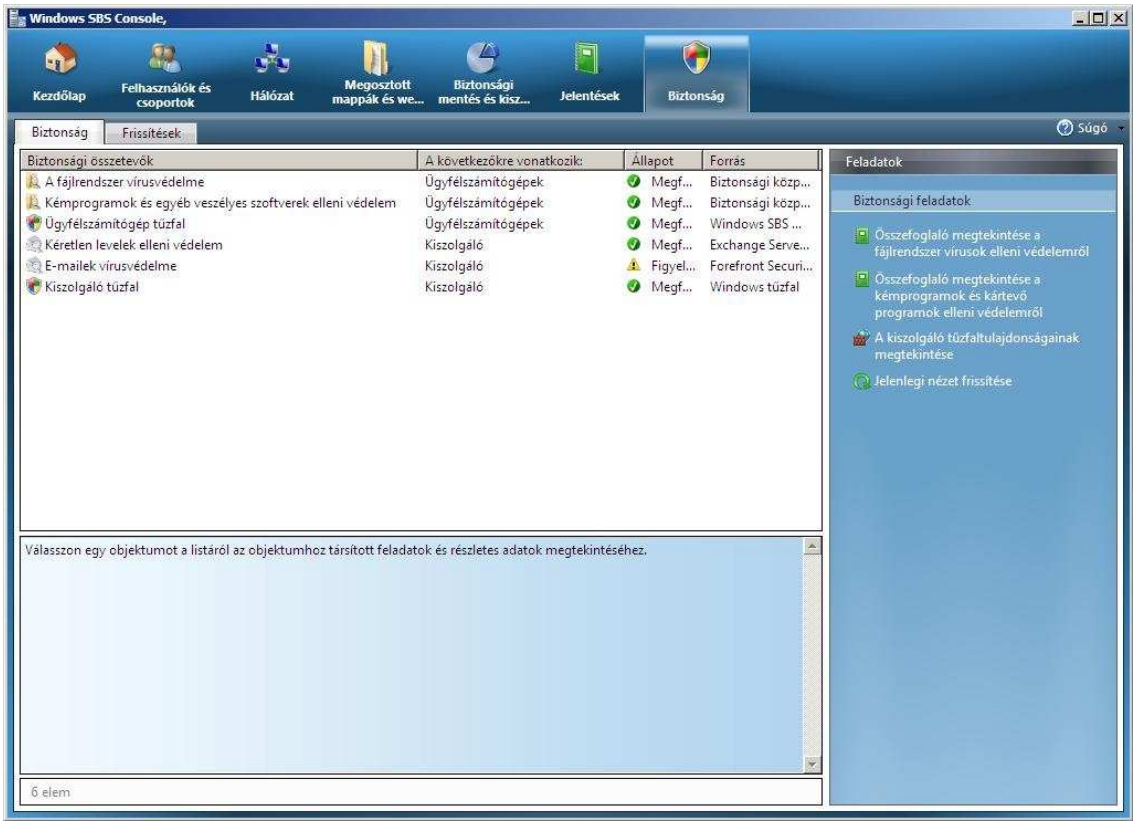
Windows SBS Console: Biztonsági mentés és kiszolgáló tárterület

Jelentések: összefoglaló jelentések készítésére képes, az SBS 2008 környezetről. Vannak előre elkészített összeállítások, de létrehozhatunk egyedieket is. Ezeket időzítve el tudja készíteni, és akár e-mailben továbbítani számunkra. Tartalmazhat a szerver eseménykezelő log-jából részeket, a biztonságról, frissítésekről, biztonsági mentésekről, e-mail használatról szóló és egyéb információkat.



Windows SBS Console: Jelentések

Biztonság: valós-idejű információt nyújt a hálózat biztonságosságáról, illetve a WSUS kezelésére ez az eszköz szolgál. Itt kaphatunk például információt arról, ha nem elég friss a vírusadatbázis, vagy valamelyik kliens gép tűzfala nincs bekapcsolva, vagy ha nem sikerült egy frissítés telepítése.



Windows SBS Console: Biztonság

3.2.3 Windows Server 2008 újdonságok

Mivel az SBS 2008 egy a Windows Server 2008 mag köré épített komponenscsomag, érdemes arról beszélni, hogy milyen újdonságokat vezetett be.

A Windows Server 2008-at és a Windows Vista-t egymás mellett, folyamatosan fejlesztették. Ezért nem meglepő, hogy kinézetünkben sok hasonlóságot találunk. Itt is, mint a Vistában a biztonságot helyezték mindenek elé (SDM = Secure Development Model). A két operációs rendszer kernele is ugyanaz, és mivel a Server 2008 a Vista SP1 megjelénes után jött ki, ezért az már kiadásakor tartalmazta a Service Pack 1 újdonságait, javításait.

3.2.3.1 Internet Information Services

A Microsoft webszervere, az Internet Information Services (IIS), nagy átalakulásokon esett át. Az IIS 7 teljesen flexibilis, kiterjeszthető, komponensekre bontható lett. Csak azokat az eszközöket kell telepíteni, amiket valóban használni is szeretnénk, így kevésbé sérülékennyé téve rendszerünket. A kezelő felülete is teljesen megújult. Lehetőségünk van arra is, hogy a már feltelepített szolgáltatások közül is csak azokat futtassuk, amikre éppen szükségünk van. Az IIS 7 lehetővé teszi a fejlesztők számára, hogy API-n át kommunikáljanak vele, így növelve a testreszabhatóságot. A konfiguráció teljes mértékben XML alapokon működik. A központi IIS beállítás történhet összetett fájlokkal is, így akár több weboldalt, alkalmazást is kiszolgálhat ugyanaz a webszerver. Az XML fájlok lehetővé teszik a hordozhatóságot is. Elég átmásolnunk a beállítást tartalmazó fájlt egyik szerverről a máikra és működik.

3.2.3.2 Terminálszolgáltatások

A terminálszolgáltatásokban is hozott újat a Windows Server 2008. A Microsoft operációs rendszerekben megtalálható Távoli asztali kapcsolat (Remote Desktop Connection - RDP) eszköz segítségével vehetjük igénybe a Terminal Server[7] szolgáltatásait. A szolgáltatás telepítése után a Server 2008 egy lokális és egy távoli felhasználó kapcsolódást engedélyez. De Terminal Server módban annyi felhasználó

[7] Több terminál kiszolgálására is alkalmas szerver.

