HADMÉRNÖK

V. Évfolyam 1. szám - 2010. március

Előházi János
elohazi.janos@gmail.com

KERESKEDELMI INFORMATIKAI VÉDELMI MEGOLDÁSOK ÉRTÉKELÉSE ÉS ALKALMAZHATÓSÁGA A VÉDELMI SZFÉRA INFORMATIKAI RENDSZEREIN

Absztrakt

Ez az értekezés megvizsgálja a legsikeresebb adat- és informatikai védelmi eljárásokat az online kereskedelem és civil alkalmazások területén. Összefoglalja szemléletüket és sikerességüket, meghatározza miként alkalmazhatóak a védelmi rendszereken, mint például a rendőrségi-, polgári védelmi- és katonai alkalmazások. Megpróbálja kiragadni a kereskedelmi és védelmi rendszerek közötti különbségeket, és módot találni arra, hogy a már jól bevált kereskedelmi megoldások átültethetőek legyenek az ilyen speciális tulajdonságokkal bíró rendszerekre.

This article evaluates the most successful defence mechanism available for online systems in the commercial and civil world. Summarises their approaches and success and identifies the way how they can be applied in defence platforms such as police, civil defence and military use. It tries to grab the differences between the civil and defence platforms and adopt the already existing commercial solutions to this special field where extra aspects have to be considered.

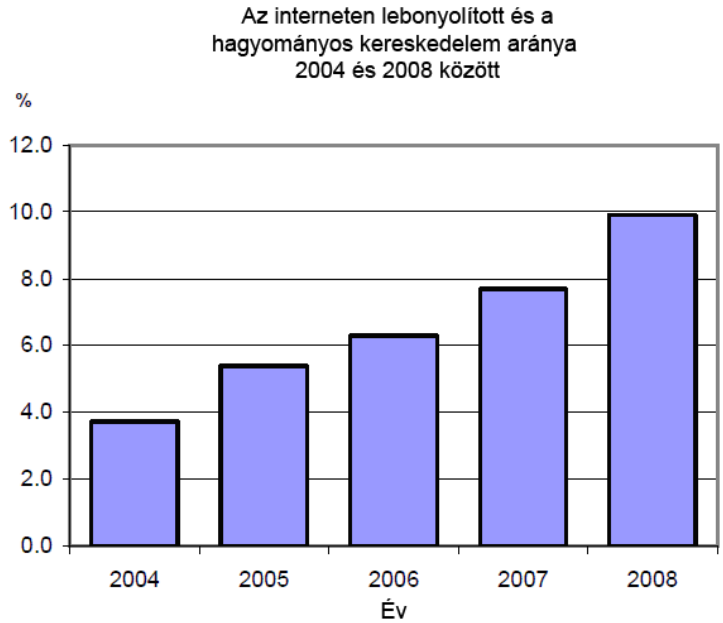
Kulcsszavak: *PCI compliance, adatvédelem, informatikai biztonság, biztonsági rendszerpolitika ~ PCI Compliance, data protection, information security, system security policy*

BEVEZETÉS

Az 1990-es évek második felére tehető első internetes fellendülés óta, kisebb nagyobb megtorpanásokkal az online kereskedelem folyamatosan bővül és évről évre nagyobb szeletet hasít ki az áru és szolgáltatások értékesítéséből. Az online rendszerek előnye, hogy határokon átívelő univerzális felületet biztosít a felhasználóknak, akik kényelmesen átböngészhetik az eladásra kínált árukat, szolgáltatásokat, összehasonlíthatják azok eladási árait, és a lehető legjobb ajánlatot kihasználva küldhetik el megrendeléseiket. Elmondható hogy ez az iparág, legalább 15-20 éves tapasztalattal rendelkezik, már túl van a gyerekbetegségein és rohamosan fejlődik. Ma már standardizált, de legalábbis széles körűen elfogadott megoldások léteznek az online kereskedelem és pénzforgalom minden részletére. Az internetes platform sérülékenységét ma már az átlag felhasználó is jól ismeri, és a nagyszámú tapasztalatnak megfelelően elmondható, hogy ennek ellenére biztonságos felületen működtethetőek ezek a rendszerek. Azonban napról napra újabb és újabb kihívásokkal kell szembenézni, és ahogy a támadó oldal újabb és újabb megoldásokat talál a védelemnek is tartania kell a lépést, hogy a biztonság fenntartható és folytonos legyen.

Az online értékesítési felületről elmondható, hogy a legolcsóbb és leghatékonyabb. Széles rétegeket ér el és hatalmas költségeket takaríthat meg az értékesítő számára. Ezért az iparág számára nagyon fontos, hogy a bizalmat ne veszítse el. Mivel ez a terület nem csak az értékesítők számára, de az online pénzügyi tranzakciókat lebonyolító szervezetek számára is hatalmas piac, ezért a biztonsági aspektus nagy figyelemnek örvend. Ennek köszönhetően ma már szabvány létezik arra, ami definiálja a biztonságos rendszer fogalmát, és egy listát ad az üzemeltető kezébe, aminek ha minden elemét ki tudja pipálni, bizton tudhatja, hogy rendszere biztonságos.

