Jéri Tamás – Pándi Erik – Jobbágy Szabolcs
jeri.tamas@gmail.com – pandi.erik@zmne.hu – jobbagy.szabolcs@zmne.hu

A HÁLÓZATOK VÉDELMI ASPEKTUSAI[1]

Absztrakt

Jelen közlemény az IT hálózatok védelmének kérdéseit világítja meg.

This publication sheds light on questions related to the defence and security of IT networks.

Kulcsszavak: *IT hálózat, védelem ~ IT network, protection*

BEVEZETÉS

A témakört tekintve legfőbb cél a biztonság elérése. Az informatikai biztonság, az informatikai rendszer olyan – az érintett számára kielégítő mértékű – állapota, amelyben annak védelme az informatikai rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint a rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.[2] Az informatikai biztonság sajnos nem egy alapértelmezett állapot, eléréséhez aktívan tevékenykedni kell, védelmet kell kiépíteni.

1. A VÉDEKEZÉSI TEVÉKENYSÉG

A védekezés az a cselekvés, amikor megvédünk valakit vagy valamit a támadástól; védelem, megvédés.[3] A védés megakadályozza azt, hogy megtámadjanak valakit vagy valamit, illetve, hogy elfoglalják.[4] A védelem – a magyar nyelvben – tevékenység, illetve tevékenységek sorozata, amely arra irányul, hogy megteremtse, fejlessze, vagy szinten tartsa azt az állapot, amit biztonságnak nevezünk. 22 Az informatikai védelem a rendszerben kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint a rendszer elemei sértetlenségének és rendelkezésre állásának védelme.”

2. VÉDENDŐ HÁLÓZATOK

A hálózatok minden fajtáját egyaránt védeni kell, azonban a rendszerek jellegéből adódóan eltérőek a hangsúlyos pontok, a megvalósítás gyakorlata, illetve módszere.

- Internetbe kötött szerverek

Speciális védendő „hálózatnak” tekinthetők, még akkor is, ha csak egyetlen szerverről van szó. Távoli hozzáférés révén úgy kell megoldani a védelmet, hogy egyrészt biztosítva legyen a szerver teljes körű adminisztrációs lehetősége, másrészt minimális legyen a támadhatóság.

1 a közlemény a Bolyai János Kutatási Ösztöndíj támogatásával készült
2 Dr. Muha Lajos : Informatikai Rendszerek Biztonsága – Előadás 2009.
3 http://wikiszotar.hu/wiki/magyar_ertelmezo_szotar/Védekezés
4 http://wikiszotar.hu/wiki/magyar_ertelmezo_szotar/Véd

- Belső hálózatok
    a) Zárt hálózatok

Ezen hálózatok valószínűleg annyira érzékeny adatokat tartalmaznak, melyek követelményként támasztják a zárt jelleg fenntartását. A védelmet az adatok ki,- és bekerülésének, illetve a hálózat szándékos kinyitásának megakadályozására kell összpontosítani.

b) Félig nyitott hálózatok

A legösszetettebb védelmet igénylő hálózati jelleg, mert a zárt hálózatoknál és az Interneten működő szervereknél kialakított megoldásokat ötvözve kell alkalmazni. Figyelni kell az Internet felöl érkező támadások kivédésére, és a lehető legjobban kell érvényesíteni a zárt jelleget annak ellenére, hogy a hálózatból létezik kilépési pont.

3. SZOLGÁLTATÁS VS. VÉDEKEZÉS

Előfordul, hogy ismerőseink megkérdeznek: vajon lehet-e feltörhetetlen szervert telepíteni? Melyre válaszunk, hogy azt a világ legegyszerűbb dolga létrehozni, melyet persze kétkedve fogadnak. Példaként az ajtó nélküli ház esetét szoktuk említeni: vajon be lehet-e törni egy olyan házba, melynek csak falai, és teteje van? A válasz egyértelműen nem, mely szimbolikusan hasonlít a szolgáltatás nélkül működő szerver esetére. Bármely szerver tehát hálózaton keresztül támadhatatlan, amennyiben nem működik rajta szolgáltatás, melyen keresztül adatcserét lehetne végrehajtani. A problémát pontosan az jelenti, hogy szervereket a szolgáltatások működtetése miatt üzemeltetünk. Tehát bármely szolgáltatás elindítása egyrészt egy alapfeladat működtetését, másrészt egy biztonsági kockázat megjelenését indukálja. Több szolgáltatással működő szerver természetesen nagyobb kockázatot jelent, főleg, ha azok közül valamelyik az operációs rendszer karbantartását szolgálja. Az Internetes kiszolgálók gyakran nagy távolságra üzemelnek annak tulajdonosától, ezért megkerülhetetlen a távoli elérés biztosításának és a megfelelő védelem kiépítésének problematikája.

