Tartalomszűrés, tartalom biztonság

A 2002-ben alapított Barracuda Networks, Inc. meghatározó tényező az **email és intenet biztonsági applikációk** piacán.
Több, mint **50,000 cég**, közöttük a Coca-Cola, FedEx, Harvard University, IBM, L'Oreal, NASA és a Europcar, védi hálózatát Barracuda Networks megoldásokkal. A Barracuda eszközök közös tulajdonsága a **könnyű installáció** és **üzemeltetés**, az **áttekinthető webfelület**, a központi automatikus frissítések, valamint a **meggyőző ár/teljesítmény** arány! A Barracuda eszközök licenszelése nem függ a felhasználók számától.

Veszély/jelenség	Javaslat	Igény az ügyfél oldalán	A gyártó megoldása
- elviselhetetelen a spamek aránya - túlterhelt a mail szerver - kliens oldalon védekeznek, de nagyon munkaigényes - állandóan tanítgatni kell a spamfiltert	- gateway oldali spamszűrés	- ne legyen pozitív hiba - ne érkezzenek spamek - ne kelljen folyamatosan felügyelni az eszközt - lehetőség a finomhangolásra - bármilyen szerverhez illeszteni lehessen	Barracuda Spam Firewall 
- a felhasználók nem a munkához kapcsolódó weblapokat nézegetnek munkaidőben - IM alkalmazásokat használnak - a vírusok átjutnak a tűzfalon, a szoftveres megoldás nem biztonságos	- gateway oldali webszűrés	- letiltani bizonyos alkalmazásokat (pl:skype, messenger) - a weblapok korlátozása kategóriákra és időpontra - a spyware letöltések leállítása és kommunikációjuk blokkolása - leállítani a vírus letöltéseket	Barracuda Web Filter 
- elvesznek a levelek és nem lehet őket visszaállítani - nehézkes bizonyos levelek megtalálása több évre visszamenőleg nézve - szándékos levéltörlések	- üzenetek archiválása	- nagy mennyiségű üzenet letárolása az eszközön - rendkívül gyors indexelés és visszakereshetőség - a régi levelek is feltölthetők az eszközre, a biztonságos eltárolás és keresés érdekében - a levelekben érkező csatolmányokat is tárolja	Barracuda Message Archiver 
- szerverek megbénítására szolgáló támadások - alkalmazás rétegben történő támadások - session állapotok elleni támadások - kifelé menő adatlopás - vírusok	- szerver forgalmát alkalmazásszinten is védeni kell	- az általa működtetett honlapok legyenek mindig elérhetőek - ne hamisítsák meg az adatok a weboldalakon - ne lopjanak adatot a webes alkalmazásokat futtató kívülről is elérhető szerverekről - SSL offload funkció - szerver load balancing funkció	Barracuda Web Application Firewall 

Tartalomszűrés, tartalom biztonság

A SafeNet a világon a 3. legnagyobb informatikai biztonsággal foglalkozó cég, amely integrált megoldásokat kínál az ügyfelei egyre növekvő biztonsági kihívásai számára. Tevékenységei között szerepel a **digitális jogok védeleme** (DRM), **az interaktív és proaktív tartalomszűrés** (eSafe), az **erős (több faktoros) azonosítás** (eToken) és a **titkosítás** (Protectdrive, Datasecure) A szervezet több, mint 25.000 ügyfelet szolgál ki a kormányzati és a vállalati szektorban több, mint 100 országban.

Veszély/jelenség	Javaslat	Igény az ügyfél oldalán	A gyártó megoldása
- spywarek, trójai programok, férgek, phishing támadások és zombik - a webhozzáférésekből adódó fenyegetések - különféle webes alkalmazásokból eredő károk pl. Skype, Messenger - adatszivárgás	- web- és spamszűrés	- segítse a biztonsági házirend betartatását - nagyvállalati megoldás - nagyfokú megbízhatóság (100%-ban blokkolja az ismert és 95%-ban az új, ismeretlen fenyegetéseket) - a felhasználót ne hátráltassa a munkában (transzparens) - széleskörű URL adatbázis/kategóriák - rugalmasan kiválasztható, skálázható - alkalmazások blokkolása - DLP	eSafe Smart Suite 

A WatchGuardot 1996-ban alapították és azóta több, mint 600.000 WatchGuard terméket telepítettek le világszerte. Mostanra több, mint 15.000 dedikált partnerrel rendelkeznek szerte a világban. A WatchGuard központja Seattleben, Washington államban található, ezen kívül vannak fiókirodák még Észak-Amerikában, Dél-Amerkiában, Európában és az ázsiai, csendes-óceáni régióban. A WatchGuard díjnyertes terméke az XTM (extensible threat management) hálózatbiztonsági tűzfala, amely megvéd a behatolásoktól, spamektől, vírusoktól és malwarektől, emellett még VPN csatornák végződtetésére is alkalmasak.