Ahogy az Egyesült Királyság Statisztikai Hivatalának alábbi ábráján is jól látható, 2004 és 2008 között, vagyis négy év alatt az online kereskedelem részesedése a teljes kereskedelmi forgalomból több mint megkétszereződött. Ez a tendencia a világ más területeire és igaz. Így belátható, hogy az online kereskedelem egyre fontosabb tényező. És mint fontos tényező, bevételeinek és működésének védelme egyre kiemeltebb figyelmet érdemel, hiszen bővülése vagy visszaesése a nemzeti bevételeket egyre növekvő mértékben befolyásolja.

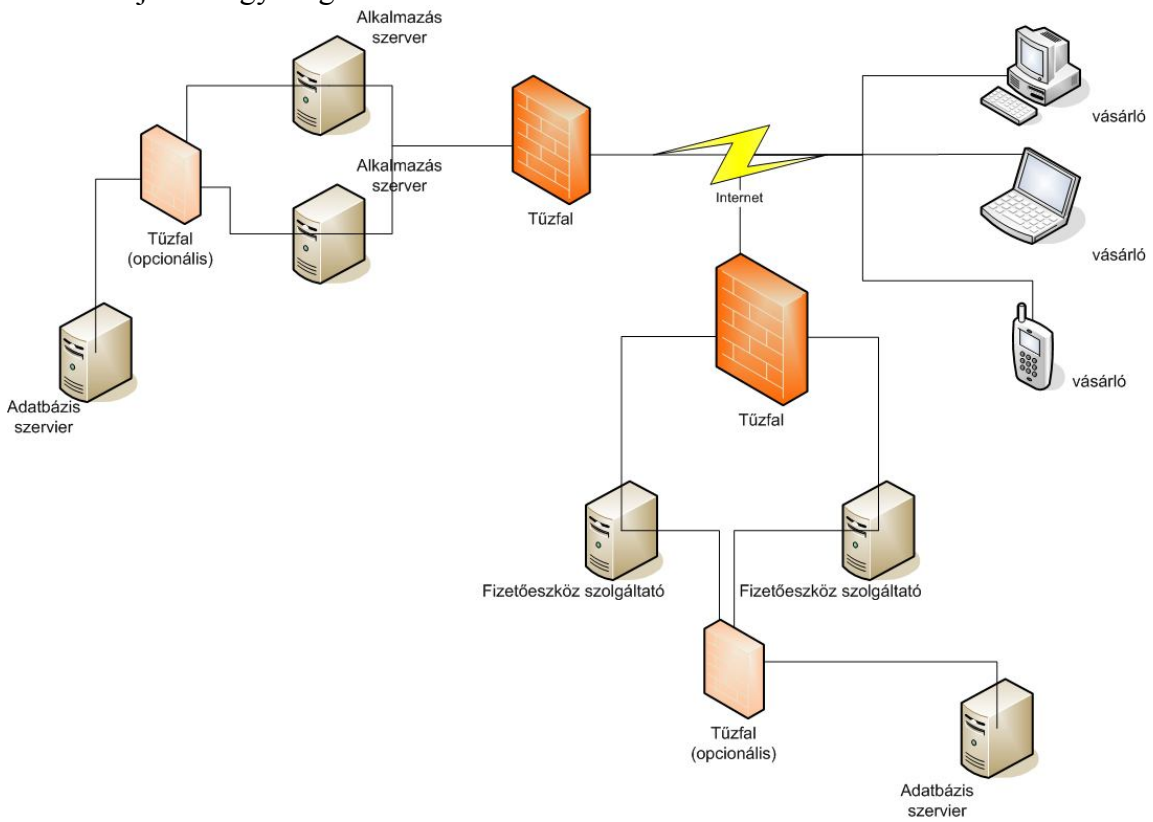


1. ábra. Az online kereskedelem részesedése az Egyesült Királyságban 2004-2008 között [1]

KERESKEDELMI RENDSZEREK SEMATIKUS ARCHITEKTÚRÁJA

Ahhoz hogy egy rendszer sebezhető felületeit azonosítani lehessen, ismerni kell annak szerkezeti felépítését, kapcsolatait saját és külső rendszerekkel, a fontos adatok tárolásának helyét és az azok továbbításához használt csatornákat és azok sajátosságait.

Az alábbi ábra mutatja, hogy a kereskedelmi rendszernek az Interneten keresztül kell csatlakoznia a fizetőeszköz szolgáltató rendszeréhez, ami pont ezeknek a lényeges adatoknak a továbbítását jelenti egy megbízhatatlan csatornán.



