Üzletmenet biztonsága az Interneten

VENESZ BÉLA
Széchenyi István Egyetem Informatikai és Villamosmérnöki Intézet
venesz@free-mail.hu

Konzulens: dr. Raffai Mária

ABSTRACT

The aim of the article is to show a special IT security technique that is not mentioned in neither Hungarian nor foreign manufacturer-independent literature. One of the reasons might be that it is very new and immature. Mellowness can appear only in the opinions of experts, so the technique, mentioned in the article, will play important role especially in the security-policy of banks, corporations specialized in finance, governments and R&D companies. So it is worth to learn other techniques apart from the currently applied firewall and antivirus software.

A cikk egy olyan technikát mutat be, amelyet jelenleg még kevés IT-biztonsággal foglalkozó, gyártófüggetlen szakirodalom tárgyal. Ennek egyik oka talán abban található, hogy egy új, és kiforratlan technikáról van szó. Bár a biztonsággal foglalkozó szakemberek látják ennek a megoldásnak az előnyeit, és érzik az alkalmazás szükségességét, de várható, hogy a közeljövőben elsősorban bankok, pénzintézetek, K+F tevékenységet folytató cégek, illetve kormányzatok informatikai biztonságpolitikájában is komoly szerepet fog betölteni. Érdemes tehát a jelenleg alkalmazott tűzfalak és víruskereső szoftverek mellett ezt az új technikát is megismerni.

Változások az IT területén

Az utóbbi 15 évben meglehetősen nagy változás történt, az egymástól elszigetelt munkahelyek a számítógéphálózatok és az Internet által összeköthetővé váltak, lehetővé téve ezzel a közvetlen kommunikációt és a csoportmunkát. Az Internet általános elérhetősége és használatának korlátlan lehetősége a legtöbb kereskedelemi vagy banki-pénzügyi tevékenységet folytató cég számára az alkalmazás/használat elengedhetetlen kényszerűségével jár, de komoly problémát jelent, hogy erős, lényegbeli eltérés figyelhető meg az infrastruktúra[6] és a kínált szolgáltatások között. Külön gondot okoz, hogy az Interneten elérhető szoftverek, utility-k gyorsan és különösebb nehézség nélkül tölthetők le. A letöltés alatt álló szoftverek telepítésekor vagy később a használat során egy olyan számítógépes környezet jön létre, amely fogékony a kívülről indított támadások (a használt közeg többnyire az Internet) iránt, és kevés védelmet nyújt a nemkívánatos tevékenységek, vagy akár a belső munkatársak ellen (márpedig ez utóbbiak jelentik a visszaélések csaknem 80%-át). A fenti folyamat egyre veszélyesebbé váló támadási formákat eredményez.

A crackerek egyre növekvő száma mellett az informatikai rendszerek ellen indított támadások is mind eredményesebbé válnak. A crackerek nemcsak a kereskedelmi alkalmazásokat, a PC-ket vagy a Java-megoldásokat támadják, hanem nyilvánosságra hozzák a támadható rendszerek gyengeségeit is, illetve az információkat jól szervezett Usenet és Mailing listákon, valamint különböző site-okon osztják meg. Egyre növekvő

[6] Ez esetben a TCP/IP v4 protokoll alapú hálózatra gondolok, amelyet a biztonsági aspektusok figyelembe vétele nélkül fejlesztettek ki.

növekvő exponenciális trend tapasztalható azoknak a szoftvereknek a terjedésében, amelyek a támadásokat automatikusan hajtják végre, így kevésbé tapasztalt crackerek is néhány perc alatt képesek olyan programokat, scripteket letölteni, amelyek támadási eszközként használhatók fel.

Azon vállalatoknál (többnyire bankok és K+F tevékenységet folytató cégek, kormányzatok), ahol a munkafolyamatok IT- és időérzékenyek (szoftverérzékeny rendszerek), ahol egy, a biztonságot veszélyeztető esemény hatása komoly károkkal járhat (például anyagi veszteség, jó hír elvesztése, hitelesség elvesztése, kínos helyzet fellépése, bizalmas, illetve stratégiai információk kiszűrődése, működési képesség elvesztése, a törvény megszegése stb.), ott jogosan merül fel a kérdés, hogy vannak-e a hagyományos védekezési mechanizmusok (víruskeresés, tűzfal) mellett a káros behatások elleni hatékony megoldások.

