Póserné Oláh Valéria
Budapesti Műszaki Főiskola NIK, poserne.valeria@nik.bmf.hu

A TÁVOLI MUNKAVÉGZÉS BIZTONSÁGI KÉRDÉSEI, MEGOLDÁSI LEHETŐSEK WINDOWS SZERVEREK ESETÉN

Absztrakt

A szervezetek hatékony működtetéséhez ma már elengedhetetlen a vállalati informatikai rendszerek erőforrásaihoz való távoli hozzáférés biztosítása, mérlegelve a velejáró kockázatokat, valamint a megfelelő technológiák kiválasztása, alkalmazása a „biztonságos" távelérés érdekében. A cikk célja az informatikai rendszerekhez távolról történő hozzáférések biztonsági kockázatainak, a leggyakoribb megvalósítási módszereknek a vizsgálata a vállalatok hálózatának védelme, valamint a kommunikációnak a biztonságossága szempontjából. A megfelelő megoldás keresése e két szempont figyelembevételével egyre sürgetőbb probléma, mivel a távelérést lehetővé tevő technológiák rohamos terjedése szükségképpen az igények egyre nagyobb mértékű növekedését vonja maga után.

Kulcsszavak: *távoli munkavégzés biztonsága, biztonságos távmunka, távelérés formái*

BEVEZETÉS

Napjainkban, amikor az információs technológia életünk szerves részévé vált, elképzelhetetlen a vállalatok működése számítógépek, számítógép-hálózatok alkalmazása nélkül. Rohanó világunkban egyre nagyobb jelentőséggel bír a távoli munkavégzés lehetősége. A mobilitás nagymértékben növelheti egy szervezet hatékonyságát, a távoli munkavégzés lehetővé teszi, hogy a munkatársak, szükség esetén a partnerek, ügyfelek otthonról vagy a világ bármely részéről feladataik elvégzése céljából el tudják érni a vállalati erőforrásokat. A távoli munkavégzést lehetővé tevő technológiák elterjedésével az igény annak használatára egyre növekszik. A háztartások egyre nagyobb arányban teszik lehetővé a hálózati kapcsolat használatát, de nyilvános helyeken (internet kávézók, hotspot-ok, repülőterek, stb.) is lehetőség nyílik interneten keresztül elérni a vállalati hálózatot. A felhasználók száma egyre nő, a vállalat saját felhasználói egyre több és több opciót szeretnének elérni otthonról is a munkahelyi hálózatból. Megjelentek a speciális dolgozók, mint a távmunkások, az utazó felhasználók, és olyan ügyfelek, partnerek, beszállítók, akiknek szükséges hozzáférést biztosítani a belső hálózathoz.

A ZyXEL legutóbbi felméréséből kiderül, hogy a távolról dolgozó felhasználók 87 százaléka az otthoni számítógépét is használja a munkavégzés során, mely eredmény indokolja a témakörrel való foglalkozás, biztonságos megoldások keresésének szükségességét. A mobil munkavégzés, mely sokszor nagyon hatékony, egyre nagyobb teret hódít, de komoly biztonsági kockázatot is jelenthet, hiszen ezek a távoli kapcsolatok veszélyeztethetik is a vállalati rendszereket. [1]

A távoli elérés sosem biztonságos, mivel távolról a tartományba bejelentkezett gépre alapesetben nem hat semmilyen tartományi eszköz (csoportházirend, központi vírusirtó, frissítéseket ellenőrző és azok naprakészségéről gondoskodó alkalmazások, stb.), nem állapítható meg, hogy biztonságos-e a vállalati hálózathoz kapcsolódó számítógép. Mindez nagy dilemma elé állítja a vállalat vezetését, a biztonságért felelős szakembereket. A következő kérdések merülnek fel: Nyújtsanak-e elérést a velejáró kockázatokat vállalva?