4. A VÉDEKEZÉS ESZKÖZEI

Tűzfalak építése

A tűzfal (angolul firewall) célja a számítástechnikában annak biztosítása, hogy a hálózaton keresztül egy adott számítógépbe ne történhessen illetéktelen behatolás.[5] Tűzfalat minden IP címmel rendelkező hálózati eszközre lehet telepíteni, ugyanakkor kiemelt jelentősége a belső hálózatok ki,- belépési pontján, valamint az Internetes kiszolgáló szervereken van. A tűzfalmegoldásokra általános érvényű szabály, hogy alapértelmezésben minden tilos, kivéve, amit szabad.

- Packet filter firewall – csomagszűrő tűzfal

Egy statikus szabálygyűjtemény alapján továbbítja, vagy eldobja a csomagokat. A szűrési feltételek protokoll fejlécekre vonatkoznak, a csomag tartalmára nem, ezért gyors tűzfal típus. A fejlett csomagszűrők csendben, visszajelzés nélkül, az elavultabbak visszajelzéssel dobják el a csomagokat. A csomagszűrés a tűzfalak leggyakrabban használt fajtája, ma már a legolcsóbb routerekben is rendelkezésre álló lehetőség.

- Circuit-level firewall – kapcsolat alapú tűzfal

Előre definiált szabályok alapján működik, viszont nem csomagokat, hanem kapcsolatokat kezel. A kapcsolatépítést figyeli, rövid ideig figyelemmel kíséri, majd dönt

5 http://hu.wikipedia.org/wiki/Tűzfal_(számítástechnika)

annak biztonságosságáról. Pozitív elbírálás után tovább már nem vizsgálódik, a kapcsolathoz tartozó csomagokat átengedi. Mivel csomagokat nem, csak kapcsolatokat vizsgál, ezért gyorsabb lehet a csomagszűrő tűzfalnál is.

- Application gateway firewall – alkalmazás szintű tűzfal

A hálózatok közötti minden kommunikációt szétvág, és közvetítőként biztosítja a kapcsolatot. Az OSI[6] modell minden szintjén ellenőriz, és teljes vizsgálatot végez, ezért meglehetősen lassú, továbbá speciális szolgáltatás működését ismeret hiányában nem képes ellenőrizni.

Rosszindulatú programok távoltartása

A vírusok, kémprogramok és általában a rosszindulatú programkódok távoltartására kitalált védekező eszköz, mely a háttérben folyamatosan futó alkalmazásként van jelen. A munkaállomások és a szerverek védelmére egyaránt használatos, ugyanakkor fontos megjegyezni, hogy elsősorban az elterjedt, megengedő típusú operációs rendszereken terjednek a rosszindulatú programok, ezért alkalmazásuk főleg ott jellemző. Az alkalmazott távoltartó programok – általában - saját adatbázissal rendelkeznek, melyben a rosszindulatú kódok vannak nyilvántartva, ezért folyamatosan szükséges az adatbázisok frissítése, a legújabb kártékony programok elleni sikeres védekezés érdekében.

A védekező szoftvereknek vannak kedvezőtlen hatásai is, mert az állandó jelenlét elvonhatja az erőforrásokat, mely főleg a kisebb kapacitású számítógépeknél vehető észre, továbbá a frissítési adatbázisok több megabájtos mérete jelentős hálózati forgalmat generálhat.

Titkosítás

A titkosítás alkalmazása nagyon hosszú időre nyúlik vissza, azonban célkitűzése mindvégig az volt, hogy a küldő által küldendő eredeti – nyílt – szöveget oly módon tegye értelmezhetetlenné, hogy harmadik személy birtokában ne legyen információértéke, azonban a címzett képes legyen a kódolt szövegből, az eredeti előállítására.

Ez a lehetőség a számítógép-hálózatokban alkalmazott kommunikációban is kiaknázható, melyet a küldendő – érzékeny – adatok nagy mennyisége is alátámaszt. A titkosítás alkalmazása a szolgáltatások nagy részében rendelkezésre, így biztonságosan lehet:

- leveleket, állományokat küldeni és fogadni;
- távoli adminisztrációt végezni;
- hálózatokat összekapcsolni;
- böngészni az Interneten, stb.