2. ábra. Egy tipikus e-commerce rendszer architektúrája (készítette a szerző)

Az e-commerce rendszerekben tárolt legkényesebb adatok általában a következők

- felhasználók azonosítására alkalmas adatok, mint a név, cím, e-mail cím, telefonszám stb.;
- hitel és betéti kártya adatok (kártyatípus, szám, ellenőrző kód, lejárati dátum);
- bankszámlaszám.

A kereskedelmi rendszerekhez szánt védelmi megoldások ezért a fent említett adatok védelmére fókuszálnak. Azok közül is a legfontosabbnak a fizetőeszközök védelmét tartják.

KERESKEDELMI RENDSZEREK VÉDELMI MEGOLDÁSAI

A kereskedelmi rendszerek védelmi megoldásai két sémát követhetnek:

- a fontos adatok megfelelő védelme az e-commerce rendszeren belül titkosított adattárolás és adatátvitel segítségével;
- a fontos adatok tárolásának mellőzése az e-commerce rendszerben, azokat a fizetőeszköz szolgáltató tárolja.

Titkosított adattárolás és adatátvitel

Ebben az esetben az adatok a kereskedő rendszerében vannak tárolva. Azok tárolása a rendszeren belül titkosítva történik. A titkosítás kulcsa megfelelően védett, a titkosítási algoritmus pedig megfelelően erős. Ha a behatolónak sikerül is bejutnia a kereskedelmi rendszerbe az ott talált adatokkal nem tud mit kezdeni, mert azok visszafejtése lineáris időn belül nem lehetséges, a kulcshoz pedig nem férhet hozzá.

Amennyiben szükség van az adatok továbbítására az megfelelően titkosított csatornán keresztül történik. SSL[1] vagy TLS[2] használatával.

Előnyök:

- egyszerű architektúra;
- az adatok egy helyen való tárolása;
- standardizált megoldások.

Hátrányok:

- a kereskedő felelős az adatok megfelelő módon való tárolásáért;
- a titkosításhoz használt kulcs védelme szintén a kereskedőt terheli.

Fizetőeszköz adatainak tárolása a fizetőeszköz-szolgáltatónál

Ebben az esetben, a hitel- és betéti kártya adatok illetve a bankszámla információk nem a kereskedő rendszerében kerülnek tárolásra, hanem a fizetőeszköz szolgáltatónál. Két elterjedt megoldást az alábbi két fejezet tartalmazza.

Előnyök:

- a felelősség áthárítása a szolgáltatóra;
- a szolgáltató már kiépített specializált rendszerrel bír, hiszen naponta nagy mennyiségű pénzügyi tranzakciót kezel.

Hátrányok:

- a felhasználó adatai több rendszerben kerülnek tárolásra.

Az alábbi két bekezdés tartalmazza a két legelterjedtebb megoldást az adatok a fizetőeszköz-szolgáltatónál való tárolására.

Future pay ID

A kereskedő visszakap egy egyedi azonosítót, ami a fizetőeszköz azonosítója a szolgáltatónál. Ezt felhasználva a kereskedő a jövőben is használhatja ugyanazt a fizetőeszközt anélkül, hogy annak bizalmas adatait a saját rendszerében kellene tárolnia. A future pay ID harmadik fél számára használhatatlan, mert csak az adott kereskedő számára használható fel. A felhasználó adja meg a fizetőeszköz felhasználási módját: rendszeres vagy pedig limitált. Első esetben a meghatározott intervallumban a kereskedő megterhelheti a felhasználót a megállapodott összeggel (előfizetéseknél való felhasználás), a második esetben a kereskedő egy nem rögzített intervallumonként, limitált vagy nem limitált összeghatárral megterhelheti a

[1] Az SSL (Secure Sockets Layer) 1, 2 és 3. verziója a Netscape által lett kifejlesztve. A 3. verzió 1996-ban. Un. best practice megoldás, de nem szabványosított. A felek azonosítása és az átvitel titkosításához szánt kulcsot nyilvános kulcson alapuló megoldásokat használnak. Az adatátvitel szimmetrikus kulcsú titkosítással történik.

[2] A TLS (Transport Layer Security) az SSL 3 továbbfejlesztése és szabványosított változata. Az első verzió szabványosítása 1999-ben történt meg. Az utolsó 1.2-es verzió 2008-ban került szabványosításra. A mechanizmus megegyezik az SSL megközelítésével, az alkalmazott titkosítási és kulcscsere algoritmusok kerültek átalakításra, hogy megfeleljenek a kor igényeinek.

felhasználót (ugyanabban a boltba több különböző alkalommal lebonyolított vásárlás) anélkül, hogy a felhasználónak újra és újra meg kelljen adnia a fizetőeszköz adatokat. A future pay ID a WorldPay szolgáltató terméke. [3]

Adatok közvetlen megadása a fizetőeszköz szolgáltató rendszerében

Ebben az esetben a kereskedő csak egy visszajelzést kap, hogy a számla kiegyenlítése rendben megtörtént-e. Pozitív válasz esetén megkezdheti a rendelés szállítását, amíg negatív válasz esetén értesítheti a felhasználót, hogy egy másik fizetési módot próbáljon meg, vagy ellenőrizze, hogy az adatait rendben megadta-e.