kapcsolódhat, ahány licencünk van. A kliens oldalt érdemes megvizsgálni, hiszen a Vista hozta magával az RDP 6-os verzióját. Automatikusan felkerül a számítógépre a webes eléréshez szüksége ActiveX vezérlő is, így nem szükséges azt külön, a böngészőből telepítenünk (hasznos, ha a felhasználónak különben nem lenne joga az installáláshoz). Fontos újdonsága a hálózati szintű hitelesítés (Network Level Authentication – NLA). Ennek segítségével még azelőtt hitelesítjük magunkat, mielőtt az RDP kapcsolat kiépülne, így biztonságosabbá téve a kapcsolódást. A biztonságot növeli az SSL (Secure Socket Layer) továbbfejlesztése, a TLS (Transport Layer Security), mely biztosítja hogy valóban ahhoz a kiszolgálóhoz kapcsolódjunk amit választottunk, és ne pedig egy rosszindulatú harmadik fél által üzemeltetett szerverhez. A biztonságon kívül, a megjelenítésben is hozott újdonságokat, lehetővé téve a megosztott képernyő használatát, illetve a maximális felbontás is nőtt. Jelentős újítás még, az EasyPrint szolgáltatás. Ez megszünteti a kliens oldali nyomtató szerverre való telepítésének szükségességét, és driver nélküli módon teszi lehetővé a nyomtatást. A módszer egyszerű, lényege hogy XPS formátumban küldi a szerver a kliensnek a nyomtatandó dokumentumot, amit a helyi gépen futó operációs rendszer feldolgoz és elküldi a nyomtatónak. Meg kell még említeni a terminálszolgáltatásoknál felhasználók számára talán leghasznosabb fejlesztést is, a RemoteApp-ot. A távoli alkalmazások futtatásában nyújt segítséget. Olyan környezetben jeleníti meg a távolról indított alkalmazást, mintha a saját gépünkön történt volna, persze közben a szerveren fut.

3.2.3.3 RODC

Bevezette a Read-Only Domain Controller-t (RODC), azaz csak olvasható tartományvezérlőket. Ezt olyan külső telephelyekre szánták, ahol nem érhető el a központéval megegyező szintű fizikai biztonság. Az Active Directory-nak csak egy olvasható másolatát tartalmazza, bármilyen írási kísérletet egy teljes értékű tartományvezérlőre irányít át. Működéséhez szükséges, hogy egy Windows Server 2008 operációs rendszert futtató tartományvezérlővel szinkronizálja adatait.

3.2.3.4 Tűzfal, hálózatba engedés

Beszélnünk kell itt a fokozott biztonságú tűzfalról. Ez egy állapot-nyilvántartó tűzfal, amely megvizsgálja és szűri az IPv4-, és az IPv6-forgalom minden csomagját. A bejövő forgalmat alaphelyzetben blokkolja, kivéve ha az válasz az állomás által kezdeményezett kérésre, vagy pedig külön engedélyezett, azaz van rá tűzfalszabály. Amikor bejövő csomag ér a számítógéphez, a tűzfal megvizsgálja, hogy megfelel-e a tűzfalszabályban megadott feltételeknek. Ha igen, akkor végrehajtja az ott leírtakat, ha nem akkor elveti a csomagot, és ha engedélyezett akkor naplózza. Megadhatunk kapcsolatbiztonsági szabályokat is, melyek segítségével konfigurálhatjuk a munkaállomások közötti egyes kapcsolatok IPsec-beállításait. Ha olyan beállítást adtunk meg, amely a kapcsolat biztonságosságát igényli (bármelyik irányban), de a két számítógép nem képes egymás hitelesítésére, akkor blokkolva lesz a kapcsolat.

Egy sok gépből álló vállalat esetén probléma lehet a veszélyes számítógépek hálózatba engedésének megállapítása. Sok módszer van erre, akár a statikus DHCP[8] szolgáltatásra gondolunk, vagy MAC címek alapján szűrünk, házirendből vírusirtót telepítünk, tűzfalat beállítjuk. De mi történik akkor ha már hozzáférést biztosítottunk a hálózatunkhoz és közben vált veszélyessé a gép? Erre kínál megoldást a Network Access Protection (NAP). A gondolat nem új keletű, hiszen már az előző verziókban is létezett a Network Access Quarantine Control (NAQC), de ezt csak a távolról csatlakozó kliensek ellenőrzésére használták. Röviden fogalmazva a NAP feladata az, hogy csak a megbízható, „egészséges” számítógépek csatlakozhassanak a hálózatunkhoz. Így nevezhetjük a gépet, ha megfelel azoknak a feltételeknek, amelyeket a NAP házirendjében megadtunk. Tehát könnyen előfordulhat, hogy míg egy kliens az egyik hálózatban „egészséges”, addig egy másikban nem. Nem csak egy szolgáltatásról, de egy egész platformról beszélünk, amely szerver és kliens oldali komponensekből áll. A NAP-nek több feladata is van:

- a kliensek állapotának kiértékelése,
- a hálózati hozzáférés korlátozása,
- egészséges állapot elérésének segítése.

Több különböző módszer áll a rendelkezésére.

[8] Dynamic Host Configuration Protocol – ez a protokoll felelős azért, hogy a hálózathoz csatlakozó végpontok automatikusan megkapják a hálózat használatához szükséges beállításokat.

- Először is a DHCP. A folyamat a következő: a kliens próbál csatlakozni a DHCP szerverhez (jelen esetben az SBS 2008-unkhoz természetesen), hogy IP címet kérjen és csatlakozhasson a hálózathoz. A NAP megvizsgálja a gépet. Ha egészséges, akkor természetesen kioszt neki egy megfelelő IP-t. Ha nem, akkor csak egy korlátozott hálózati hozzáférést kap, amely arra elég, hogy az esetleges „gyógyító" szerverrel tudjon kommunikálni.
- VPN-el is közreműködhet. A VPN kliens megpróbál csatlakozni a VPN szerverhez (SBS 2008). Ellenőrzi a kliens állapotát. Ha az eredmény pozitív, akkor kapcsolódhat a hálózathoz, ha pedig nem akkor csomagszűrőket alkalmaz, melyek karanténba zárják.
- Lehet a hálózati hozzáférést portonként is szabályozni. A fizikai infrastruktúrát használjuk a szabályozásra. Amennyiben a switch-hez csatlakozó eszköznek engedélyezzük a forgalmat, úgy a port nyitott, egyébként pedig tiltott. Fontos, hogy a kliens Extensible Authentication Protocol (EAP) képes legyen. Ha a számítógép egészséges, akkor a NAP utasítja a switch-et a port nyitására, egyébként pedig arra hogy külön V-LAN-ba kerüljön.
- Az IPsec technológia is felhasználható szabályozásra. Ha a munkaállomás nincs megfelelő állapotban, akkor egyszerűen nem kap tanúsítványt, így nem tud kommunikálni a többi számítógéppel, azok elvetik az ettől érkező csomagokat.
- Lehetőség még, a TS Gateway szolgáltatás NAP-el való integrációja, de ez nem igazán jó módszer, nincs lehetőség a gyógyításra.