Komoly matematikai kutatások eredményeként többféle titkosítási eljárást fejlesztettek ki, azonban mindegyikre igaz, hogy, egy kulcs segítségével hozza létre a titkos szöveget (ciphertext-et). A szimmetrikus kulcsú titkosítás problémája, hogy a kulcsban az adónak és a vevőnek meg kell egyeznie, azt egymásnak át kell adni, melyre rendszerint ugyanaz a kommunikációs csatorna áll rendelkezésre, s a kulcs megszerzésével a rosszindulatú támadó vissza tudja fejteni, a titkosított szöveget is. A problémára megoldást jelentett a nyilvános, aszimmetrikus kulcsú titkosítás.

A(z) N(T(x))=x és T(N(x))=x képletben ’T’ a titkos, ’N’ a nyilvános kulcsot, ’x’ pedig a kódolandó információt szimbolizálja. A két kulcs együttes alkalmazása szükséges a

6 Open Systems Interconnection Reference Model, magyarul a Nyílt rendszerek Összekapcsolása

titkosított információ visszanyeréséhez, így a széles körben ismertetett 'N' kulcs, a titkosító - kizárólagos - birtokában levő 'T' kulcs nélkül nem alkalmas a dekódolásra.

Az aszimmetrikus titkosító kulcs előnye a biztonságos kulcscsere, hátránya a lassúság, a szimmetrikus kulcs előnye a gyorsaság, hátránya a biztonságos kulcsátadás problematikája. A mai korszerű (SSL[7]) titkosítási eljárásoknál a vegyes használat a jellemző, amikor a kapcsolatépítés aszimmetrikus, majd a tényleges adatcsere szimmetrikus titkosítási kulccsal hajtódik végre.

Proxy használata

„Számítógép-hálózatokban proxynak, helyesebben proxy szervernek (angol „helyettes", „megbízott", „közvetítő") nevezzük az olyan szervert (számítógép vagy szerveralkalmazás), ami a kliensek kéréseit köztes elemként más szerverekhez továbbítja."[8] Mivel a proxy közbenső elem a tényleges kliens és szerver között, beavatkozásra ad lehetőséget, feltételhez kötheti, hogy mit továbbít a kliens felé. A proxy szerver lehetséges használata:

- átmeneti tárolóként (cache) megvalósított gyorsítás;
- tűzfal funkciók alkalmazása;
- kapcsolatok szűrése.

A proxy megoldások több szolgáltatási funkcióra is rendelkezésre állnak, de a legelterjedtebb a web-proxy, mellyel egy belső hálózatból biztosítható, hogy a felhasználók

- közvetlen web kéréseket ne tudjanak az Internet felé indítani;
- a gyakrabban látogatott oldalak tartalmát gyorsabban megkapják;
- csak a munkájukhoz szükséges oldalakat látogathassák;
- nem kívánt adattartalmat ne tudjanak a munkaállomásukra letölteni.

ezáltal ne tudják kitenni a belső hálózatot támadásnak.

Egyéni – ismeretlen – megoldások alkalmazása

Hasonlóan a hétköznapi élethez, a számítógép-hálózatba betörő sem számíthat minden körülményre. A váratlan „fogadtatás", az egyéni kreatív védelmi intézkedések nagyban megnehezíthetik a támadók dolgát, sőt jó eséllyel meg is gátolhatják a behatolást. A védelem feladatai között szereplő észlelés és reagálás együttesen alkalmazható, ha felkészülünk egyes események bekövetkezésére, és kidolgozott tervünk van a reakció végrehajtására.

Az egyéni megoldások kialakítására általában operációs rendszer szinten van lehetőség, mely jól kamatoztatható tűzfalak, átjárók, vagy saját internetes szerver üzemeltetése esetén. Itt meg is jegyezném, hogy egyéni védelmi intézkedést nem lehet, vagy nagyon nehéz alkalmazni célhardvereken. Gyakran halljuk, hogy a legbiztonságosabb tűzfalak hardveresek, aminek biztosan van igazságtartalma, de hogy az operációs rendszereken megvalósított tűzfalakhoz képest kicsi a reagálási képesség, abban biztos vagyok. A hardverekben általában bedrótozott mechanizmusok állnak rendelkezésre, melyek kevés mozgásteret adnak.