Ez a módszer Magyarországon is elterjedt. Sok online kereskedő a bankok által üzemeltetett felületre küldi tovább a felhasználókat, ahol megadhatják a kártya vagy bankszámlaszám adataikat. Az űrlapok kitöltése mindig titkosított csatornán keresztül történik. A hazai bankok szinte mindegyike rendelkezik ilyen szolgáltatással. Hátránya, hogy minden egyes alkalomkor meg kell adni a fizetőeszköz adatait a banknak, illetve hogy a felhasználó a tranzakciókat csakis a banki kivonaton követheti nyomon.

Léteznek bankoktól független fizetési szolgáltatók, melyek közül a legnagyobb a PayPal (www.paypal.com). Itt az egyes felhasználók létrehozhatják saját profiljukat, regisztrálhatják a különféle bankkártyáikat és bankszámláikat. Egy online tranzakció lebonyolítása során, a felhasználókat a kereskedő a PayPal oldalára irányítja át, ahol a felhasználható kiegyenlítheti a számláját. A fizetőeszköz információi ebben az esetben sem kerülnek a kereskedő birtokába, csupán a tranzakció sikerességéről kap visszajelzést. A felhasználó a profilján tudja nyomon követni a saját tranzakcióit.

KERESKEDELMI RENDSZEREK HITELESÍTÉSE A PCI SZABVÁNY ALAPJÁN

A kereskedelmi rendszerekben tárolt kényes adatok jól definiáltak. Ennek ellenére egy ilyen rendszerben is számos veszélyforrás lappang, amelyek ellen komplex védelmi megoldások képesek csak megfelelő védelmet nyújtani.

A 2004-ben elfogadott PCI [3]szabvány, és a 2006-ban illetve 2008-ban elfogadott újabb verziók egy komplex forgatókönyvet nyújtanak a kereskedők számára, hogy rendszerüket megfelelően biztonságossá tegyék. A szabvány a hálózat összes lehetséges eleméhez kínál mind technológiai mind pedig menedzsmentbeli megoldásokat. Az előírások követésével és betartásával a kereskedő biztos lehet abban, hogy rendszere megfelelően védett, és a tárolt adatok biztonságban vannak. A PCI szabványnak való megfelelőséget PCI auditorok vizsgálják meg, és minden évben ellenőrzik az adott rendszert, hogy biztosítsák a folytonos megfelelőséget.

A PCI szabvány a következő területekre terjed ki [4]:

- biztonságos hálózat kiépítése és fenntartása:
    - megfelelő tűzfalrendszer;
    - hálózati eszközök alapértelmezett adminisztrációs jelszavainak megváltoztatása.
- adatvédelem:
    - tárolt adatok védelme;
    - titkosított adattovábbítás.
- sebezhetőség elleni védelem:
    - antivírus termékek alkalmazása és frissen tartása;

[3] A PCI betűszó a Payment Card Industry Data Security Standard a gyakorlatban elterjedt és használt rövidítése.

    - biztonságos alrendszerek és alkalmazások használata.
- hozzáférés szabályozás:
    - bankkártya adatokhoz való hozzáférés szigorú szabályozása, csak azok férhessenek hozzá, akiknek erre az üzletmenet szempontjából szüksége van;
    - egyedi azonosítók használata;
    - védett adatokhoz való fizikai hozzáférés megakadályozása (adatbázis vagy adathordozó szintű titkosítás).
- rendszerek monitorozása és tesztelése:
    - minden hozzáférés naplózása;
    - rendszeres ellenőrzések.
- információbiztonsági szabályzat elfogadása és betartása a szervezeten belül.

VÉDELMI CÉLÚ HÁLÓZATOK SAJÁTOSSÁGAI

A védelmi hálózatokon tárolt adatok sokkal szélesebb körű forrásokkal rendelkeznek. Az itt tárolt védendő információk számos különféle formában találhatóak meg:

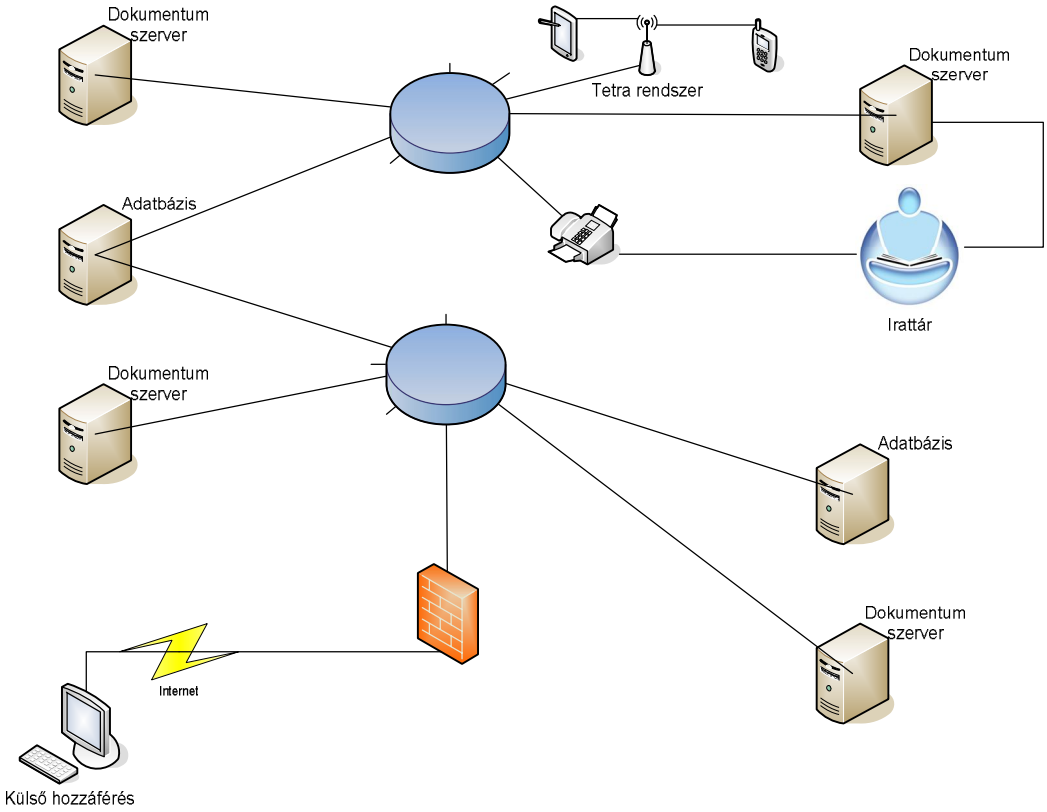
- helyzetismereti alkalmazások:
    - a helyzetre vonatkozó információk tárolása, elemzése különböző aspektusok mentén (katasztrófa elhárítás, békefenntartó- és háborús műveletek stb.);
    - tárolt adatok vizualizációja;
    - térinformatikai módszerek;
- számvetések, előrejelzések:
    - mérlegelésre, megítélésre számítások eredményeként kialakított számszerű információk tárolása, azokon matematikai és logikai műveletek elvégzése;
    - jövőbeni folyamatok és állapotok meghatározása, előrejelzése;
    - rendeltetése állandó szervezetek és ideiglenes hadműveleti elemek feladat-végrehajtási képességeire vonatkozó jellemzők meghatározása;
    - adott feladat végrehajtására kialakított cselekvési változatokhoz rendelkezésre álló erők és eszközök elosztása;
    - manőverszámvetések;
    - erőforrás-felhasználás és veszteség-számvetések;
- csoportmunka alkalmazások:
    - csoportmunka informatikai támogatása;
    - virtuális környezetek;
- szimulációs alkalmazások:
    - valóság objektumainak, jelenségeinek, folyamatainak, rendszereinek hasonlóságán alapuló modellezése;
    - szimulációs műveletek;
- civil műveleti adatok:
    - civil szervezetek rendszeréhez hasonló eszköz- és bérnyilvántartás stb.[6]

Ezek az információk ráadásul ellentétben a kereskedelmi rendszerekkel, különböző szervereken, vagy szerver csoportokon helyezkednek el, melyek egymástól független vagy lazán csatolt hálózatokon találhatóak meg.

Az alábbi ábra próbálja meg szemléltetni a védelmi hálózatok bonyolult és heterogén felépítését. A védelmi hálózatokért felelős szabályrendszer és technológia ezért a különböző, más-más felügyelet alá tartozó hálózatok közös védelmi menedzsmentjét igényli. A szervezetek között összehangolt és fegyelmezett együttműködésre van szükség.

A védelem fogalma szintén bővebb, hiszen nem csak a külső illetéktelen behatolókkal szemben kell megvédeni a rendszert, de a rendszeren belüli különböző szintű hozzáféréseket is biztosítani kell. A kialakított szabályrendszernek pedig elég rugalmasnak kell lennie ahhoz,

hogy minden féle formátumú és forrású (nyomtatott vagy digitális stb.) adatra alkalmazható legyen.



3. ábra. Példa védelmi hálózatok architektúrájára (készítette a szerző)

KERESKEDELMI VÉDELMI MEGOLDÁSOK ALKALMAZHATÓSÁGA VÉDELMI CÉLÚ RENDSZEREKBEN

A PCI szabványról elmondható, hogy a gyakorlatban bizonyított forgatókönyvet ad az üzemeltetők kezébe, aminek segítségével feltérképezhetik védendő adataikat és a rendszerük gyenge, védendő pontjait. Bár a szabályokat a banki adatok védelmére dolgozták ki, azok átalakíthatóak és kibővíthetőek olyan módon, hogy bármilyen védendő információs rendszerre alkalmazhatóak legyenek.