3.2.3.5 Hyper-V

A Windows Server 2008 egyik legfontosabb újdonsága a Windows Server Hyper-V. Ez a Server 2008 rendszer hypervisor[9]-alapú virtualizációs technológiája. Fokozott rugalmasságot nyújt, mert dinamikus, megbízható és méretezhető platformot nyújt egy beépített felügyeleti eszközkészlettel, mely egyaránt alkalmas fizikai és virtuális erőforrások kezelésére. A technológia segítségével több virtuális operációs rendszert is

[9] Platfom virtualizációs szoftver, mely segítségével több operációs rendszert futtathatunk egy számítógépen.

futtathatunk egyetlen kiszolgálón, természetesen az x64-alapú platform teljesítményének maximális kihasználásával. A Hyper-V négy alapvető területen hasznosítható jól, ezek:

- **Kiszolgálók összevonása:**

  Minden cégnek az a célja, hogy egyszerűbbé tegyék a felügyeleti munkát, mindezt a költségek csökkentésével, persze semmiképpen sem a megbízhatóság és a biztonság rovására. A Hyper-V segítségével kisebb a hardverigény, a terhelés jól eloszlható, mindemellett 32 és 64 bites munkafeladatok is beépíthetők ugyanabba a környezetbe.

- **Folyamatos üzem és katasztrófa-helyreállítás:**

  Cél, a tervezett és nem tervezett leállások, mint például biztonsági mentés, áramszünet, karbantartás minél rövidebb időre csökkentése. Sok eszközt biztosít ennek megkönnyítésére. Fontos a természeti katasztrófák, szándékos támadások, vagy akár konfigurációs fájlok hibája ellen védekezni.

- **Tesztelés és fejlesztés:**

  A fejlesztők sok különböző fejlesztői környezetet alakíthatnak ki egyetlen rendszeren belül, így még több mindenre fel tudják készíteni programjaikat. Ellenőrzőpontokat hozhatunk létre, az esetleges visszaállításokhoz. A Hyper-V sok vendég operációs rendszerrel használható, többek között linux disztribúciókkal is.

- **Dinamikus adatközpont:**

  A technológia segítségével dinamikus adatközpontokat alakíthatunk ki, amelyek önmagukat ellenőrző rendszereket jelentenek. Lehetőség van a virtuális gépek automatizált újrakonfigurálásra, az erőforrások rugalmas kezelésére, és a virtualizációt akár a változó igények előrejelzésére is használhatjuk.

Nézzük a platform fontosabb jellemzőit:

- Az új, továbbfejlesztett, 64 bites mikrokerneles architektúra révén a nagyobb teljesítmény mellett, fokozott biztonságot nyújt.
- Lehetőség van akár 4 processzort tartalmazó szimmetrikus multiprocesszoros (SMP) rendszerek támogatására a virtuális környezetben, így kihasználva a többszálas alkalmazások előnyeit.

- Közvetlen lemezhozzáférés („pass-through”) és tárolóhálózatok (SAN) felhasználásával nyújt nagyobb rugalmasságot a tárolási környezet kialakításához.
- Szabványos WMI[10]-illesztőfelületei és API-felületei segítségével gyorsan lehet egyéni megoldásokat készíteni hozzá.
- Új virtuális átkapcsolási lehetőségeket biztosít, így könnyen konfigurálhatók a virtuális gépek a Windows hálózati terheléselosztási (NLB) szolgáltatásának futtatására.
- Lehetővé teszi egy működő virtuális gép gyors, minimális leállási idő melletti áttelepítését egyik fizikai rendszerről a másikra, illetve pillanatképet is készíthetünk róla, így bármikor vissza tudunk térni működő állapothoz.

3.2.4 Microsoft Exchange Server

A legtöbb vállalat számára az e-mail a működés szempontjából elengedhetetlen kommunikációs forma, elengedhetetlen az eredményes munkavégzéshez. Lényeges az alkalmazottak számára, hogy hozzáférjenek az leveleikhez, naptárukhoz, csatolt dokumentumokhoz, névjegyalbumukhoz és még sok máshoz, függetlenül attól, hogy hol tartózkodnak, vagy hogy éppen milyen eszközt használnak.

3.2.4.1 Szerepkörök

A korábbi Exchange verziók esetében a feltelepített szerver egy egységet alkotva oldott meg minden feladatot. Nem volt lehetőségünk arra, hogy a különböző feladatokat szétbontsuk. Ez a felépítés változott meg gyökeresen az Exchange 2007-ben. Különböző szerepek jöttek létre a funkciók ellátására. Ezek:

- Client Access
- Hub Transport
- Mailbox

[10] Windows Management Instrumentation

- Edge Transport
- Unified Messaging.

Akár arra is lehetőségünk van, (bizonyos megkötésekkel) hogy különböző szerverekre telepítsük ezeket, így nagy rugalmasságot és skálázhatóságot biztosítva. Természetesen, mivel az SBS 2008 kis- és középvállalatoknak készült, ezért itt egyazon szerveren fut mindegyik. Nézzük sorba az egyes szerepköröket.

A **Client Access** teszi lehetővé a felhasználóknak a leveleikhez való hozzáférést. Ide tartozik az Outlook Web Access, az Outlook Anywhere (részletesebben később), az ActiveSync for Exchange és persze léteznek a POP3 és IMAP szolgáltatások is, de alapértelmezésben ki vannak kapcsolva. Az ActiveSync felelős a mobileszközök hálózaton történő szinkronizációjáért. Ide tartozik még két további funkció is, az egyik a találkozók szervezésében, a másik pedig az Outlook 2007-nek segít abban, hogy egy e-mail cím alapján be tudja állítani az egész profilt automatikusan.

A **Hub Transport** a korábbi Exchange-ekben megtalálható SMTP szolgáltatás szerepét vette át. Ez a szerepkör felelős a levelek továbbításáért a vállalaton belül és kívül. (Ha az Edge Transport nem veszi át a külvilág felé való küldést.) Feladata a konverzió a MAPI és az SMTP szerverek által használt MIME e-mail formátumok között. Az Outlook-ban megszokott szabályokhoz hasonlóan képes kategorizálni, megjelölni a leveleket, vagy jogi nyilatkozatot fűzni a végükre. Rendelkezik integrált spam-szűrővel és naplózási lehetőségekkel, amikkel az esetleg elvárt biztonsági szabályoknak megfelelhetünk. Előbbi általában ki van kapcsolva, mert az Edge Transport-ra van bízva.

A **Mailbox** végzi el a MAPI kliensek kiszolgálását, de Hub Transport nélkül, önmagában nem alkalmas levelezésre.