7 Secure Socket Layer – biztonsági alréteg, mely a szállítási és valamely alkalmazási réteg között helyezkedik el

8 http://hu.wikipedia.org/wiki/Proxy

5. ÁLTALÁNOS VÉDEKEZÉSI MECHANIZMUSOK

Minden általánosságban alkalmazható védelmi intézkedést meg kell tenni, a lustaság nem kifizetődő. Ebben a részben megpróbáljuk összefoglalni azokat a kötelezően alkalmazandó védelmi intézkedéseket, melyek az alacsony befektetéshez képest, nagyban növelik a rendszerek védelmét.

Általános védelmi intézkedések:

- Operációs rendszerek, alkalmazások frissítése

A programok gyártóinak konkurencia harca gyakran hibás, vagy biztonsági réseket tartalmazó kódok fejlesztéséhez vezet. A nyilvánosságra kerülő hibák kihasználhatók, gyenge láncszemek, ezért a gyártók által kiadott javításokat szükségszerű alkalmazni. A programok készítői – általában – internetes frissítő oldalak üzemeltetésével biztosítják a legfrissebb javítócsomagok letöltését.

- Rosszindulatú programok adatbázisainak frissítése

Hiába működnek rosszindulatú kódokat távoltartó programok, ha azoknak adatbázisai nem naprakészek és nem ismerik fel a legújabb kártékony programokat. A folyamatos frissítés tehát elengedhetetlen a biztonság szinten tartásához.

- Internet elérés szabályozása proxy szerver alkalmazásával

Használata a fentebb leírt előnyök miatt javasolt, növeli a biztonságot. Alkalmazásának kétféle megközelítése jellemző. A megengedőbb, a nemkívánatos weboldalak felsorolásával, a tiltóbb az engedélyezett oldalak deklarálásával biztosítja a működést.

- Jogosultságok alkalmazása, jelszavak kikényszerítése

A felhasználók megszemélyesítése account-ok alkalmazásával valósítható meg. Ahol lehetőség van rá, használni is kell, hisz elhagyásával a támadók dolga nagyban megkönnyíthető. Hasonlóan fontos a megfelelő bonyolultságú jelszavak kikényszerítése, illetve az alapértelmezett jelszavak megváltoztatása, mellyel nagyban megnehezíthető a támadási tevékenység. A felhasználói hozzáférések kialakításával, jogosultsági szintek beállítására nyílik lehetőség, mellyel meghatározható a rendszerben tárolt adatok (állományok, adatbázisok) illetékessége.

- Titkosított csatornák alkalmazása

Használatával megakadályozható, megnehezíthető az egyszerű lehallgatással, szaglászással történő információszerzés. Kiváló – ingyenes – titkosító eljárások állnak rendelkezésre, melyek alkalmazása bonyolítja a szolgáltatások konfigurációját, ugyanakkor nagyban növeli a biztonságot.

- Hálózati eszközök elzárása

A rendszerben működő hálózati elemek fizikai hozzáférésének megakadályozására zárható helyiségeket, szekrényeket kell használni, melyek képesek az illetéktelen személyeket a rendszertől távol tartani.

- Használaton kívüli végpontok inaktiválása

A támadók szeretnének csatlakozni a hálózathoz, ezért keresik az elhagyatott aktív hálózati végpontokat. A nyilvántartásokat folyamatosan aktualizálni kell, s a magára hagyott végpontokat pedig kötelező inaktiválni.

- Felhasználói fluktuációk követése

A munkáltatóknál bekövetkező fluktuációt kötelező az információ-technológia szintjén is követni, mellyel szavatolható, hogy - mindig - csak és kizárólag az aktív dolgozóknak legyen hozzáférésük a rendszerhez. A bosszúsan távozó munkatársak - aktívan hagyott belépési kódjukkal – kellemetlenséget okozhatnak.

- Hálózati információk elrejtése

Minden hálózatban léteznek olyan – a működést meghatározó – beállítások, adatok, melyeket eltitkolni ugyan nem lehet, de kerülendő velük hivalkodni. Egyrészt célszerű az IP címeket névfeloldással helyettesíteni, másrészt feltűnés nélkül használni a tűzfal,- átjáró,- proxy,- adatbázis-szerverek címeit.