A szabályrendszert tovább kell alakítani a szerint is, hogy egy adott alrendszernek milyen kapcsolatai vannak a védelmi rendszer más szegmensei felé, és azok milyen adatokhoz jogosultak hozzáférni. Az informatikai biztonság szabályrendszerének megalkotása során „társ" hálózatokat is bizalmatlanul kell kezelni az adatok maximális védelme érdekében.

Biztonságos hálózat kiépítése és fenntartása

Az adott hálózat összetartozó elektronikus és nem elektronikus elemeit össze kell gyűjteni, egymáshoz való kapcsolódásukat és a közöttük lévő hierarchiát dokumentálni kell, az átláthatóság és megérthetőség eléréséért.

A PCI szabvány [5] 1. pontjában leírt feladatok a következő módon ültethetőek át a védelmi rendszereken:

- A hálózat más hálózatokkal és publikus rendszerekkel való kapcsolódási pontjait azonosítani kell. A kapcsolódási pontokon lévő tűzfalak, routerek és egyéb hálózati elemek konfigurációjával szemben támasztott követelményeket össze kell írni. A hálózati elemek bármilyen konfigurációs változtatását jóváhagyó procedúrát definiálni

kell. A folyamat betartását biztosító szabályzatokat meg kell írni és a személyzettel megismertetni.

- A hálózat belső és külső (más hálózatból érkező) felhasználóit azonosítani kell, felelősségüket és jogaikat definiálni kell, az egyszerűbb adminisztrációért az azonos jogokkal és felelősségekkel rendelkező felhasználókat csoportokba kell szervezni. Meg kell különböztetni a publikus, hálózatközi és hálózaton belüli felhasználói csoportokat.
- A hálózat minden szolgáltatását és általuk használt kommunikációs csatornákat azonosítani kell, az általuk elvégzett feladatokat össze kell írni.
- A hálózaton tárolt minden formátumú védendő adatot azonosítani kell, a szolgáltatásokat melyek ezekhez az adatokhoz bármilyen módon hozzáférhetnek, össze kell írni és az információkhoz rendelni. Az adatokat és szolgáltatásokat megfelelő módon minősíteni kell.
- A hálózatok egymás közti, belső és külső kommunikációját a fent meghatározott szolgáltatásokra kell korlátozni. A hálózat bármilyen egyéb kommunikációban nem vehet részt.
- A hálózatok közötti szinkronizáció illetve rendszeres biztonsági másolatok készítését, telepítési és fenntartási feladatokat elvégző folyamatokat át kell alakítani, hogy a biztonsági követelményeknek megfeleljenek. Termékeiket, mint pl.: biztonsági másolatot tartalmazó adathordozók szintén be kell vonni a szabályzat hatásköre alá.
- A hálózatok közötti kommunikációt megfelelő módon titkosítani kell.
- A minősített adatokat tároló és azokhoz hozzáférő komponensekhez való hozzáférést szabályozni kell.
- Alapértelmezett jelszavakat és felhasználói fiókokat törölni illetve megváltoztatni kell. A rendszerben feleslegessé vált felhasználói hozzáféréseket azonnal meg kell szüntetni.
- Az olyan hozzáféréseket melyekre a szabályzat szerint nincsen szükség azonnal meg kell szüntetni, így minden egyes felhasználó csak a számára megengedett adatokhoz és szolgáltatásokhoz fér hozzá.
- A felhasználói fiókokat megfelelően kell védeni, a védett adat minősítésének megfelelő azonosítási procedúrákat kell érvényesíteni.
- A hálózat komponenseihez való távoli hozzáférést megfelelő módon titkosítani kel.
- Kerülni kell a megosztott szolgáltatásokat a rendszerben.
- A kommunikációs csatornákat irányuk és szerepük szerint osztályozni kell, a rajtuk lebonyolítható szolgáltatásokat és adathozzáféréseket differenciálni kell. A differenciálást adat szinten kell elvégezni (egy információ tartalmazhat részadatokat, melyek elérhetőek a „társ”-hálózatokon keresztül, de pl. publikus hálózaton keresztül nem, stb.)

Adatvédelem

A PCI szabályrendszer adatvédelmi ajánlásai közül a legalapvetőbb, miszerint a tárolt kényes információk mennyiségét korlátozni kell, a védelmi hálózatokban nem minden esetben kivitelezhető. Emiatt az információk védelmében a legszigorúbb módon meg kell előzni az illetéktelen hozzáférést és a biztonságos adatkommunikációt:

- A hozzáférést biztosító azonosító információkat biztonságosan kell tárolni, azok kiszivárgását, illetéktelen hozzáférést, az azonosítás megkerülésével vagy kijátszásával meg kell előzni.
- A rendszer szintű (operációs rendszer, hálózati belépés stb.) azonosítási mechanizmusoktól független felhasználó azonosítási módszer bevezetésére van

szükség, ami a felhasználó azonosító adatait megfelelően titkosítva, illetéktelen számára használhatatlanul és módosíthatatlanul tárolja.