Kinek, mennyit? Milyen technológia alkalmazásával tehető biztonságossá a távoli elérés, stb.? A cikk célja e kérdésekre keresni a válaszokat, és megfelelő eszközöket, technológiát javasolni.

1. A TÁVOLI MUNKAVÉGZÉS BIZTONSÁGA

A távoli munkavégzés biztosítása ma már több szempontból is elengedhetetlen. A hatékonyabb működés érdekében nem lehet figyelmen kívül hagyni sem a dolgozók, sem pedig az ügyfelek, partnerek igényeit. A legtöbb cég esetében biztosítani kell webszerverek, SharePoint portál szerverek (SPS) távoli használatát legalább a belső dolgozók számára, azonban fokozott körültekintéssel kell eljárni, mert, ha egy kapcsolat nem biztonságos, akkor a támadók komoly károkat okozhatnak a vállalat informatikai rendszereiben.

A távoli munkavégzés biztonságának vizsgálatát két oldalról közelítettem meg. Az egyik **a vállalatok hálózatának védelme**, a másik pedig magának **a kommunikációnak a biztonságossága**. A megfelelő megoldás keresése közben egyik szempont sem hagyható figyelmen kívül. Mindkettőt alaposan át kell gondolni, mielőtt bármilyen technológia alkalmazása mellett döntenénk, hiszen a vállalati hálózathoz csatlakozó távoli számítógép megfelelő állapotvizsgálata nélkül az komoly veszélyt jelenthet a vállalati informatikai rendszerekre, ugyanakkor legalább ilyen jelentőséggel bír a kommunikáció nem megfelelő titkosításának hiányában lehallgatható információhoz való illetéktelen hozzáférés lehetőségének kizárása is.

A legtöbb esetben a legbiztonságosabb megoldásnak a Virtual Private Network (VPN) kialakítását tartják, ami kétségkívül megoldja a kommunikáció biztonságának kérdését, mivel ilyenkor egy titkosított alagút jön létre a vállalati hálózat és a távoli kommunikációs eszköz között. De a későbbiekben látható, hogy bár tényleg ez tűnik a legbiztonságosabb módnak a távoli elérés biztosítására, azonban sok esetben felesleges, sőt akár kockázatos is lehet, vagy kivitelezhetetlen (pl. a távoli számítógép operációs rendszere nem támogatja), annak ellenére, hogy majd minden cégnél működik VPN-szerver.

A távoli elérés kommunikációja biztonságosan megvalósítható Secure Shell (SSH) segédprogram használatával is Microsoft és Unix/Linux rendszerek esetén egyaránt, azonban a kliens alkalmazások konfigurálása egy általános felhasználó ismeretei alapján nem valósítható meg, ezért ez a technológia nem tekinthető általánosan jó megoldási módszernek.

A problémakör pontosabb feltárásának érdekében megvizsgáltam a távmunka-rendszerekkel szemben támasztott követelményeket, sorra vettem a legfontosabb területekre irányuló távelérési formákat, azok biztonsági problémáit és a problémák megoldása kapcsán figyelembe vehető megoldási módokat.

1.1 A távmunka-rendszerekkel szembeni általános elvárások

Az igényeket, körülményeket, lehetőségeket felmérve megállapítható, hogy a távmunka-rendszerekkel kapcsolatos legfontosabb elvárások a következők:

1 A bejelentkezés egyszerűen, lehetőleg „egy gombnyomásra” történjen,

2 megfelelő sebesség a kliens oldalon,

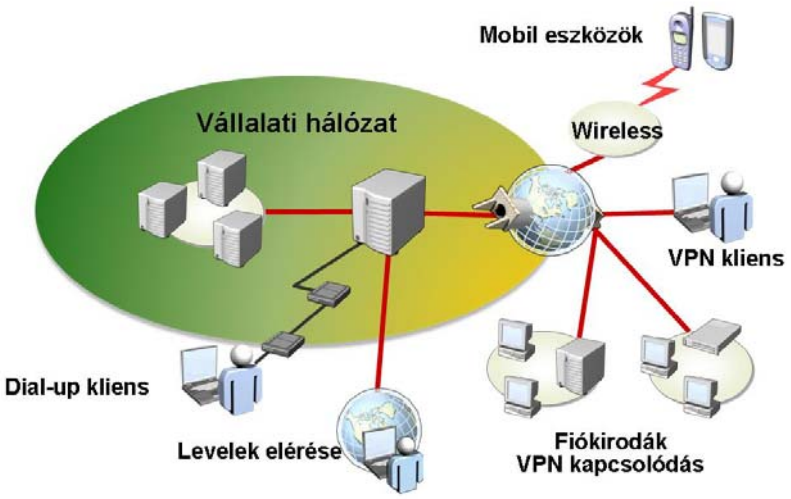
3 a kommunikáció olcsó legyen, és helyfüggetlen,

4 a bejelentkezőt egyértelműen tudja azonosítani,

5 a kommunikáció megfelelő algoritmussal titkosított legyen.

1.2 A távelérés formái az elérendő célok tükrében

A vállalati hálózathoz való kapcsolódási igények leggyakoribb formáit az 1. ábra szemlélteti.



1. ábra: A vállalati hálózathoz való kapcsolódási igények formái [2]

A távelérési formákat az elérni kívánt cél szerint három fő csoportba lehet sorolni:

1. **Levelezés, csoportmunka:** ennek a szolgáltatásnak az elérése teszi ki az igények döntő többségét és a vállalatok túlnyomó része meri is és biztosítja is.

2. **A vállalati erőforrások teljes körű (jogosultságoknak megfelelő) használata:** az erőforrások teljes körű használata távoli helyről ma még nem túl gyakori, de előfordulhat, hogy szükséges például fájl megosztások elérése (megnyitás, szerkesztés, nyomtatás, stb.).

3. **Alkalmazások futtatása, távfelügyelet:** helyi erőforrások használata Remote Desktopon keresztüli munkához (korábban a Neptun tanulmányi rendszer is ilyen terminál rendszerrel működött).

1.3 Problémák és biztonságos megoldási lehetőségek a távelérés különböző formáira

1.3.1 Levelezés, csoportmunka

Ha csak levelezési szolgáltatást kíván a vállalat nyújtani, arra véleményem szerint nem szükséges VPN kapcsolat kialakítása, sőt veszélyes is lehet, mert VPN esetében az esetleg vírusos távoli gép is a vállalati hálózat részévé válik, ezenkívül a megvalósításhoz használt technológia függvényében bizonyos szakértelmet kívánhat meg a távoli számítógép felhasználójától, amivel az esetek túlnyomó részében a felhasználók nem rendelkeznek.

A távoli eszköz biztonságosságának vizsgálata, valamint a szakértelem hiánya megoldható ugyan egyéb eszközök kombinált alkalmazásával, azonban ebben az esetben felesleges, mivel számos, webes felületen elérhető, a távmunka-rendszerekkel szembeni elvárásoknak

többségében megfelelő levelező-alkalmazás áll rendelkezésre, melyek segítségével a távoli felhasználó biztonságosan hozzáférhet postafiókjához:

- Outlook Webaccess, – használata esetén be lehet állítani, hogy titkosítatlanul ne közlekedjen soha a jelszó, hátránya, hogy nem lehet offline módban használni.

- Outlook – RPC over http használatával az Outlook kliens egy titkosított csatornán közvetlenül kapcsolódik a kiszolgáló Exchange szerverhez, SSL alagútba tereli a forgalmat a tűzfaltól kifele illetve a tűzfalig.

- Pop3, IMAP: alkalmazásuk esetén sem túl nehéz letiltani a titkosítatlan változatot, ekkor nem csak a jelszavakat védik, hanem a levél tartalmát SSL csatornába tereli.