- Szolgáltatások biztonságos beállítása

Manapság a szolgáltatások konfigurációs lehetőségei annyira sokrétűek, hogy az üzemeltetőnek gyakran döntenie kell az egyszerűbb használat,- nagyobb kockázat, vagy a bonyolultabb beállítás,- nagyobb biztonság mellett. Véleményünk szerint vállalni kell a nehézkesebb konfigurálást, de mindenképpen törekedni kell a biztonságos üzemeltetésre (pld. FTP szerver gyökér könyvtár meghatározása).

- Használaton kívüli szolgáltatások kikapcsolása

Ma egy operációs rendszer telepítése után, szerver és munkaállomás tekintetében egyaránt rengeteg használaton kívüli szolgáltatás működhet. Mivel minden hálózati szolgáltatás üzemeltetése biztonsági kockázat, a feleslegeseket ki kell kapcsolni, ezáltal erőforrás takarítható meg és csökkenthető a támadási felület.

- Adatbázis hozzáférések korlátozása

A féltve őrzött adatokhoz történő hozzáférés - szakszerű - beállítása alapkövetelmény. A hálózati porton figyelő adatbázis-kezelők (pld. Oracle, MySql) a megfelelő kliens programokkal megszólíthatók, csatlakozási kérések indíthatók. Alkalmazásuk esetén, amíg lehetséges kerülni kell a nyilvános hozzáférés beállítását, ha viszont elengedhetetlen, akkor jelszavakkal és lehetőleg titkosított csatornán keresztül kell az elérhetőséget biztosítani. Az adatbázis-kezelőkkel kapcsolatban az elérhetőség mellett létfontosságú a hozzáférési szintek alkalmazása, az elégséges jogosultságtól többet kiadni tilos. (Például lekérdezési tevékenységhez felesleges módosítási jogot adni az adatbázis-kezelőben.).

- Tűzfalak használata

A szolgáltatások túlterhelése (DOS, DDOS) elleni védelem, továbbá a hálózati kapcsolatok megfelelő mederben tartásának alapvető eszköze a tűzfal. Alkalmazása nélkül mind a hálózatok, mind a szerverek veszélynek vannak kitéve, ráadásul – lelkes fejlesztők százainak köszönhetően - alacsony költségvetéssel is kiváló tűzfalak építhetők.

- Mentések végrehajtása

Hálózatok üzemeltetésekor kötelező rendszeresen mentéseket végezni, melyekből nem várt események bekövetkezése esetén, visszaállíthatók az elveszett adatok. Az automatizált, rotációs rendszerű archiválások a legcélszerűbbek, a rendszeres visszaellenőrzések végrehajtása mellett. Az archívumokat célszerű a szerverszobától elkülönítetten, jól elzárható helyen tárolni.

- Rendszerállományok jogosultságainak ellenőrzése

A - szerverek operációs rendszerein fellelhető - rendszerállományok jogosultsági beállításai, megfelelő védelmet biztosítanak a véletlen, vagy szándékos károkozás, továbbá

az adminisztrátori jogok megszerzése ellen. A kielégítő állapot ellenőrzésére szkriptek, programok állnak rendelkezésre, melyek futtatásával meg lehet győződni az operációs rendszer sértetlenségéről.

- Jelszavak biztonságos tárolása

Az operációs rendszerek jelszavainak kezelése és tárolása biztonságosabb, ha azok, a felhasználói nevektől külön helyen, úgynevezett - különleges jogosultsági szinttel rendelkező - árnyék állományokban kerülnek elhelyezésre.

A mai modern kiszolgáló programokban lehetséges az adatbázis alapú azonosítás, amikor a felhasználók hozzáférési adatai táblákban és rekordokban helyezkednek el. Ezzel a megoldással operációs rendszer szinten nem keletkeznek hozzáférések, így a szolgáltatások lehallgatásával nem szerezhető közvetlen hozzáférés.

- Levelező szerver rendszerbeállítása

A hálózatok védelmében, kulcsfontosságú szerepe van az elektronikus levelek kezelésének. Az internet szolgáltató által biztosított SMTP[9] szerver és a munkaállomások levelező kliensei közé célszerű saját – vírusfigyelő és kéretlen levél ellenőrző funkcióval felruházott – levelezőszervert iktatni, mely hatékony védelmet biztosít, a levélben érkező kártevők ellen. A levelezőszerver tovább finomítható Webmail[10] alkalmazásával, mely rugalmassá teszi a levelek figyelését, csökkenti a hálózati adatforgalmat, és mellőzi a munkaállomások levelező klienseinek használatát.