Védelmi megoldások

A védekezést alapvetően két különböző szinten lehet megvalósítani [4]:

- Egyrészt a *víruskereső programok* segítségével, amelynek feladata, hogy ellenőrizze az éppen végrehajtásra előkészített állomány integritását, azaz az adott állomány eredeti állapotában van-e, és nem került bele olyan végrehajtható rész, amely a víruskereső adatbázisa szerint vírusra utaló jeleket tartalmaz. A tapasztalatok szerint a támadásoknak ezzel csak egy része detektálható, és az is csak utólag, amikor az ellenőrzést végrehajtjuk. Azokat a támadásokat viszont, amelyek nem sértik az állományok integritását (például azok amelyek a jogosultsági rendszert módosítják) ezzel a módszerrel nem lehet kiszűrni.
- A *tűzfalak* csak bizonyos kapcsolatfajták szűrésére alkalmasak, ugyanakkor az általuk engedélyezett forgalmat nem tudják további vizsgálatnak alávetni. A fentiek alapján a hiányzó láncszem a betörésdetektáló eszközök (IDS: Intrusion Detection System) alkalmazása, amelyeknek célja, hogy felismerje a bizalmasság és/vagy rendelkezésre állás és/vagy az integritás megsértésére irányuló próbálkozásokat, azokat jelentse a biztonságért felelős személynek, illetve a megfelelő ellenintézkedéseket végző komponensnek (IRS: Intrusion Response System).

A következőkben ez utóbbi megoldást mutatom be.

Az IDS architektúra és működés

Az IDS-rendszert alapvetően négy összetevő alkotja:

- adatgyűjtő komponens (hálózati vagy hoszt alapú)
- adatbank-komponens
- menedzsmentállomás
- kiértékelő komponens (analizátor)

Adatgyűjtő komponens

Az adatgyűjtő komponens (továbbiakban szenzor) általános, kvantitatív jellegű információkat gyűjt a rendszer állapotáról. Mivel ezek az adatok nem számszerűsíthetők, ezért nagyon nehéz feladat a megfelelőket összegyűjteni. A kiértékelési folyamatot ugyanis nemcsak a túlzottan sok naplózott adatmennyiség nehezíti meg, hanem a szükségesnél kevesebb is. A legjobb kiértékelő komponens is hatástalan, ha nem áll rendelkezésre elegendő és megfelelő mennyiségű adat. A releváns auditadatok forrásai a támadás detektálási helyétől függően alapvetően kétfélék lehetnek.

A *hálózat alapú* (network based) adatgyűjtő szenzor feladata, hogy összegyűjtse és a kiértékelő komponens segítségével ellenőrizze az adott számítógép vagy egy hálózati szegmens forgalmi adatait. A gyakorlatban minden szenzorhoz egy dedikált, komoly erőforrásokkal rendelkező számítógépet kell alkalmazni, miközben biztosítani kell azt, hogy működése más alkalmazásokat ne zavarjon. Ha szegmensenként egy szenzort alkalmaznánk, akkor a mai hálózatokban, ahol egy szegmensben csak egy hoszt helyezkedik el, nagyon megdrágulna az eszköz alkalmazása.

A megoldás alkalmazása előnyökkel és hátrányokkal jár.

Előnyök:

- A hálózaton elhelyezett szenzor a szerver és munkaállomás erőforrásait nem használja.
- A támadás már akkor detektálható, mielőtt az elérné célját, így az IRS révén megfelelő időben való automatikus beavatkozásra van lehetőség.
- A szenzorok úgy konfigurálhatók, hogy azok észrevehetetlenek maradnak a támadó részéről, IP-cím híján pedig címezni sem tudja őket.