- Outlook Mobile Access – könnyen lehet titkosítani, de hátránya, hogy nem lehet offline módban használni.

1.3.2 A vállalati erőforrások teljes körű (jogosultságoknak megfelelő) használata

Az lenne az ideális, ha létezne egyidejűleg egyszerű és biztonságos módszer.

Lehetőségek:

- **FTP:** felhasználói körökben a legnépszerűbb, legelterjedtebb távoli hozzáférési forma, azonban nehéz vagy nem lehet megoldani, hogy az információ, a jelszavak titkosított formában közlekedjenek a hálózaton. Vállalati oldalról le lehet ugyan tiltani a szolgáltatást, de a felhasználó attól még próbálkozhat és attól függetlenül, hogy a szolgáltatás nem biztosított a jelszó átmegy a hálózaton. Ezt bizonyította például az Elender feltörésekor nyílvánosságra került felhasználónév-jelszó lista is, ahol esetenként egy felhasználónévhez több jelszó is társult, mert a felhasználó a bejelentkezési kísérletezés során begépelte a jelszavát, újra próbálkozott, esetleg elgépelte és újrapróbálkozott. [2]

- **SSL-en keresztül a SharePoint segítségével:** a megtervezett, rendszeresen felügyelt és karbantartott konfiguráció többségében eleget tesz az 1.1-ben megfogalmazott elvárásoknak. **„…**lehetővé teszi a közösségi csoportmunkát, és biztosítja a felhasználók számára a dokumentumokon, a feladatokon, a kapcsolattartókkal és az eseményekkel kapcsolatban végzett közös munka feltételeit. Emellett lehetővé teszi a csoportok és a webhelyek kezelői számára a webhely tartalmának és a felhasználók tevékenységének egyszerű felügyeletét.” [3]

- **Karantén VPN:** ha nincs lehetőség SharePoint használatára, akkor karantén VPN alagutat kell használni, célirányosan korlátozva, hogy csak bizonyos szolgáltatást lehessen használni, mint például. néhány szerveren néhány erőforrás elérése, ami alapján kideríthető a bejelentkező számítógépről, hogy az állapota megfelelő-e vagy sem. A VPN karantén a VPN kliensek számára egy olyan vizsgálatban való kötelező részvétel, amely során különböző feltételeket támaszt az üzemeltető a klienssel szemben és a VPN kliensnek kötelessége azokat teljesíteni. Ilyen feltételek lehetnek például: legyen bekapcsolt vírusirtója, tűzfala, legyen rajta a megfelelő szervizcsomag, stb. Ha a kliens nem felel meg a támasztott követelményeknek, akkor hozzáférhet azokhoz az erőforrásokhoz, amelyek alapján teljesítheti a követelményeket (megfelelő jogosultság esetén), például letöltheti a szükséges frissítéseket. Ha ezek után teljesülnek a klienssel szemben támasztott követelmények, akkor beléphet a hálózatba, ha nem akkor bejelentkezési kérelme

elutasításra kerül.

1.3.3 Alkalmazások futtatása, távfelügyelet

Lehetőségek:

- **RDP 6.0 (Remote Desktop Protocol):** a távoli felhasználó kap egy távoli asztalt, az admin távvezérelheti a hálózatot (szervereket, kliens gépeket). Akkor célszerű használni, ha többre van szükség, mint a webes alkalmazások elérése, de nincs szükség teljes hálózati elérés biztosítására (VPN kapcsolat). 128 bites az alapértelmezett titkosítás.

- **RDP over SSL technológia:** ha nagyobb biztonságra van szükség, mint amennyit az RDP 6.0 biztosít, mivel TLS hitelesítést és titkosítást tesz hozzá az RDP kapcsolathoz.