Felhasználóknál, munkaállomásokon alkalmazandó védelmi intézkedések:

- Felhasználók oktatása

A felmérések szerint 90 %-ban a felhasználók jelentik a biztonsági kockázatot, ezért kötelező őket rendszeres oktatásban részesíteni. Tudniuk kell, hogy a jelszavakat miért kell bizalmasan kezelni, mit jelent a social engineering és mit jelent a hálózatok védelme.

- Szkript nyelvek tiltása

A munkaállomások támadása gyakran többletfunkciókat biztosító szkript nyelvek használatával valósul meg, melyek alkalmazása opcionális. A megfelelő arányú tiltások és engedélyezések beállításával, elviselhető mértékűre csökkenthető a kockázat.

- Munkaállomások lockolása

Tipikus felhasználói magatartás a használatban levő munkaállomás felügyelet nélkül hagyása, gyakran alkalmazói programok futtatása közben is. Ezeknek az eseteknek elkerülésére mindenképpen fel kell hívni a felhasználók figyelmét, továbbá bizonyos üresjárati idő eltelte után szerver oldalon kezdeményezni kell a kapcsolat megszakítást, vagy kliens oldalon a jelszavas képernyő-kímélő indítását.

- Interfészek tiltása

A felhasználók előszeretettel szeretnék munkahelyükre bevinni, s ott használni saját adathordozóikat (CD/DVD/pendrive), melyek akár kártékony programokat is tartalmazhatnak. A munkaállomások felesleges interfészeinek tiltásával, a veszélyes alkalmazások, programok bejutását, illetve érzékeny adatok kijutását lehet megakadályozni.

9 Simple Mail Transfer Protocol
10 Web alapú levelező program

- Indítási jelszavak alkalmazása

Amennyiben köztudott, hogy a hálózat munkaállomásaihoz – például takarítási céllal – külső személyek fizikailag hozzáférnek, érdemes BIOS felhasználói jelszót használni, mely képes megakadályozni a munkaállomás indítását.

- Korlátozott jogok alkalmazása a munkaállomásokon

Beállításával egyrészt megakadályozható, hogy a felhasználó programokat telepítsen, töröljön, vagy módosítson a munkaállomáson, másrészt szavatolható, hogy az alkalmazott hálózati, biztonsági és egyéb beállítások ne változzanak meg.

6. ELKÉPZELÉSEINK

Az előző alfejezetben kitértünk az egyéni megoldások alkalmazására, melyek a váratlanság, vagy az ismeretlenség erejével erősítik a hálózatok védelmét. A bemutatásra kerülő megoldások kifejlesztését a hétköznapi élet tette szükségessé.

Szolgáltatások leállítása, indítása

A távoli szervereken egyszerre megvalósítandó biztonságos üzemeltetés és a teljes körű adminisztrációs tevékenységek között ellentmondás húzódik. Több távoli webszervert is üzemeltetünk Debian GNU Linux operációs rendszerrel, alfanumerikus környezetben. A szervereken a HTTP(S), SMTP, FTP kiszolgálók végzik a szolgáltatási feladatokat, azonban az adminisztrációs tevékenységek miatt titkosított shell-t, azaz SSH kiszolgálót is működtetni kell.

Az SSH az operációs rendszer vezérlésének kulcsa, mert közvetlen bejelentkezési lehetőséget, azaz adminisztrációs tevékenységet biztosít. Aszimmetrikus kulcsú titkosítást használ, tehát kicsi az esélye, hogy lehallgatással megszerezzék a bejelentkezési azonosítót vagy jelszót, ugyanakkor „biztosítja” a próbálgatást, azaz a véletlen bejelentkezés lehetőségét, továbbá erőforrásokat von el.

A problémát tehát két ellentétes érdek okozzák:

- az operációs rendszer és a szolgáltatások normális működése esetén az SSH egy „kolonc”, mert biztonsági kockázatot jelent és viszi az erőforrásokat;
- bármilyen szolgáltatási, vagy operációs rendszer szintű probléma esetén az SSH az egyetlen megoldás a beavatkozásra, hiányában utazni kell a szerverhez.

Ennek az ellentétnek a feloldására kerestük a kielégítő megoldást, és arra a következtetésre jutottunk, hogy amennyiben az SSH-t valahogy ki-be lehetne kapcsolgatni, akkor „a kecske is jóllakna és a káposzta is megmaradna”, hisz leállítása esetén megszűnne a kapcsolódás lehetősége, és vele együtt a biztonsági kockázat, bekapcsolása esetén pedig ismét rendelkezésre állna, tehát végrehajtható lenne minden adminisztráció.