Hátrányok:

- Sok, ma rendelkezésre álló szenzor nem képes nagysebességű hálózatok (100 Mbps) esetén az adatforgalmat kielégítően átvizsgálni.
- Osztott rendszerek vagy redundáns kihelyezett hálózat esetén a szenzor csak egy szegmens (illetve hoszt) forgalmát látja.
- A titkosított adatforgalmat (például SSL, IPsec használata esetén) nem tudja ellenőrzés alá vetni.
- Korlátozottan képes az észrevett támadás céljának meghatározására.
- A támadás felismerése nem egzakt és nem hibátlan.

A *hoszt alapú* (hoszt based) szenzor a védendő hoszton kerül telepítésre. Feladata többrétű:

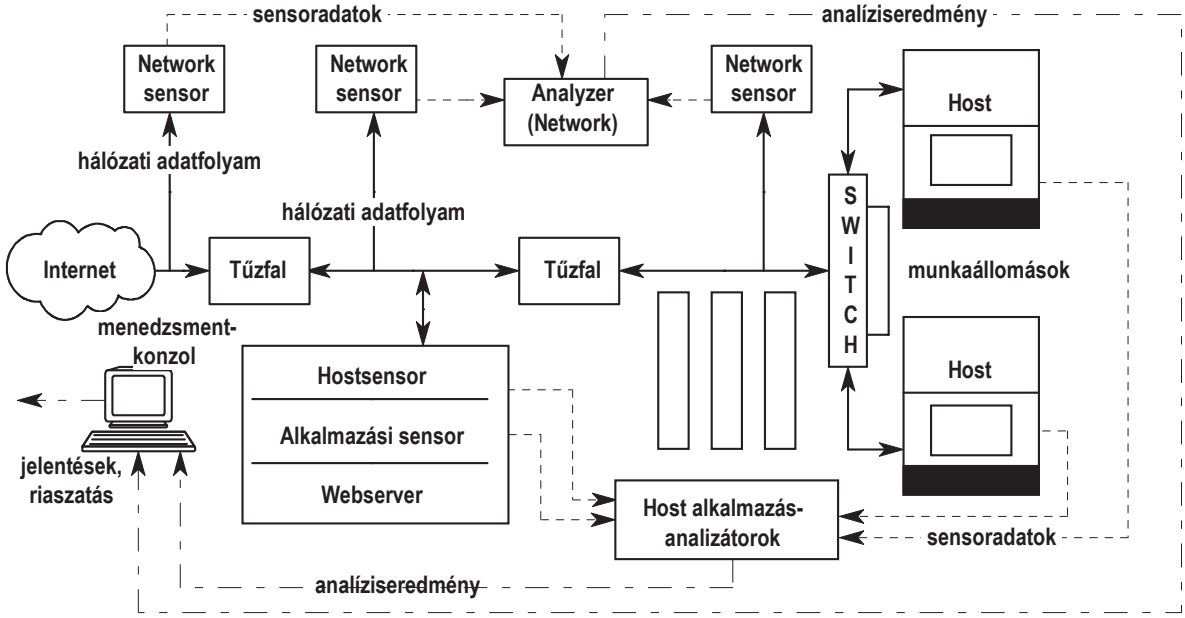
- operációs rendszer-felügyelet,
- alkalmazásfelügyelet,
- integritásvédelem és
- hosztspecifikus adatforgalom-ellenőrzés.

Az operációs rendszer védelme alkalmazásszinten történik. A vizsgálat kétféleképpen hajtható végre:

- egyrészt a logolási (naplózási) rendszeren keresztül (induláskor megfelelően konfigurálni kell, majd a logok tartalmát kell vizsgálni és észrevenni az eredeti beállításoktól eltérő eseményeket),
- másrészt speciális IDS Plugin szoftverek segítségével.

Alkalmazásfelügyeletet biztosító *szenzor* használata akkor javasolt, ha egy speciális applikációnak a védelme sem operációs rendszer, sem pedig hálózatfelügyeleti szenzorok segítségével nem garantálható. Az ellenőrzés általában az alkalmazás logadatainak kiértékelése útján történik.