- **Remote Desktop Web Connection:** egy ActiveX vezérlő segítségével böngészőből lehet használni az RDP kapcsolatot. Alacsony sávszélesség-igénye van – akár még modemen is tűrhető sebesség érhető el vele. További előnye, hogy nem csak Windows platformra alkalmazható. Régi hardverek számára is ideális. Hátránya, hogy az RDP over SSL-t nem támogatja, valamint, hogy az ActiveX vezérlők használata fokozott körültekintést kíván meg a klienstől, mert ugyan a weblapokon megjelenő aktív tartalom nagy része biztonságos, bizonyos weblapok olyan aktív tartalommal is rendelkezhetnek, amely veszélyezteti a számítógép biztonságát. Az Internet Explorer biztonsági szintjeinek használatával megelőzhetők az esetleges adatvédelmi problémák kialakulása, de ennek biztonságos kezelése további szakértelmet igényel.

- **W2K3 üzemeltetés HTTPS-sel:** elérhető a távfelügyelt szerver néhány beállítása a 8098-as porton https-sel, mint például admin jelszó változtatása, szerver neve, a Webszerver szinte összes fontos beállítása. Megtekinthetők például egy IP kapcsolat tulajdonságai (át lehet nevezni, meg lehet változtatni az IP-t, a DNS-t, stb.). Hozzá lehet férni a helyi felhasználói adatbázishoz, meg lehet nézni, törölni, letölteni a naplófájlokat, ha van SMTP kiszolgáló riasztással e-mail küldését beállítani, szükség esetén le lehet állítani vagy újraindítani a szervert, stb.

1.4 A jelszavak problémája

Vizsgálódásaim alapján megállapíthatom, hogy a legnagyobb gondot – a távolról elérni kívánt információ bizalmasságának megőrzésén túl – a jelszavak használata okozza. Köztudomású, hogy egy informatikai rendszerben mindig az ember a leggyengébb láncszem, aki a jelszavak biztonságos használatában döntő fontosságú tényezőként játszik szerepet. A felhasználók sok esetben nem használják kellően körültekintően, elárulják a jelszavukat (könnyű elkövetni akaratunkon kívül is). Ehhez társul még az is, hogy lehetőség van a Single Sign On – mindenhova egy jelszó – alkalmazására, ami nagyon kényelmes, hisz a felhasználónak a rendszerbe történő belépésekor pusztán egyetlen név-jelszó párost kell megadnia ahhoz, hogy jogosultságának megfelelően hozzáférjen az összes vállalati erőforráshoz, nem kell külön bejelentkezni a különböző szolgáltatások igénybevételéhez. A belső hálózathoz való hozzáférés esetén általában erős jelszó használatát követelik meg az üzemeltetők, de mindez mit sem ér, ha a távoli munkavégzés során is ezt az azonosító párost kell használni, például interneten keresztül is titkosítatlanul, ahol tudvalevő, hogy léteznek még 30-40 éves technológiák is, melyek esetén nincs megfelelő védelem.

A jelszavak alkalmazásának kiváltása más azonosító módszerrel, mint például

tanúsítványok vagy biometrikus jellemzők alkalmazása területen folynak ugyan kutatások, de széleskörű elterjedése egyelőre várat magára. A biometriai azonosítók alkalmazása egyértelműen megoldaná a jelszavak problémáját, azonban a megbízható technológia jelenleg még nem áll rendelkezésre, vagy csak igen költségesen valósítható meg. [4]

2. TÁVOLI HOZZÁFÉRÉSI MEGOLDÁSOK

2.1 E-parlament

Egy természetes igény a parlamenti munka kapcsán is, hogy a képviselők megfelelő biztonsági szabályok betartása mellett otthonról, illetve távoli munkahelyről is be tudjanak kapcsolódni a parlamenti munkafolyamatokba.