Egyik legnagyobb újítás, az **Edge Transport** szerepkör. Az elmúlt időkben eljutottunk oda, hogy az e-mailek mintegy 70 százaléka levélszemét (spam, vírus, adathalász támadás), ezért jó ötletnek tűnik, hogy ne az éles Exchange szerverre zúdítsuk ezt a levélmennyiséget. Az Edge Transport feladata tehát, hogy a DMZ-ben (plusz biztonsági réteg a LAN felett) elhelyezve lebonyolítsa a vállalat külvilággal folytatott kommunikációját. Ez lesz ami fogadja a bejövő leveleket, illetve SmartHost-ként (később részletesebben) is működhet. Beépített megoldásként megtalálható benne a korábbi Exchange verziókból már ismert IMF (Intelligent Message Filter), ami kiegészíthető a Microsoft ForeFront Security for Exchange eszközzel (következő fejezetben részletesebben). Tartalmaz egy szabályvarázslót is, mely segítségével módosítani tudjuk a

leveleket, vagy az útvonalukat. Ha kevésnek bizonyul a gyári varázsló, akkor programozottan kibővíthető a funkcionalitása Transport Agent-ek használatával. Feladata még a címátírás (Address Rewrite). Akkor lehet jelentősége, ha például két cég egybeolvad, és azt szeretnénk elérni hogy kifelé homogénnek tűnjön.

Az **Unified Messaging** szerepkör a hang- és fax-funkcionalitással kapcsolatos eszközöket valósítja meg. Nem rendelkezik semmiféle ISDN kártya, vagy modem meghajtóval. Tisztán VoIP (Voice over Internet Protocol) alapú a működése. Session Initiation Protocol-t (SIP) használ a hang és fax üzenetek fogadására. A rendszer felépítése szempontjából ez annyit tesz, hogy ha hagyományos IP interfésszel nem rendelkező telefonközponttal szeretnénk összekötni az Exchange-ünket, akkor mindenképpen szükségünk lesz egy VoIP gateway-re.

3.2.4.2 Újdonságok a felhasználóknak

A felhasználók részére is sok újdonsággal találkozhatunk. A naptárkezelési funkciókat (Scheduling Assistant) bővítették, így megkönnyítve a találkozók szervezését. Az Out Of Office szolgáltatás is kiterjedtebb lett. Ennek lényege, hogyha egy alkalmazott valamilyen okból nem dolgozik egy ideig, akkor e-mail érkezés esetén automatikus választ küld az Exchange. Különböző szöveg adható meg a vállalaton belüli és kívüli e-mailekre, továbbá beállítható előre az időintervallum, illetve beállítható hogy bizonyos partnereknek ne küldjön üzenetet, így például elkerülhetőek a levelezőlistákra feleslegesen küldött üzenetek.

Hasznos újdonság a WebReady funkció (részletesen az OWA szolgáltatásnál). A LinkAccess segítségével hozzáférhetünk olyan adatokhoz is, amelyek nem az Exchange adatbázisában találhatóak.

A csoportmunka megkönnyítésére is nagy hangsúlyt fordítottak. A foglaltsági adatok megjelenítéséhez külön webszolgáltatást rendeltek, amely közvetlenül a felhasználók postafiókjából veszi az információkat, így mindig naprakész. Sokkal finomabban állíthatjuk be a naptárban tárolt információkhoz való hozzáférést. Például beállíthatjuk, hogy aki nekünk találkozót szervez, az láthassa hogy mikor vagyunk elfoglaltak, viszont azt ne hogy mivel töltjük az időnket.

A mobileszközök támogatásában is sokat fejlődött az Exchange. Sok hasznos szolgáltatást használhatunk, többek között:

- keresés a szerveren tárolt postaládában a megfelelő elemek után,
- egyes üzenetek letöltése akár csatolmányokkal is, anélkül hogy teljes küldés/fogadást indítanánk,
- az Out of Office státusz beállítása, lekérdezése,
- találkozókat tudunk továbbküldeni további résztvevőknek.

Elérhető már a Service Pack 1 az Exchange 2007-hez, ebben további biztonsági lyukakat foltoztak be és kényelmi funkciókat vezettek be. Többek között volt sok beállítás, amit csak PowerShell-ben[11] lehetett megtenni, ezek száma csökkent a felhasználói kívánságoknak megfelelően.

3.2.5 Microsoft Forefront Security for Exchange Server

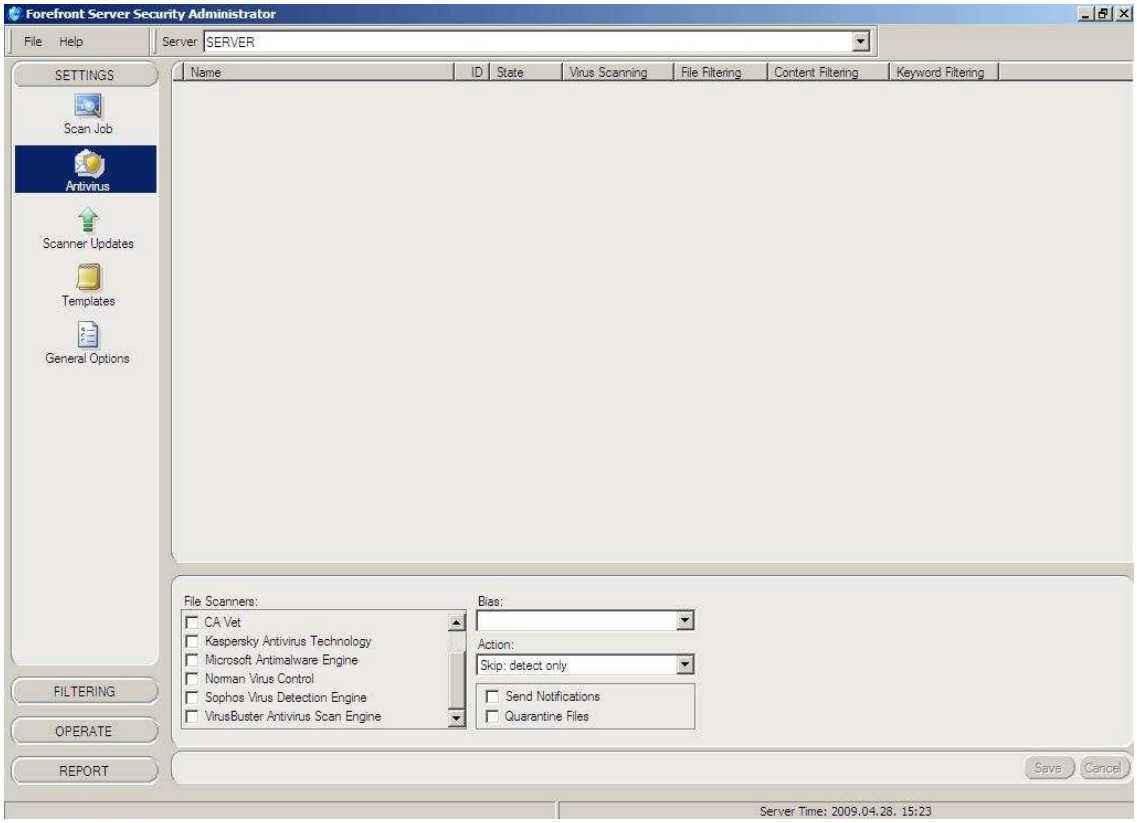
A Microsoft ForeFront Security for Exchange Server (FSE) több, az iparágban vezető biztonsági cég víruskereső motorját is integrálja, ezáltal megvédve üzenetkezelési környezetünket. A Service Pack 1-el frissített verziója támogatja a Windows Server 2008-at, és az Exchange Server 2007 SP1-et is.