Integritás-ellenőrzés során az IDS gyakori időközönként (adott esetben minden adathozzáféréskor) ellenőrzi, hogy az adattár (adatok, program) módosulása (ez esetben nem tartalmi ellenőrzésről van szó) elfogadható-e. Ez jellegzetesen az ellenőrzőösszeg egy előre definiált értékkel való összehasonlítása útján történik. Konkrétan felismert, nem megengedett változtatásnál ideális esetben az IDS az adatotokat visszaállítja az eredeti állapotukba. Ez azonban az integritás megsértése, a túl gyakori ellenőrzés vagy a processzorfolyamat feldolgozási szabálya miatt (multiprogramozott batch üzemmód) nagyon kritikus, és gyakran nem történhet meg valós időben. A túlzottan sok ellenőrzés elviselhetetlenül megterheli a rendszert, a túlzottan ritka pedig a kockázat növekedését eredményezi. A megfelelő konfiguráció megválasztása meglehetősen nehéz, és sok időt vesz igénybe. Fontos megemlíteni, hogy amíg az operációs rendszer specifikus szenzor az adatok tartalmát (logadatok) vizsgálja és megbízik azok integritásában, addig az integritásvizsgálat nem függ az adatok tartalmától.



6-2. ábra: IDS-rendszer architektúrája és működése

Hosztspecifikus hálózati adatforgalom ellenőrzése révén lehetőség nyílik a hálózaton egyébként titkosított adatforgalom dekódolására, és valamennyi, a hoszt kommunikációját végző IP-stackbe történő beépülésére. Mivel a hosztnak címzett csomagok száma aránylag csekély, ezért lehetőség van a teljes adatforgalom kimerítő átvizsgálására. A megoldás hátrányaként meg kell említeni, hogy az ilyen rendszerek nem tudják felismerni az elosztott, egyidőben több célhosztot érintő támadásokat. A piacon jelenleg kapható IDS-termékek nem nyújtanak megoldást erre a problémára.

Az általános jellemzők az alábbiak szerint foglalhatóak össze:

- Képes azonnal megfigyelni és kiértékelni a védett hoszton működő rendszer reakcióját (ellentétben a hálózat alapúval).
- Minden ellenőrizni kívánt hosztra telepíteni kell.
- A hoszt alapú szenzornak alkalmazás- és operációs rendszer-specifikusnak kell lennie, ellentétben a hálózat alapúval, ezért valamennyi védendő platformra rendelkezésre kell állnia, és egymáshoz igazítva kell működnie. A hoszt alapú IDS bevezetése általában magasabb költségekkel jár, mint a tisztán hálózat alapú.
- Nem tud észrevétlenül működni (ellentétben a hálózat alapúval). A támadónak lehetősége van egyidejűleg a védett rendszert és a hosztszenzort, ezáltal az IDS-t támadni.
- A védett rendszer erőforrásait használja, alulméretezett rendszer esetén ez problémát jelenthet.

Adatbank-komponens

Az adatbank-komponensben minden, az eszköz által ismert támadási módszer jellemzői leírásra kerülnek. Az IDS feladata, hogy az éppen vizsgált aktivitást összehasonlítsa az adatbázisbeli összes mintával, és ha valahol egyezőséget talál, azt jelezze. A megoldás egyszerű, azonban a megvalósítás során számos probléma merül fel. Minél nagyobb biztonságra akarunk törekedni, annál több elemet kell elhelyeznünk a minta-adatbázisban, ami azt jelenti, hogy az éppen vizsgált aktivitást egyre több elemszámmal kell összehasonlítani, ráadásul valós időben. A probléma két úton oldható meg: vagy az erőforrások növelésével, vagy a minta-adatbázisbeli elemszám csökkentésével. Míg az első megoldás tri-

viális lehet, addig az elemszám csökkentése látszólag csökkenti a védelem erősségét. Ha azonban az adatbázisban elhelyezett minták a rendszer sérülékeny pontjaira vannak kihegyezve és nem az összes fenyegető tényezőre, akkor csökkenthetjük az elemszámot, és így a rendelkezésre álló erőforrásokat a potenciálisan sikeres támadások detektálására tudjuk fordítani [4]. (A fenyegetettség és a sebezhetőség megértése elengedhetetlenül fontos nemcsak az optimalizálási folyamat, hanem az informatikai biztonsági stratégia kialakítása során is.)