A megfelelő biztonság megteremtése érdekében 2003-tól szigorú szabályok mellett használható, előre konfigurált laptopokat alkalmaznak, melyekkel csak előre meghatározott célokkal és helyekről (hivatali környezet, ülésterem, a felhasználó által megjelölt helyszínek) lehet kapcsolódni a Hivatal hálózati erőforrásaihoz. A távmunka biztonságát, a hitelesítést, titkosítást, elektronikus aláírást X.509 digitális tanúsítványok tárolására is alkalmas intelligens (smart) kártya garantálja. Külön védelmet biztosít a laptop jogosulatlan tulajdonba kerülése ellen, hogy az operációs rendszer indítása a felhasználó részére kiadott chipkártya (OGYchip) azonosításához kötött. A felhasználó azonosítása az OGYchip és a hozzáférési hely azonosításával történik. Központi hálózatról történik a vírusvédelem rendszeres frissítése. A felhasználó nem rendelkezik rendszergazdai jogosultsággal, így idegen programot nem telepíthet. A hálózati támadások ellen a Hivatal által kialakított, lokálisan nem megváltoztatható szabályrendszerrel működő tűzfal véd. [5]

A módszer hátránya, hogy igen költséges ezért vállalati környezetben ma még elképzelhetetlen, hogy a cég minden dolgozója, partnere, ügyfele számára így biztosítson távoli hozzáférési lehetőset.

2.2 Az operációs rendszer USB flash memóriáról történő betöltése

A számítógép bekapcsolása után az operációs rendszer egy USB flash memóriáról töltődik be, melyre előre konfigurálhatók a távoli elérést biztosító kapcsolat beállításai. Ha a merevlemez tartalmaz is kártékony kódot, ebben az esetben az nem tud tovább fertőzni. Az eljárás már jóval költségkímélőbb, mint az előző megoldás, hisz egy USB flash memória költsége elenyésző egy laptop árához viszonyítva, azonban gondot okozhat az operációs rendszer és egyéb alkalmazások licenszelési kérdésköre. [6]

2.3 A Cisco„Önvédő hálózat” koncepciója

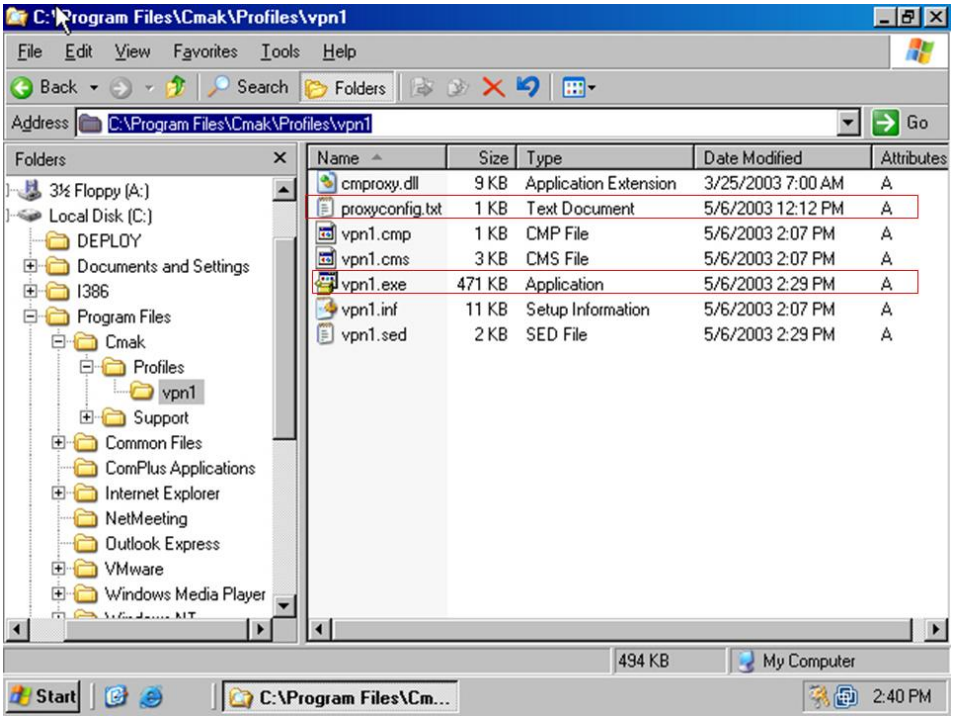
Lényegében megegyezik a karantén VPN elveivel. [7]