Egyértelművé vált, hogy a feladat csak az „állandó” szolgáltatásokon keresztül valósítható meg, amennyiben képesek az SSH indítására, vagy leállítására, ami azonban rendszeradminisztrátori (root) jogosultságokba ütközik, amivel egyetlen „állandó” szolgáltatás sem rendelkezik.

A tervünk egy böngészővel meghívható, webszerver által futtatandó program létrehozása volt, mely URL[11] paramétereken keresztül vizsgálja a jogosultságot és dönt az SSH indításáról, vagy leállításáról. Az adminisztrátori jogok szükségessége miatt a feladatot két részre bontottuk és

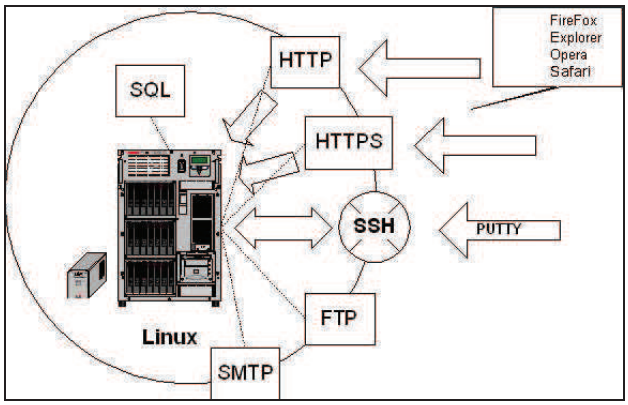
11 Uniform Resource Locator- Webcím

- Perl szkriptet (service.cgi) írtunk, amely - CGI-n keresztül - bináris programot képes futtatni webszerver segítségével;
- elkészítettük a parancssori argumentumokkal vezérelhető, SSH indítására, vagy leállítására alkalmas bináris programot (service.bin).

service.cgi	?	→	start/stop	service.bin
www-data	→	sudo	→	root

A sematikus ábrán követhető a szolgáltatás-vezérlés metodikája.

- Először „service.cgi" kerül meghívásra böngésző segítségével, melyet ténylegesen a webszerver futtatója, azaz „www-data" hajt végre;
- Az URL-ben átadott paramétereknek megfelelően döntés születik a szkript végrehajthatóságáról, valamint a végrehajtandó tevékenységről;
- Pozitív elbírálás esetén jogosultság átadás történik „sudo" segítségével, melynek eredményeként „www-data" felhasználó rendszergazdai jogosultsággal hajtja végre „service.bin" programot, a paraméterben átadott (start/stop) értékkel;
- Az SSH szolgáltatás az utasításnak megfelelően elindul, vagy leáll, melyről visszajelzés érkezik a böngészőben.



1. ábra: SSH vezérlése HTTP(S)-n keresztül
Forrás: Saját

A megoldással elértük célunkat, az SSH szolgáltatást feleslegesen nem működtetük, azonban ha szükség van rá, egyszerűen böngészőn keresztül elindítjuk. Egyedüli problémát a webszerverre irányuló kiszolgáltatottság jelenti, mert annak leállása esetén megszűnik az SSH indítási lehetősége. A bizonytalanságot a webszerver duplikált működtetésével oldottuk meg, külön üzemeltettük a HTTP és a HTTPS kiszolgálókat, így bármelyik kiesése esetén a másik még biztosítja az SSH indítását. A szolgáltatások egyszerre történő leállására kicsi az esély, amennyiben mégis bekövetkezne, akkor vélhetően komolyabb a probléma, a szerverhez fizikai hozzáférés szükséges.

Figyelő scriptek futtatása

A belső hálózatban működtetett Linux szerverek üzemeltetése közben, gyakran felmerült a kérdés bennünk, hogy miként lehetne reagálni egy - esetleges - illetéktelen bejelentkezésre? A költői kérdésre válaszul írtunk egy szkriptet, mely véleményünk szerint egy lehetséges megoldása a problémának. Abból a feltételezésből indultunk ki, hogy a szerverre a hálózaton

csak és kizárólag saját laptopról, vagy pedig a szerverszobában konzolról jelentkezek be, amiből egyenesen következik, hogy amennyiben bármely bejelentkezéshez tartozó IP cím nem a laptopé, akkor az illetéktelen jelenlétre utal.