Menedzsmentkomponens

A menedzsmentkomponens lehetővé teszi az IDS konfigurálását és beállítását. Mindez a következő feladatokat foglalja magába.

- IDS-komponensek felvétele (szenzor, adatbank, menedzsmentállomás)
- IDS-komponensek közötti kommunikációhoz szükséges paraméterek beállítása (IP-cím, titkosítási kulcs, életjel-intervallum)
- az ellenőrizendő objektumok felvétele (hálózat, hoszt)
- ellenőrzési szabályok (IDS Policies) előállítása, testreszabása és csoportosítása.
- IDS-szenzorok csoportosítása
- ellenőrzési feladatok kiosztása az egyes szenzorok, illetve csoportok között.

A gyakorlatban a menedzsmentállomás és a kiértékelő egység egy komponensként kerül megvalósításra.

Kiértékelő komponens

A tényleges felismerési folyamat a kiértékelő komponensben történik, amelynek további feladatai is vannak, így

- az események osztályozása,
- reakció- és riasztásküldés,
- tüzetes jelentés előállítása, valamint
- a kiértékelt adatok tárolása későbbi feldolgozás céljából.

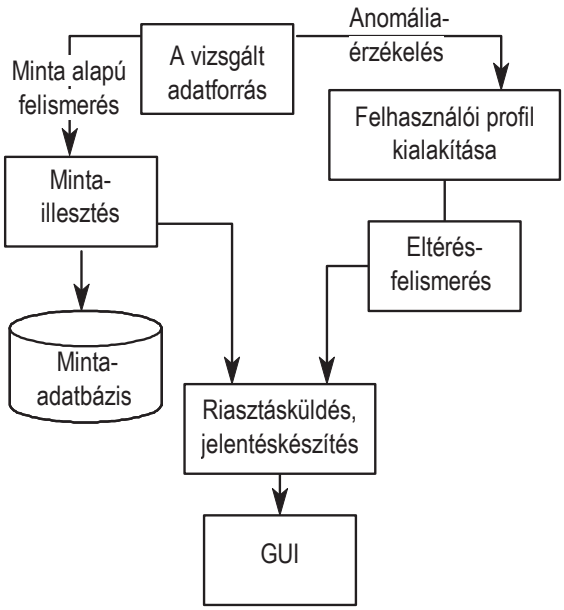
Az egység feladata az is, hogy a létrehozott eredményeket – figyelembe véve a felhasználó személyiségi jogait – megjelenítse, és a helyes kommunikációs utat megválasztva (e-mail, SMS stb.) közölje azt a biztonsági megbízottal és az IRS-sel.

Felismerési eljárások

A piacon ma fellelhető termékek alapvetően az alábbi támadás-felismerési technikákat használják:

- minta alapú betörésdetektálás és
- anomáliaérzékelés,

A cikk eddigi részében külön jelzés nélkül a minta alapú betörésdetektálási módszer került ismertetésre, ezért itt külön nem ejtek szót róla (lásd 6-3. ábra).



6-3. ábra: A minta alapú támadásfelismerés és az anomáliaérzékelés általános modellje

Anomáliaérzékelés

A támadás felismerése azon az elgondoláson nyugszik, hogy a támadás egy tipikus rendszerviselkedést okoz, amelyen keresztül az felismerhető. Ezért mindenekelőtt fontos, hogy meghatá-

rozzuk a védendő rendszernek a normális körülmények közötti viselkedését. Erre azért van szükség, hogy meg lehessen állapítani a szituációtól eltérő viselkedést (anomália).

Alapvetően három technika alkalmazása lehetséges:
- protokollvizsgálat,
- statisztikai adatok elemzése és
- mesterséges intelligencia alkalmazása.