2.4 Előre definiált VPN beállítások csomagban

Ha már mindenképpen elkerülhetetlen VPN kapcsolat kialakítása, akkor például a Microsoft Connection Manager Administration Kit (CMAK) segítségével előredefiniált VPN kliens beállítások és (opcionálisan) kiegészítő eszközök, mint például proxy beállítások csomagolhatók össze a felhasználónak egy .exe fájlba, melyet, ha bármelyik távoli számítógépen lefuttat, akkor automatikusan egy testreszabott VPN kapcsolatot képes kialakítani a vállalati hálózathoz. Előnye, hogy ekkor a VPN kliens kötelezően azokkal a

beállításokkal fog majd belépni a hálózatba, amit a csomagban számára előre előírtunk. [8]

Megadható például, hogy hitelesítés, titkosítás szükséges-e a bejelentkezéshez, ha igen, akkor milyen. Az adott felhasználó milyen kapcsolaton keresztül jelentkezhet be, mi történjen a kapcsolat felépítése után és a leváláskor (például törlődjenek a beállítások, ami nyilvános számítógép esetén különösen hasznos). Milyen telefonszámon kérhet segítséget probléma esetén, stb. A 2. ábrán látható, eredményként keletkező .exe és esetlegesen (proxy beállítás megadása esetén) .txt fájlokat kell a felhasználóhoz eljuttatni, mely megtehető akár egy USB kulcs átadásával is, melyen a még nagyobb biztonság érdekében önkicsomagoló formában (egy jelszót fog kérni a kicsomagoláskor) titkosítva adhatók meg a fájlok (a kulcs esetleges elvesztése, illetéktelen kezekbe jutása esetén védelmet nyújt).



2. ábra: A CMAK eredménye

Ezután a felhasználónak csupán az .exe fájlt kell lefuttatnia a világ bármely számítógépén és készen kapja a VPN kapcsolatot a vállalati hálózathoz.

3. ÖSSZEGZŐ MEGÁLLAPÍTÁSOK

A ZyXEL felmérése arra is rávilágít, hogy a biztonsági szakemberek aggodalma ellenére tovább fog nőni a távoli munkavégzés népszerűsége, éppen ezért szükséges annak biztonságos voltát szavatoló konstrukciók kidolgozása. Néhány megoldás született már, mint a Microsoft karantén VPN technológiája, vagy a Cisco „Önvédő hálózat” koncepciója, ami lényegében megegyezik a karantén VPN elveivel.

A BeCrypt pedig a hordozható számítógépek használatával járó veszélyforrások a („… notebookokról számos kártékony program kerülhet be a vállalati rendszerekbe, illetve onnan bizalmas adatok szivároghatnak ki …”) [4] megszüntetése érdekében USB flash memóriákra épülő biztonságos rendszert tervezett, melynek lényege, hogy a notebook bekapcsolása után az operációs rendszer egy USB flash memóriáról töltődik be. Így, ha a PC merevlemeze tartalmaz is kártékony kódot, az nem tud tovább fertőzni.

Első megközelítésben távoli munkavégzés biztonságos megvalósítására VPN kialakítása lenne célszerű, de tekintve a megvalósítás nehézségeit (szakértelem hiány, operációs rendszer nem teszi lehetővé, nyilvános helyek problémái, stb.) és kockázatait (kellő körültekintés nélkül könnyen bekábelezhető a vállalati hálózatba nem biztonságos számítógép is), érdemes alaposan megfontolni, hogy milyen célok elérésére is van szüksége a távoli felhasználónak és annak megfelelően kiválasztani az anyagi lehetőségektől is függő megfelelő technológiát.