Nézzük milyen lehetőségei vannak a FSE-nek:

- antivírus szolgáltatás, több víruskereső motort használva,
- kiterjesztett védelem minden a forgalomért és tárolásért felelős Exchange szerepkörben, beleértve az Edge, Hub, és Mailbox/Public Folders szervereket,
- fájlszűrés fájlnév, kiterjesztés vagy méret alapján,
- mindenre kiterjedő értesítések a rendszergazdáknak, illetve a levél küldőknek és címzetteknek.

Az antivírus kereskedéssel foglalkozó cégek mindig a lehető leghamarabb próbálják kiadni a vírusadatbázisok frissítését, de mindig van különbség abban, hogy milyen gyorsan tudnak reagálni. Az Forefront-ot használók élvezhetik a megosztottság előnyét. Ha minden üzenet több motorral van tesztelve, sokkal nagyobb a valószínűsége hogy valamelyik le tudja kezelni a frissen készített vírust.

[11] A Microsoft új generációs, parancssoros felügyeleti eszköze.



Látható a több víruskereső motor

Mint már említettem, a FSE több szerepkörön keresztül is vírusvédelmet biztosít, de eközben a szervereken történő többszörös, felesleges keresést elkerüli. Új felderítési logikát vezetett be, amely nem ellenőrzi azon e-maileket amelyeket már egyszer biztonságosnak nyilvánított. Alapértelmezés szerint először az Edge Transport-on vagy a Hub Transport-on ellenőriz, és a postafiókokba történő kézbesítéskor, vagy route-olás közben már nem teszi meg még egyszer. Így minimalizálja a többletmunkát, a levelező rendszer teljesítményének optimalizálása érdekében. Természetesen igény szerint konfigurálható ez a magatartás. Ahhoz, hogy felismerje a már ellenőrzött leveleket, első alkalommal a fejléchez egy biztonsági bélyeget ad hozzá. A következő szerepkör felismeri ezt a bélyeget. Amikor a levelek a tárolóba kerülnek, akkor ez a fejléc egy MAPI tulajdonsággá konvertálódik. Nézzük milyen keresési forgatókönyvek léteznek.

- **Beérkező levelek:**

  Az Edge szerver ellenőrzi az e-mailt, ezután további szerepkörök nem teszik. De miután a Mailbox szerver eltárolja, az beállítható, hogy új vírusadatbázis kiadása esetén újraellenőrzés történjen.

- **Kimenő levelek:**

  Alapértelmezés szerint a kimenő leveleket a Mailbox szerver nem ellenőrzi, viszont a Hub igen. Ha Edge szerver is telepítve van, akkor az sem vizsgálja már.
- **Belső levelezés:**

  Mivel itt csak belsőleg közlekednek az e-mail-ek, a Hub szerver felelős az ellenőrzésért. A Mailbox sem küldéskor, sem érkezéskor nem vizsgál.

Az antivírus bélyeg akkor kerülhet egy levél fejlécébe, ha teljesül a következő három feltétel:

- legalább egy víruskereső motor ellenőrizte,
- nem talált vírust, vagy ha igen, akkor törölve, irtva lett,
- ha a levél változtatva lett, a ForeFront sikeresen visszaírta az Exchange számára

A Mailbox szerepkörben alapértelmezésként nincsen vizsgálat, de a szolgáltatás meg van rá. Van valósidejű és háttér keresője, illetve kézi lehetőséget is biztosít. Ha mégis érkezik a szerepkörhöz antivírus bélyeget nem tartalmazó levél, akkor az On-Access-Scanning keres. Ez akkor lép működésbe, ha el akarjuk érni a levelet. Például előnézetnél, megnyitásnál, indexelésnél. Védelmet nyújt az Elküldött üzenetek mappára és a Megosztott mappákra is. Itt meg kell jegyezni, hogyha az Outlook 2007 levelezőkliensben be van kapcsolva a cache-elési lehetőség, akkor a levelek letöltése után, amikor csak a cache-ből nyitja meg, az On-Access-Scanning nem aktivizálódik. Ezért érdemes használni a Background Scanning-et is. Ez biztosítja a rendszergazdák számára, hogy beállíthassanak keresést, akár egy konkrét időpontra. Például az is megadható hogy csak az utóbbi két nap leveleit vizsgálja. A cache-elt leveleket is ellenőrzi, és ha talált egy vírusosat, akkor letörli és újraszinkronizálja a szerverről. Létezik még egy Proactive kereső is, mely akkor vizsgálódik, mikor a tárolóra új adat kerül. A Microsoft javasolja ennek használatát File szerverek esetében.

Az FSE licenchez jár egy prémium anti-spam szolgáltatás. A következőket kapjuk vele:

- **Microsoft IP Reputation Service**, amely azon IP címeket szolgáltatja, amelyek ismertek mint spam küldők. Természetesen folyamatosan frissül, akár naponta többször is.
- **Spam signature frissítések**, ezek segítségével felismeri az ismertebb spam mozgalmakat.

- Folyamatos frissítések az automatikus **tartalomszűrőkhöz**, mint a Microsoft Smartscreen, illetve egyéb Intelligent Message Filter (IMF) eszközökhöz.

A Forefront Security a következőket teszi egy e-mail vagy fájl vizsgálatakor:

- **Engedélyezett feladók vizsgálata:**

  Ha a funkció engedélyezett, az FSE összehasonlítja a feladó címét vagy tartományát a biztonságosnak ítélt felhasználók listájával, és ha rajta van, akkor a többi lépést kihagyja és kézbesíti a levelet.

- **Tartalomszűrés:**

  Két részből áll. Egyrészt szűri a feladót címének tartománya szerint, illetve az e-mail tárgyában lévő szavakat is hasonlítja a listájában lévőkkel.

- **Kulcsszó szűrés:**

  A levél tartalmában lévő szavakat hasonlítja össze a listájában lévő kulcsszavakkal.

- **Melléklet vizsgálat:**

  Ha az üzenet tartalmaz csatolmányt, akkor azt is ellenőrzi háromféleképpen. A Worm Purge az ismert férgeket keresi, és ha megegyezik a melléklettel, akkor törli. A File Filtering eszköz a fájlok neve, típusa és mérete szerint tud szűrni. Illetve természetesen a különböző víruskereső motorokkal is leellenőrzi a csatolt dokumentumot.

- **Szövegtörzs vizsgálat:**

  A levél szövegében keres férgeket, illetve egyéb rosszindulatú scripteket, linkeket.