- Azokat az információkat, melyekre már nincsen szükség a lehető leghamarabb meg kell semmisíteni. Az ilyen információk gyors és alapos kiszűrésére szolgáló mechanizmusokat kell bevezetni. Az ilyen információkról készült mindenféle (biztonsági) másolatot az információ érvényességének lejártával egyidejűleg kell megsemmisíteni. Ha az információ más társrendszerekbe is át lett másolva, az ottani megszüntetésükről is gondoskodni kell.
- A titkosítási algoritmusokban használt kulcsokat megfelelően kell védeni és rendszeres időközönként cserélni. Minden kulcs-menedzsment folyamatot jól dokumentálni kell az átláthatóság érdekében.
- Elektronikus adatátvitel során a lehető legerősebb titkosítási és azonosítási algoritmusokat kell alkalmazni (TLS, IPSEC[4]). A kompromittálódott titkosítási és biztonságos hash függvény stb. eljárások használatát azonnal eliminálni kell a rendszerből.
- A zárt hálózatok zártságában nem szabad megbízni. Hálózaton belüli adatátvitelt is megfelelő módon kell titkosítani, és a másik felet szigorúan azonosítani kell.
- Az információhoz való hozzáférést naplózni kell minden szinten a reprodukálhatóság érdekében.

Rendszervédelem

A rendszer bármely hardver és szoftver elemének lehetnek gyenge pontjai, melyekről azok piacra kerülésekor a gyártó nem tudott, vagy nem volt képes kijavítani. Az ilyen hibákat a gyártók rendszeres frissítések folyamán orvosolják. A rendszer minden hardverelemén futó alacsony szintű szoftverhez szükséges a frissítések minél hamarabbi telepítése. Ilyen alacsonyrendű szoftverek például az operációs rendszerek, adatbázis- és egyé dokumentumkezelő rendszerek, web-szerver alkalmazások, a hálózati elemeken (router, switch, VPN [5]stb.) futó rendszerszoftverek (un. firmware). Ezen szoftverek nyilvántartása, a hozzájuk kibocsátott frissítések folyamatos követése és telepítése tehát elengedhetetlen, hogy az alapvető szoftver elemek ellenálljanak a támadásoknak.

A frissítések rendszeres telepítése mellett egyéb kiegészítő rendelkezések is szükségesek a rendszer védelme érdekében. Főleg a Microsoft alapú rendszerekre jellemző a vírusfenyegetettség. Ezért mindenhol, ahol a körülmények megkövetelik antivírus programokat is alkalmazni kell. Az azokhoz kiadott vírusadatbázist naprakészen kell tartani.

A Linux/Unix alapú (így a Macintosh) rendszerek az un. rootkit[6]-ek ellen védtelenek. A rootkit programok elleni védelem hasonlít a vírusok elleni védekezésre. A kereső programok heurisztikus algoritmusokkal az ismert rootkitek szignatúráját keresik a fájlokban (hasonlóan, ahogy az antivírus programok teszik ezt a vírusok keresésekor). Mivel ezek a programok a rendszerfájlokat támadják meg, eltávolításuk lehetetlen, bonyolult vagy túl sok időt vesz igénybe. A legtöbb esetben az operációs rendszer újrainstallálását javasolják. A gyártók rendszeresen adnak ki frissítéseket, melyekkel az operációs rendszer védetté tehető a különböző rootkit támadások ellen.

[4] Internet Protocol Security: Alacsony (protokoll) szintű védelem és azonosító eljárás az IP csomagokban továbbított adatfolyam védelmére.

[5] Virtual Private Network: publikus hálózaton keresztüli magánhálózat, a felhasználó megfelelő azonosítás után titkosított csatornán éri el a kívánt zárt hálózatot.

[6] A rootkit egy szoftver ami egy vagy több programból állhat. A már fertőzött számítógépen lehetővé teszi, hogy a támadó hozzáférjen a rendszerhez, annak rendszergazda szintű hozzáférést adva. Ezáltal lehetősége nyílik a támadónak arra, hogy rendszerprogramokat módosítson, hogy azok a saját céljainak megfelelően működjenek.

Változtatások a rendszerben

Egy rendszerben, ami már megfelel az elvárásoknak, véghezvitt minden módosítás jól indokolt és dokumentált kell, hogy legyen. Minden változtatást, mielőtt az az éles környezetben telepítésre kerülne, alaposan le kell tesztelni, hogy a változtatás telepítése után is megfelel-e a rendszer a követelményeknek. Erre a célra egy tesztkörnyezetet kell létrehozni, ami teljesen szeparált az éles környezettől. A sikeres tesztelés után, a teszthozzáférések törlése mellett alkalmazható a változtatás az éles rendszeren.