Ma még a kliensek az esetek többségében csupán leveleik letöltésére használják a vállalati hálózatot, mely esetben a komplett VPN helyett érdemes inkább megfelelő titkosítási lehetőséggel rendelkező levelező alkalmazás használata, mint például az Outlook Web Acces, illetve az Outlook azon képességét kihasználni, hogy képes HTTPS-en keresztül szinkronizálni a levelesláda tartalmát.

Ha ezen túlmenően még a hálózati megosztásokra is szükség van, szűkített VPN-kapcsolatot ésszerű használni, ami mindössze ezt a funkciót nyújtja, a kártevőknek viszont nem nyit utat.

Gyakran szükséges emeltszintű munkavégzés biztosítása is, a távoli asztal (Remote Desktop), távfelügyelet használata, melynek segítségével biztonságosan kezelhetünk akár egy tucat szervert távolról.

Ha már mindenképpen elkerülhetetlen a VPN kapcsolat kialakítása, akkor célszerű a felhasználó, ügyfél, partner számára a megfelelő beállításokkal előre preparálni azt, és például a CMAK segítségével előállított fájlokat megfelelő titkosítással a rendelkezésükre bocsátani. Így biztosítható, hogy a VPN kliens kötelezően azokkal a beállításokkal fog belépni a vállalat hálózatába, amit a csomagban előre előírtunk számára.

Felhasználóknak szóló tanácsok:

- Ne használjunk FTP-t, vagy, ha igen, akkor, amennyiben megoldható ne a fontos titkos név-jelszót használjuk.
- Ne használjunk titkosítatlan levélolvasást (pl. POP3, bár szerver oldalon be lehet állítani az SSL titkosítást és le lehet tiltani a titkosítatlant).
- Ne használjuk a vállalati jelszavunkat, ha az URL sima http-vel kezdődik, bár gyakran egy http bejelentkezési oldal esetleg titkosított oldalra dobja tovább a kérést.

FELHASZNÁLT IRODALOM

[1] Biztonságportál: Aggodalmak a távoli munkavégzés miatt, http://www.biztonsagportal.hu/article3088.html , 2007.10.03.

[2] Gál Tamás: Távoli elérés és munkavégzés, http://www.microsoft.com/hun/webcast/default.aspx?id=ddc36344-a968-4386-95b3-f990b46cb346, 2006.12.21.

[3] Microsoft: Windows SharePoint Services – áttekintés http://www.microsoft.com/hun/windowsserver2003/sharepoint_overview.mspx, 2007.06.01.

[4] Zs. Zs. Kurdi: „Adaptive User-Authentication with Biometrics”, Proceedings of the 5th International Conference of Ph.D. Students, Miskolc, 2005., ISBN 963 661 679 5

[5] Kertészné Gérecz Eszter: AZ E-PARLAMENT http://www.neumann-centenarium.hu/kongresszus/prog16.html?v%5Bid%5D=63, 2007.10.03.
[6] Kristóf Csaba: Operációs rendszer USB-memórián http://computerworld.hu/operacios-rendszer-usb-memorian.html, 2007.04.18.
[7] Cisco Systems: PREVENTING WORM AND VIRUS OUTBREAKS WITH CISCO SELF-DEFENDING NETWORKS, http://www.cisco.com/application/pdf/en/us/guest/netsol/ns481/c654/cdccont_0900aecd801dff73.pdf, 2007.10.05.
[8] Microsoft TechNet: Microsoft Windows Server 2003 TechCenter, http://www.microsoft.com/technet/prodtechnol/windowsserver2003/hu/library/ServerHelp/5cd571d6-7fdc-483d-8899-0a337acc9cf9.mspx?mfr=true, 2007.06.01.