3.2.6 Windows Server Updates Services 3.0

A Windows Server Updates Services 3.0 (WSUS), korábban Software Updates Services (SUS) néven volt ismert, majd Windows Update Services (WUS) ami még csak operációs rendszer hotfix-eket tartalmazott. A WSUS kibővített eszköz, már más szoftverekhez is nyújt frissítési felületet. A WSUS infrastruktúra segítségével automatikusan letölthetők frissítések, szervíz csomagok, eszközök illesztőprogramjai, mindezt úgy, hogy a kliens gépek a szerverről töltik le közvetlenül és nem pedig a Windows Update honlapról. Ezzel

sávszélességet, időt és lemezterületet spórolva. Előnye még, hogy a rendszergazdák tudják meghatározni mi és mikor települjön a számítógépekre.

3.3 Levelezési beállítások

3.3.1 Mail relay, ETRN

Mivel a SBS 2008 szerverünket valószínűleg egy irodában fogjuk működtetni, így a 100 százalék felé tartó, legalább 95-98 százalékos rendelkezésre állás nem biztosítható. Célszerű a leveleinket egy másik szerverre is érkeztetni. Ebben segít a mail relay szolgáltatás. Lényege, hogy a DNS (Domain Name System) bejegyzések közé felveszünk egy újabb MX (Mail eXchange) rekordot. Ezek felelőssége, hogy a domain-re érkezett e-mailek továbbítása egyértelmű legyen. Minden MX rekordhoz tartozik egy precedenciát jelző szám. (A kisebbel rendelkező az elsődleges szerver.) Mail relay esetében egy nagyobb súlyszámú rekordot veszünk fel, amely egy másik szolgáltató levelezőszerverére mutat. Természetesen ezzel a szolgáltatóval előzetes egyeztetésnek kell történnie. A folyamat a következő. Ha valaki levelet küld a cégünk által használt domain-re, akkor megnézi a szerverünk, hogy milyen MX rekordok vannak a DNS-ben. A nagyobb precedenciájú kiszolgálóval próbálja felvenni a kapcsolatot, amennyiben ez nem sikerül, akkor megy a következőre. Tehát, ha a saját szerverünk éppen nem elérhető (áramszünet, karbantartás…), akkor a másik szolgáltatóhoz érkeznek a levelek. Általában kétféle lehetőséget biztosítanak arra, hogy miképpen kapja meg Exchange-ünk a leállás miatt nem kézbesített e-maileket, ha már elérhető. Egyik módszer, ha folyamatosan küldi a kézbesítetlen e-maileket a másodlagos levelezőszerver, várva arra, hogy eléri az elsődlegest. Ez problémás lehet ha hosszú a leállás, mert a legtöbb kiszolgáló egy idő után feladja.

A másik megoldás az ETRN (Extended Turn). Ekkor a szolgáltató szervere úgy van beállítva, hogy tárolja a leveleket, és a mi Exchange-ünk majd küld egy ETRN üzenetet, amikor elérhetővé vált, és kéri azokat az e-maileket, amelyek a leállás alatt érkeztek.

3.3.2 Smarthost

A Smarthost is egyfajta Mail relay szolgáltatás, de ennek a levelek küldésénél van jelentősége. Egy hétköznapi kisvállalat internetszolgáltatója által kiosztott IP tartományokban szereplő címek (még ha fix IP is,) előfordulhat, hogy felkerülnek feketelistákra (olyan listák, melyekre spam-eket küldők címe kerül fel). Így könnyen megtörténhet, hogy az általunk küldött e-mailek a levélszemetek közé vándorolnak. Ennek elkerülésére használhatjuk a Smarthost szolgáltatást. A lényege, hogy mikor elküldünk egy e-mailt, egy közbenső (a megkért szolgáltató) levelezőszerverén keresztül jut el a címzetthez. Tehát kézbesítéskor nem csak azt látják, hogy egy esetlegesen feketelistán lévő címről, hanem közvetlenül egy megbízható internetszolgáltató levelezőszerverétől érkezett a levél. Ha valahogyan sikerül egy vírusnak bejutni, valamelyik a hálózatunkban lévő számítógépre, amely annyit tesz, hogy nagy mennyiségű spam-et küld szét, akkor könnyedén előfordulhat velünk is, az említett feketelistára tétel. A Smarthost ez ellen is védekezést nyújt.

3.4 Microsoft Windows Vista

Már rendelkezünk egy erős tűzfallal, illetve a szerverünkön egy SBS 200 operációs rendszerrel. Térjünk ki hát a kliens gépekre is. Feltételezzük, hogy új gépállományról van szó, nem pedig meglévő számítógépeket kell a hálózatba csatolni. Ilyen módon mi döntünk, milyen operációs rendszert telepítünk. Mivel a Microsoft legújabb 2007 elején kiadott operációs rendszere a Windows Vista, így arra esik a választás. Mivel a diplomamunkám témája, a rendszer kiépítése, így nem a Vista előnyeiről beszélnék az Windows XP-vel szemben, hanem inkább azokról az eszközökről, amik megkönnyítik a géppark telepítését.

3.4.1 Windows Automated Installiation Kit

Nyilvánvaló, hogy nem fogunk Vista telepítőlemezzel a kezünkben minden egyes klienshez odamenni és installálni az operációs rendszert, nem beszélve a különböző beállításokról. A Microsoft ebben is segítséget nyújt számunkra egy komplett

eszközcsomaggal, melynek neve Windows Automated Installation Kit (WAIK). Része többek között, a WinPE, ImageX és a System Image Manager.

3.4.2 WinPE

A WinPE (Windows Preinstallation Environment) a Windows rendszermagján alapul, de egy könnyített verzió, a hardverigénye nagyon alacsony, és ennek köszönhetően CD-ről, USB tárolóeszközről, hálózatról is indítható. A felhasználó felülete az igényeknek megfelelően, egyénileg alakítható. Eredetileg a különböző Microsoft operációs rendszerek telepítéséhez hozták létre az MS-DOS-os felület helyett, de ma már széles körben használatos más tevékenységekre is.