Emellett a változtatásoknak jól dokumentáltnak kell lenniük. A dokumentációnak tartalmaznia kell a változtatás telepítésével járó változásokat, azok céljait, a tesztelés folyamatát, a szükséges visszaállítási lépéseket, ha valamilyen probléma merülne fel. A megfelelő hatáskörrel rendelkező személyek írásos hozzájárulása is szükséges a rendszerben való módosítások elvégzéséhez.

A rendszert minden változtatás során tesztelni kell:

- külső és belső sebezhetőségi pontok alapján;
- külső és belső behatolás-védelem szempontjából.

Hozzáférés szabályozás

A rendszerhez annak felületén kívül alacsony szinten is hozzá lehet férni. Ide sorolandó a hálózati elemek rendszergazda szintű felhasználói, az adatbázis-kezelő rendszerek felhasználói, és az egyéb nyilvántartó rendszerek rendszerszintű felhasználói. Az ilyen hozzáféréseket korlátozni kell, hogy csak a szükséges személyzet érhesse el a rendszert ilyen módon. Minden hozzáférésnek egyedinek – egy emberhez köthetőnek – kell lennie. A felesleges felhasználói fiókokat azonnal meg kell szüntetni. A hozzáférési azonosítókat és jelszavakat olyan módon kell megválasztani, hogy azok szótár alapú támadással ne lehessenek megfejthetőek. A jelszavak cseréjéről megfelelő időközönként gondoskodni kell.

A rendszer elemeihez való fizikai hozzáférésnek szintén jól szabályozottnak kell lennie. A hardver elemek (legfőképpen az adathordozók) titkosítása is szükséges lehet, hogy az azok eltulajdonítása ellen védekezzünk.

Mindenféle elektronikus, papír és egyéb alapú másolatok az üzemelő rendszertől elkülönítve kell legyenek tárolva. A hozzáférésüket ugyanolyan szigorúan kell szabályozni, mint az üzemi környezetét.

Monitoring

A rendszerben tárolt minden kényes információhoz való hozzáférést fel kell jegyezni. A feljegyzéseket védeni kell az illetéktelen hozzáféréstől, és olyan módon kell őket tárolni, hogy ne lehessen őket módosítani.

A megfigyelendő eseményeket a PCI szabvány írja le [5]:

- védendő információhoz és szolgáltatáshoz való hozzáférés;
- a felhasználók minden akciója a rendszeren belül;
- a monitor-feljegyzésekhez való hozzáférés;
- azonosítási funkciók használata;
- rendszerinicializálás;
- rendszer komponensek létrehozása, módosítása és inicializálása.

A fenti adatokat rögzítő feljegyzéseket rendszeres időközönként át kell nézni, és minden illetéktelen vagy gyanús esetet ki kell vizsgálni.

ÖSSZEGZÉS

Látható, hogy a civil szférában már bevált védelmi megoldások a védelmi rendszerekre is adoptálhatóak. Egy olyan megoldás, mint a PCI egy kereskedelmi rendszerben is többlet adminisztrációt igényel, és egy védelmi rendszerben, annak sajátosságai miatt még nagyobb ez az adminisztrációs többlet. Azonban az erőfeszítéseknek köszönhetően, a védelmi rendszerek biztonsága egy magasabb szintre emelhető, ezáltal a nemzetgazdaság számára létfontosságú elemek maximális biztonságban üzemeltethetőek.

A fent leírt eset sajnos egy az egyben nem ültethető át a műveleti területeken alkalmazott speciális, főként vezeték nélküli kommunikációt és korlátozott erőforrásokat használó információs rendszerekre. Ebben az esetben a használhatóság és a biztonság egészséges kompromisszumát kell megalkotni. Az infrastruktúra megbízhatatlansága és pehelysúlya miatt a kereskedelmi életben elterjedt védelmi megoldások egyáltalán nem, részben vagy erősen módosítva alkalmazhatóak csak.

Felhasznált irodalom

[1] http://www.statistics.gov.uk/pdfdir/ecom1109.pdf E-commerce and information and communication technology (ICT) activity, 2008 [Egy. Kir. Nemzeti Statisztikai hivatal 2009.11.29.]

[2] http://en.wikipedia.org/wiki/Transport_Layer_Security Transport Layer Security [2009.12.06.]

[3] http://www.rbsworldpay.com/shopper/kb/shoppermanagementsystem/sms1200.html Recurring Payment (FuturePay) Agreements [2009.12.06.]

[4] http://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard Payment Card Industry Data Security Standard [2009.12.06.]

[5] https://www.pcisecuritystandards.org/security_standards/download.html?id=pci_dss_v1-2.pdf PCI DSS Requirements and Security Assessment Procedures, v1.2.1, 2009 [2009.08.14.]

[6] Munk Sándor: KATONAI INFORMATIKA II. Katonai informatikai rendszerek, alkalmazások, Egyetemi Jegyzet, ZMNE 2006