- számtalan kéretlen email - a levelező szerver leterheltsége - adatszivárogtatás - felnőtt és egyéb nem munkához kötődő webes tartalmak	- emailek többrétegű átvizsgálása és web szűrés	- email szűrő megoldás - kis-, és középvállalkozások igényeihez fejlesztették - webes forgalom szűrése - clusterezhető - email titkosítás	WatchGuard XCS 170, 370,570 
- számtalan kéretlen email - a levelező szerver leterheltsége - adatszivárogtatás - felnőtt és egyéb nem munkához kötődő webes tartalmak	- emailek többrétegű átvizsgálása és web szűrés	- email szűrő megoldás - nagyvállalatok számára - webes forgalom szűrés - clusterezhető - email titkosítás	WatchGuard XCS 770,970,1170 

Erős (több faktoros) azonosítás

Veszély/jelenség	Javaslat	Igény az ügyfél oldalán	A gyártó megoldása
- nem biztonságos VPN használat - védelem nélküli laptopok/desktopok - könnyen hozzáférhető jelszavak - könnyen hozzáférhető tanúsítványok	SafeNet eToken (korábban Aladdin eTokenként ismert) termékcsalád a jelszavak kiváltására	- sok jelszó használata webes alkalmazásokhoz, vállalati hálózati erőforrásokhoz és windows alkalmazásokhoz - erős jelszavak használatának szükségessége - központi menedzselhetőség - egyszerű bejelentkezés (Simple Sign-On) - egyszerű integráció	SafeNet
- gyenge jelszavak használata	eToken PRO	- a leggyakrabban használt USB kulcs megoldás, amely segítségével a kétfaktoros azonosítás megvalósítható - tanusítvány tárolás - elektronikus aláírás	
- gyenge jelszavak használata	eToken NG-OTP	- az eszközön manuálisan generálhatunk egy számsort, ez által csak egyszer használjuk a belépési jelszót - tanusítvány tárolás - One-Time Password - elektronikus aláírás	
- gyenge jelszavak használata	eToken NG-FLASH	- az eszközben található egy flash tárhely, amely tulajdonképpen úgy funkcionál mint egy pendrive - tanusítvány tárolás	
- gyenge jelszavak használata	eToken PASS	- nem tanúsítványos megoldás, egyszeri jelszót tudunk vele generálni - RSA tokenek kiváltására - olcsóbb maintenance - egyszerűen bevezethető One-Time Password techn.	
- gyenge jelszavak használata	smart kártyák	- tanusívány tárolás - elektronikus aláírás - fénykép a kártyalapra, ezáltal lehetőség van arcképes azonosításra is	

	Az Omnikey® smart kártya olvasók nagy megbízhatósága régóta közismert, így vált a legnépszerűbb kártyaolvasóvá hazánkban is. Minőségi kidolgozásuk, rendkívül alacsony meghibásodási rátájuk és megbízható, probkémamentes driverei emelték az integrátorok kedvenc kártyaolvasójává. A 2008-ban végbement ASSA ABLOY ITG és HID Global összeolvadás óta a HID termékpalettáján szerepel.			
- nem biztonságos VPN használat - védelem nélküli laptopok/desktopok - könnyen hozzáférhető jelszavak - könnyen hozzáférhető tanúsítványok	USB token helyett megszemélyesíthető, nyomtatható, bankkártya méretű smart kártya	Omnikey 3111 Omnikey 3121 Omnikey 3621 Omnikey 3821 Omnikey 4040 Omnikey 4321	Omnikey 4321 Omnikey 6121 Omnikey 6221 Omnikey 6321 Omnikey 5321 ... és még sok más	