3.4.3 Windows Imaging, ImageX, SysPrep

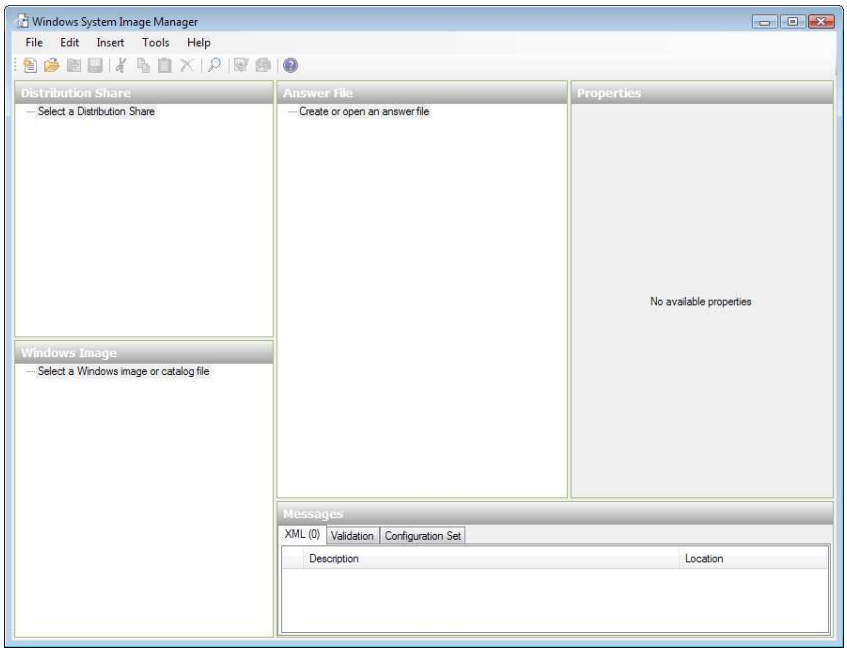
A telepítőkészletek kezelését jelentősen megkönnyíti az új Windows Imaging (WIM) fájlformátum, amely szemben a többi hasonló képkezelő eszközzel (pl. Norton Ghost), nem szektor-, hanem fájlalapú. A képfájl nem a fizikai lemez pontos mását tartalmazza, hanem mindössze a rendszer fájljait, könyvtárrendszerét. Egy ilyen fájlban (kb. 2,5 GB) elfér a hét különböző kiadású Vista telepítőkészlete is, köszönhetően a Single Instance technológiának, mellyel a többször előforduló, de fizikailag teljesen megegyező fájlokat csak egyszer tartalmazza. A képfájl tartalmát az ImageX program segítségével másolhatjuk fizikai könyvtárba. Fontos, hogyha hozzárendeljük (mount) a képfájlt a mappához, a dolgunk végeztével vegyük is ki onnan (unmount).

A Windows Vista teljes egészében komponensekre lett bontva, így szabadon tudunk elvenni, hozzáadni, módosítani különböző részegységeket. A WIM fájlban tárolt éppen ezért rendszerkép nyelv- és platformfüggetlen. Így ha a megfelelő drivereket integráljuk a képfájlba, különböző hardverkonfigurációkra is automatikusan telepíthető. Több lehetőségünk is van egyéni telepítőkészletet létrehozni. Használhatjuk a már említett ImageX és a Vistában már beépített Sysprep (System Preparation) alkalmazásokat. A Sysprep egy már működő rendszert képes előkészíteni képfájl készítésre. Amennyiben feltelepítettük egy gépre az operációs rendszert, a szükséges drivereket, megtettük az alapvető beállításokat, akkor a sysprep /generalize parancsot kiadva az eltávolítja az egyedi információkat a Windowsból, így lehetővé téve hogy újrahasználjuk. Ennek nagy a jelentősége, hiszen például a szerverünk Active Directory-ja a SID (Security Identifier)

alapján azonosítja a gépeket, és ez problémákhoz vezet ha minden gépen megegyezik. Használhatjuk a /oobe kapcsolót is, melynek hatására újraindítás után, a következő boot-oláskor a telepítés utáni kezdőképernyővel indítja a Windows-t, mintha egy frissen telepített példány lenne. De ekkor van lehetőségünk Windows PE-t indítani (például egy pendrive-ról), és ImageX segítségével lementeni a Sysprep által már előkészített rendszert egy képfájlba.

3.4.4 Windows System Image Manager

Nyújt más megoldást is a Microsoft. Az úgynevezett Windows System Image Manager használatával. A rendszer szinte összes paraméterét képes előre definiálni, és létrehozni a megfelelő válaszfájlt egy grafikus felhasználói felületet (GUI) nyújtva. A válaszfájl egy XML dokumentum, a telepítő installálás közben ebből olvassa ki a különböző beállításokat, így nincs szükség felhasználói interakcióra.



Windows System Image Manager panel

Első dolgunk, hogy bemásoljuk a Vista telepítőről az *install.wim* fájlt (a már említett ImageX segítségével), egy tetszőleges mappába, ezt betöltve tudjuk a különböző beállításainkat megtenni. Mivel, egy képfájlban több rendszer is lehet, annak a kiválasztását is itt tehetjük meg. Ezután hozzuk létre a válaszfájlt (Answer file). Ennek különböző kategóriái vannak, például „specialize”, „generalize”, melyek meghatározzák,

hogy a telepítés mely fázisában érvényesüljön az ott lévő beállítás. A „generalize” szekcióban szereplők általános beállításokat tartalmaznak, melyek platformfüggetlenné teszik az image-ünket. A „specialize”-ban, a különböző célcsoportokra szabott egyedi beállításokat állíthatjuk be, így a hálózati beállításokat, nyelvbeállításokat, a tartomány információkat. Itt adható meg például az Internet Explorer kezdőlapja is. A „specialize”-ban megadott ugyanazon szabályok felülírják a „generalize”-ban lévőket. Ezen a GUI-n is megadhatunk különböző drivereket arra az esetre, ha gyárilag nem támogatott hardverkonfigurációra telepítenénk. Ha végeztünk a komponensek testreszabásával, validálhatjuk az elkészített válaszfájlunkat. Az esetlegesen hozzáadott meghajtóprogramokat, egy külön kis parancssori programmal, a Package Manager-el kell integrálnunk a WIM image-be.

3.4.5 Távtelepítés

Távtelepítési szolgáltatással is szolgál számunkra a Microsoft. A Windows Server 2008-hoz kiadott Windows Deployment Service (WDS) lehet segítségünkre. A Remote Installation Service[12] (RIS) továbbfejlesztett verziója. A hálózaton keresztüli operációs rendszer telepítést oldja meg. Használata a következőképpen történik. Először is a szerverünkön (Windows Server 2008) installálnunk kell a szolgáltatást, hozzá kell adnunk egy szabályt. A Server Manager-ben ezt könnyen megtehetjük. Ezután a WDS-ben hozzá kell adnunk egy boot képfájlt (a Server 2008 telepítő cd-jén található Boot.wim), amiről a kliens gép először hálózaton keresztül boot-ol, illetve egy az előző módszerek valamelyikével elkészített képfájlt. A telepítendő gépen ezután be kell állítani, hogy hálózatról induljon, és ott máris látható a WDS-ben beállított képfájl, indulhat a telepítés.

3.5 Távoli munkavégzés

Természetes annak az igénynek a felmerülése, hogy ha az alkalmazottak nincsenek rácsatlakozva a biztonságos, belső hálózatunkra, akkor is ellenőrizni tudják leveleiket, illetve hasonló körülmények között dolgozhassanak. Az SBS 2008 szerverünk ehhez is támogatást nyújt.

[12] Az ügyfélgépek üzembehelyezését megkönnyítő beépített eszköz.