Másik kiindulópontként két lépcsőssé tettük, azaz letiltottuk a – hálózati – direkt rendszeradminisztrátori bejelentkezést, tehát bárki csak és kizárólag normál felhasználóból válhat adminisztrátorrá. Miután a betörő is csak két lépésben lehet rendszergazda, amely jogosultság megszerzéséhez biztosan némi idő kell, egy rövid ellenőrzés – percenkénti automatizált – végrehajtásában gondolkoztunk.

A szkript algoritmikus működése:

- a rendszerbe bejelentkezett felhasználókhoz tartozó IP címek lekérdezése;
- az IP címek vizsgálata, hogy megegyezik-e a notebooké-val;
- eltérés esetén illegális bejelentkezés történt:
    a) azonnali beavatkozás, hálózati kapcsolatok zárása;
    b) naplóállomány készítése időbélyeggel és a lekérdezett IP címekkel.

A program rövid, alacsony az erőforrás igénye, a betörőnek pedig összesen egy perc áll rendelkezésére, hogy megpróbáljon „root” felhasználóvá válni. Egyik mit sem sejtő kollegánk egyszer megpróbált bejelentkezni, és „azonnal” a szkript áldozatává vált. Ez, és ehhez hasonló megoldások sikeresen alkalmazhatók Linux-ból épített tűzfalakon, routereken is, melyek véleményünk szerint nagyban növelik a védendő hálózat biztonságát.

ÖSSZEFOGLALÁS, KÖVETKEZTETÉSEK

A mai rohanó világban kulcsfontosságú szerepük van a kritikus információs infrastruktúráknak, melyek működése nélkül egyszerűen megállna az élet. Még belegondolni is borzongató mi lenne, ha a védelmi szféra, a bankok és egyéb intézmények informatikai rendszerei üzemképtelenné válnának, vagy a telefonszolgáltatók szerverei megállnának.

Az említett kritikus információs infrastruktúrák azonban mára teljes mértékben az Internet részévé váltak Az internetes elérésből pedig egyenesen következik a támadhatóság, a próbálkozás, valamint a kiberbűnözők felbukkanása. A háttérben megjelenő adat- és pénztömegek csábító hatása „szakértő-bűnözői” csoportok kialakulását és szervezett támadások összehangolását dimenzionálják. A hatékony védekezés szükségessége megkérdőjelezhetetlen, melyben az oktatásnak, az elfogulatlan tájékoztatásnak, valamint a védelmi szakértők alkalmazásának egyaránt nagy szerepe van.

FELHASZNÁLT IRODALOM

[1] Pulai András, Sziklássy Fábián, Tóth Péter, Udvaros H. Vilmos : Védd magad az Interneten – Kossuth Kiadó Rt., 1997

[2] Brian W. Kernighan - Dennis M. Ritchie : A C programozási nyelv, Budapest, Műszaki Kiadó, 1994

[3] László József : Dinamikus weboldalak, CGI programozás

[4] Négyesi Imre: CHANGING ROLE OF THE INTERNET IN THE LIGHT OF AN INTERNATIONAL CONFERENCE (Az internet szerepének változása egy nemzetközi értekezlet tükrében) (Hadmérnök on-line, III. évfolyam (2008) 3. szám, 147-153. oldal)

[5] Négyesi Imre: DIE VISION DER TRAGBAREN INFORMATIONS-TECHNOLOGIEGERÄTE (A viselhető számítástechnikai eszközök jövőképe) (Hadmérnök on-line, III. évfolyam (2008) 4. szám, 173-179. oldal)

[6] Négyesi Imre: Az információgyűjtés jövőképe (Hadtudományi szemle on-line, I. évfolyam (2008) 3. szám, 95-100. oldal)

[7] Négyesi Imre: A megfigyelés és információgyűjtés múltja, jelene és jövője (MK KBH Szakmai Szemle 2009. 3. szám, 35-50. oldal, ISSN 1785-1181)

[8] Négyesi Imre: Az önkormányzatok informatikai stratégiája és a Magyar Információs Társadalom Stratégia összefüggései (Hadtudományi szemle on-line, II. évfolyam (2009) 2. szám, 85-92. oldal HU ISSN 2060-0437)

[9] Négyesi Imre: Informatikai rendszerek és alkalmazások a védelmi szférában (DUF Konferencia előadás, 2010.03.05.-06.)

[10] Négyesi Imre: Informatikai rendszerek és alkalmazások a védelmi szférában (DUF Konferencia kiadvány, 2010.03.05.-06.)