Aktív hálózati elemek / Hálózatbiztonság www.barracudanetworks.com

Veszély/jelenség	Javaslat	Igény az ügyfél oldalán	A gyártó megoldása
- szűretlen hálózati forgalom - a nem használatos portok engedélyezve vannak - hálózati szintű támadások - vírus-, web-, spamszűrés, IPS használata nélküli fenyegetések - fájlcserélő szoftverek burjánzása - távoli hozzáférés igénye	- integrált tűzfal bevezetése	- nagy megbízhatóság - Layer 7 alkalmazáskontrol - peer-to-peer alkalmazások blokkolása - web és mail szűrés - vírus és malware védelem - behatolásgátlás (IPS) - hozzáféréskontrol (NAC) - VPN - szofisztikált központi menedzsment	Barracuda NG Firewall 
- a clusterben működő szerverek leterheltsége nincs egyenlően megosztva	- bejövő forgalom optimális szétosztása a szerverek között	- egyszerű kezelhetőség egy webes interfészen keresztül - SSL offload funkció - HA kiépítési lehetőség - IPS - a forgalom tartalom alapján történő irányítása a megfelelő szerver felé - web tartalom cachelése - Layer 4 és Layer 7 load balancing (Model 340-től)	Barracuda Load Balancer 

Aktív hálózati elemek / Hálózatbiztonság www.watchguard.com

A WatchGuardot 1996-ban alapították és azóta több, mint 600.000 WatchGuard terméket telepítettek le világszerte. Mostanra több, mint 15.000 dedikált partnerrel rendelkeznek szerte a világban. A WatchGuard központja Seattleben, Washington államban található, ezen kívül vannak fiókirodák még Észak-Amerikában, Dél-Amerikában, Európában és az ázsiai, csendes-óceáni régióban. A WatchGuard díjnyertes terméke az XTM (extensible threat management) hálózatbiztonsági tűzfala, amely megvéd a behatolásoktól, spamektől, vírusoktól és malwarektől emellett még VPN csatornák megvégződtetésére is alkalmasak.

Veszély/jelenség	Javaslat	Igény az ügyfél oldalán	A gyártó megoldása
- szűretlen hálózati forgalom - a nem használatos portok engedélyezve vannak - hálózati szintű támadások - vírus-,web-,spam-szűrés, IPS használata nélküli fenyegetések	- Integrált tűzfal/ IPSec, SSL és PPTP VPN	- kisvállalatok számára - vírusirtó és kémprogramok elleni védelem (AVG) - spamszűrés és webes tartalom korlátozása - mély csomagelemzés és behatolás detektálás (Deep Inspection) - IPSec, SSL, PPTP és Site-to-Site (IPSec) VPN-re való használhatóság - WiFi képesség 802.11 b/g/n - termékcsaládon belül upgradelhető licence segítségével - több Internet kijárat támogatásának lehetősége	WatchGuard XTM 2 
- szűretlen hálózati forgalom - a nem használatos portok engedélyezve vannak - hálózati szintű támadások - vírus-,web-,spam-szűrés, IPS használata nélküli fenyegetések	- Integrált tűzfal/ IPSec, SSL és PPTP VPN	- közép és nagyvállalatok számára - vírusirtó és kémprogramok elleni védelem (AVG) - spamszűrés és webes tartalom korlátozása - mély csomagelemzés és behatolás detektálás (Deep Inspection) - IPSec, SSL, PPTP és Site-to-Site (IPSec) VPN-re való használhatóság - Reputation Authority - termékcsaládon belül upgradelhető licence segítségével - több Internet kijárat támogatásának lehetősége	WatchGuard XTM 5, 8 és 1050 
- a kívülről érkező felhasználók nincsenek megfelelően azonosítva - a külső felhasználók gépei nincsenek átvizsgálva biztonsági szempontból	- SSL VPN hozzáférés biztosítás a hálózati erőforrásokhoz	- sok távmunkás a hálózaton - erőforrás biztosítása más cégek számára - biztonságos hozzáférés megteremtése - távmunkások technikai problémáinak megoldása	WatchGuard SSL 100 és 560 