3.5.1 Remote Web Workspace

A Remote Web Workspace (RWW) egy dinamikusan frissített weboldal, ami egy egyedülálló, egyszerű, biztonságos belépési pont a vállalatunk hálózatába. A belépésre jogosult felhasználók csatlakoztathatnak a Remote Web Workspace-hez bármely számítógépről, amelyen van internet hozzáférés, és Internet Explorer böngésző. Sőt, akár Windows Mobile okostelefonnal is bejelentkezhetünk és szinkronizálhatjuk naptárunkat, kapcsolatainkat, megnézhetjük e-mailünket, böngészhetjük a belső vállalati weboldalt. A Remote Web Workspace-nek két kezelési felülete van, egy a rendszergazdák számára, és egy az alkalmazottak számára. Ez utóbbi interfész a következő lehetőségeket nyújtja:

- teljes hozzáférés az e-mailekhez, naptárakhoz az Outlook Web Access, belső webhelyhez, a SharePoint Services segítségével, illetve csatlakozás egy számítógéphez Remote Desktop Protocol-on (RDP) keresztül,
- egyszeri bejelentkezés segítségével, minden olyan alszolgáltatást elér a felhasználó, amihez joga van,
- és jelszó módosításra is lehetősége van.

Az adminisztrátori felület mindezeket szintén nyújtja, de pluszban még hozzáférést kap az SBS 2008 konzolhoz, illetve egy linket a Felügyeleti eszközökhöz. Alapbeállításként minden felhasználónak van joga használni a RWW-t, ezt az SBS konzol Megosztott mappák és webhelyek fülén tudjuk tiltani egy szabály létrehozásával. A RWW beállítása automatikusan megtörténik, amikor végrehatjuk a szerveren a Csatlakozás az internethez folyamatot.

3.5.2 Outlook Web Access

Az Outlook Web Access (OWA), egy web alapú levelezőszolgáltatás. A Microsoft Exchange Server 5.0-s változata óta létezik. Segítségével elérhetjük e-mailjeinket, naptárunkat, kontaktjainkat és más a fiókunkhoz tartozó szolgáltatásokat, amikor nem tudjuk elérni a Microsoft Outlook alkalmazásunkat közvetlenül. Az Exchange 2007-ben már a SharePoint által tárolt dokumentumokhoz is hozzáférünk, igaz csak olvasásra. Az

OWA számára mindösszesen internetkapcsolat és egy Internet Explorer böngésző szükséges. Lényeges különbség a Microsoft Outlook és az OWA között, hogy utóbbit csak állandó internetkapcsolat mellett tudjuk használni. Bejelentkezéskor két interfész közül választhatunk. Van a teljes kezelési felület, OWA Premium, ekkor minden szolgáltatását igénybe tudjuk venni. Viszont készítettek egy OWA Light felületet is, hogyha lassú kapcsolat mellett szeretnénk dolgozni, vagy nagyon szigorú biztonsági böngészőbeállításokkal működő számítógépről. A Light ügyfélprogram más böngészőkkel is elindul, míg a Premium működéséhez legalább Internet Explorer 7.0 szükséges. Az OWA felületén, a WebReady eszköz segítségével megnyithatunk csatolmányokat (PDF, Office dokumentumok), külön programcsomag telepítés nélkül. Működése során HTML lapként jeleníti meg a dokumentumokat.

3.5.3 RPC over HTTPS (Outlook Anywhere)

Az Outlook Anywhere, régi nevén RPC over HTTPS szolgáltatás segítségével használhatjuk a Microsoft Outlook programot a levelezésre akkor is, ha nem vagyunk a céges hálózatra csatlakoztatva. Ehhez mindössze annyi a teendő, hogy az Exchange 2007 szerverben és a levelezőkliensben engedélyezzük a szolgáltatást. Így a használatban mindössze annyi lesz a különbség, hogy ha nem a vállalati hálózatra van csatlakoztatva a kliens, akkor az Outlook, indításakor kéri azt a felhasználónevet és jelszót, amit a tartományba bejelentkezéskor is használ a felhasználó.

4 ÖSSZEFOGLALÁS

A diplomamunkám egyik fő célja az volt, hogy az olvasót rádöbbentsem, milyen nagy veszélyek fenyegetik a számítógépes rendszereket. Persze nem az a szándékom, hogy mindenki paranoiásan, túlzottan nagy biztonsági szabályokat vezessen be ezek után. Sajnos inkább a másik oldal jellemzőbb, akik nem foglalkoznak egyáltalán ezzel a kérdéssel. Leginkább nekik szól az irományom. A felvázolt lehetőségek segítségével remélem sikerült hozzájárulnom egy biztonságos struktúra megismeréséhez. Jól mutatja, hogy ugyan feltörhetetlen rendszer nem létezik, de nagyon sok mindent megtehetünk a rosszindulatú betolakodók ellen. Természetesen ez a pár oldal csak arra volt elég, hogy néhány szóban megemlítsem a Juniper és a Microsoft néhány eszközét, nincs lehetőség, hogy a teljes rendszert kidolgozva kulcsrakészen kidolgozzam. Az elveket viszont remélem sikerült érzékeltetni és alapjaiban bemutatni az alapvető szoftvereket, hardvereket, amikkel átvihetők a gyakorlatba.

5 KÖSZÖNETNYILVÁNÍTÁS

Ezúton szeretnék köszönetet mondani a szakmai segítségért és a számomra hozzáférhetővé tett dokumentumokért, témavezetőmnek Dr. Krausz Sándornak és bátyámnak László Csaba Ferencnek.

6 IRODALOMJEGYZÉK

O'REILLY: WINDOWS SERVER 2008: THE DEFINITIVE GUIDE

MICROSOFT FOREFRONT SECURITY FOR EXCHANGE SERVER USER GUIDE

HTTP://WWW.BS7799.HU/TOVABB.PHP?TOVABB=109

HTTP://EN.WIKIPEDIA.ORG/WIKI/IPSEC

HTTP://EN.WIKIPEDIA.ORG/WIKI/NTLM

HTTP://WWW.JUNIPER.NET/US/EN/PRODUCTS-SERVICES/SECURITY/SSG-SERIES/SSG5/

HTTP://TECHNET.MICROSOFT.COM/EN-US/LIBRARY/CC527593.ASPX

HTTP://WWW.MICROSOFT.COM/HUN/WS2008/HYPERV.MSPX

HTTP://EN.WIKIPEDIA.ORG/WIKI/WINDOWS_SERVER_UPDATE_SERVICES

HTTP://WINPORTAL.NET/?ID=659

HTTP://WWW.INFOTECHGUYZ.COM/SERVER2008/WDS.HTML

HTTP://TECHNET.MICROSOFT.COM/EN-US/LIBRARY/CC749082.ASPX

HTTP://TECHNET.MICROSOFT.COM/EN-US/LIBRARY/AA997437.ASPX