	Az Avira GmbH a vállalati és az otthoni IT-biztonsági megoldások egyik vezető globális szállítója, ügyfeleinek száma világszerte meghaladja a 120 milliót. A 20 éves múltra visszatekintő német vállalat 300 alkalmazottal és több országra kiterjedő partnerhálózattal rendelkezik. Az Avira felhasználói táborában egyaránt megtalálhatók a világ tőzsdéin is szereplő nagyvállalatok, kis- és közepes cégek, otthoni felhasználók, valamint oktatási, illetve köz- és államigazgatási intézmények.		
Veszély/jelenség	**Javaslat**	**Igény az ügyfél oldalán**	**A gyártó megoldása**
- az Interneten keresztül érkező vírusok, malwarek - emailek nem esnek át vírus vizsgálaton (POP3, IMAP, SMTP)	- kliens oldali antivírus rendszer cégek számára	- Vírus és malware védelmi rendszer - AntiAd/Spyware eltávolítja az ad/spyware-eket - AntiPhising megvédi az adatainkat az adathalászati támadásokkal szemben - MailGuard ellenőrzi az emailen keresztül érkező forgalmat (POP3/SMTP/IMAP) - megvéd a rosszindulatú weboldalaktól - AHeaDTechnology profilok alapján detektálja a még ismeretlen vírusokat	Avira AntiVir Professional
- az Interneten keresztül érkező vírusok, malwarek - emailek nem esnek át vírus vizsgálaton (POP3, IMAP, SMTP)	- kliens és szerver oldali vírus védelem - Avira AntiVir Professional - Avira AntiVir Server (Windows, Linux/Unix) - Avira Security Management Center	- Kliens oldai vírus védelem (Avira AntiVir Professional) - Szerver oldali védelem, mely az alábbi funkciókat tartalmazza (Avira AntiVir Server) - Offline VMWare image ellenőrzés (Windows) - Archív fájlok megvizsgálása több beágyazási szinten keresztül és még más opciók is az archív vagy scannelésen átesett fájlokra - 32 és 64 bites Linux rendszereken is futtatható beleértve az on-access scannelést - központilag menedzselhető rendszer (Avira Security Management Center)	Avira AntiVir NetWork Bundle
- az Interneten keresztül érkező vírusok, malwarek	- kliens és szerver oldali vírus védelem - Avira AntiVir Professional - Avira AntiVir Server (Windows) - Avira Security Management Center - Avira AntiVir Exchange + Avira AntiSpam	- Az összes ki-, és bejövő és a rendszeren belül küldött emailek valós idejű átvizsgálása - Az emailek csatolmányainak rekurzív vizsgálata, még akkor is ha azok tömörített fájlban vannak - Csatolmányok vizsgálata, azok típusa és/vagy mérete alapján - Fingerprint detektálás bináris és/vagy név minta alapján - A manipulált Outlook elemek és Outlook formok teljeskörű vizsgálata az emailekben - Spam szűrő és a bizalmas vagy nem kívánt tartalom blokkolása	Avira Business Bundle

Végpont védelem

DriveLock 6 Intelligent Data Protection

A CenterTools-t 1999-ben alapították Németországban azért, hogy ügyfél specifikus megoldásokat fejlesszenek cégek részére. A CenterTools egyik zászlós hajója a DriveLock, ami vezető megoldást nyújt a végpontok ellenőrzésében. Napjainkban több telephellyel rendelkezik Európában és Észak-Amerikában.

Veszély/jelenség	Javaslat	Igény az ügyfél oldalán	A gyártó megoldása
- a hálózatban működő desktopok / laptopok portjai nincsenek védve, eszközök csatlakoztatása korlátlan	- vállalati adatvagyon védelme	- szabályok létrehozás a különböző portok használatára - a szabályok mindenkori érvényre juttatása - egyszerű, intuitív kezelőfelület - különböző mobil eszközök tiltása, ill. engedélyezése - akár személyenként is konfigurálható szabályok - fájl szűrők létrehozása az egyes fájltípusok blokkolására	DriveLock 6
SafeNet	A SafeNet a világon a 3. legnagyobb informatikai biztonsággal foglalkozó cég, amely integrált megoldásokat kínál az ügyfelei egyre növekvő biztonsági kihívásai számára. Tevékenységei között szerepel a **digitális jogok védeleme** (DRM), **az interaktív és proaktív tartalomszűrés** (eSafe), az **erős (több faktoros) azonosítás** (eToken) és a **titkosítás** (Protectdrive, Datasecure) A szervezet több, mint 25.000 ügyfelet szolgál ki a kormányzati és a vállalati szektorban több, mint 100 országban.		
- elveszett vagy ellopott laptop / desktop merevlemeze nincs védve	- merevlemez titkosítás	- merevlemezen tárolt adatok biztonságban tartása - céges és személyes adatok védelme - központi menedzsment - pendrive titkosítás	ProtectDrive
- az illetéktelen hozzáférések nincsenek korlátozva a fájl szervereken és munkaállomásokon tárolt dokumentumokhoz - a Windows jogosultságkezelés nem elegendő	- fájl titkosítás	- fájlok védelme mind a kliens, mind a szerver gépeken - transzparens titkosítás felhasználói oldalról nézve	ProtectFile
- adatbázis szervereben tárolt információk ellopásának lehetősége	- adatbázis titkosítás	- transzparens adatbázis titkosítás, SQL server, Oracle, DB2, stb.	ProtectDB
- biztonságos távoli hozzáférés a válalati hálózathoz	- VPN	- hálózati forgalom titkosítása - tetszőleges gyártó termékével együttműködjön	HighAssurance Remote Desktop VPN