Protokollvizsgálat

A megoldás feladata a hálózati forgalomanomália felismerése. A normál rendszerviselkedés meghatározása protokolldefiníció alapján történik, ezután már csak azt kell vizsgálni, hogy a hálózati forgalom megfelel-e az alapul vett protokollspecifikációnak. Az eljárással nagy megbízhatóságot lehet elérni, mivel nincs szükség nagy számú jelzésmintának egy külön egységet képező adatbankban történő elhelyezésére. Hátrány, hogy azok a támadások, amelyek ismeretlen vagy hibás protokollspecifikáción nyugszanak, nem felismerhetőek.

Felismerés statisztikai adatokkal

A támadásfelismerés ezen módja abból indul ki, hogy támadás esetén a rendszerviselkedés szignifikánsan eltér a statisztikai úton meghatározottól. Ahhoz, hogy a rendszer normális viselkedését meg lehessen határozni, különböző objektumokat (felhasználó, háttértár, alkalmazások stb.) és a hozzátartozó viselkedési szokásokat (a hibás bejelentkezések száma, bejelentkezés napszakja, bejelentkezési gyakoriság, használat időtartama stb.) kifejező statisztikai érték megállapítása szükséges. Az értékek alapján az IDS meg tudja állapítani, hogy az aktuális aktivitás szignifikánsan eltér-e a normálistól.

A megoldás előnye, hogy lehetőség nyílik a hamis felhasználói account-tal véghezvitt támadás felismerésére, anélkül hogy a támadó a szerzett felhasználói jogaival visszaélne. Hátrányként említhető, egyrészt, hogy a paraméterbeállítások megválasztása az egész rendszer viselkedésétől függ, ezért meglehetősen kritikus elem, másrészt pedig az eljárás nagy intuíciót kíván, hiszen sem a normális működés, sem pedig a felismerni kívánt támadás nem specifikus. Például nem lehet azt megállapítani, hogy a statisztikai adatok által megállapított normálértékek nem rejtenek-e magukban olyan, támadó viselkedésre utaló jeleket, amelyek később a normális viselkedés részeként kerülnek megállapításra.

Mesterséges intelligencia alkalmazása

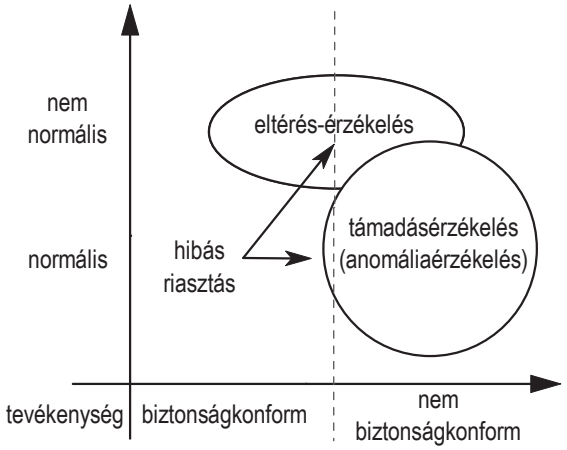
A mesterséges intelligencia gépi eljárást biztosít a manuális vizsgálathoz szükséges intuíciók kompenzálására. A cél a feldolgozás sebességének fokozása, mégis a magas hibaráta miatt manuális utómunka szükséges. Az eljárás még nem kiforrott, így pillanatnyilag egyik IDS-gyártó sem kínálja.

A rendszerek hatásfoka

A piacon kapható IDS-rendszerek szinte mindegyike minta alapú betörésdetektáló eszközként funkcionál. A rendszer által nyújtott védelem elsősorban a mintadatabázisbeli elemek naprakészségétől függ, azaz attól a jellemzőtől, hogy az adatbázisban milyen teljességgel találhatók meg a lehetséges támadási módok. Ezért alapvetően fontos, hogy a gyártói háttérapparátus mennyire folyamatosan követi a napvilágra kerülő új támadási formákat, és hogy azokat milyen gyorsasággal juttatja el a felhasználónak.

Az anomáliaérzékelő rendszerek jelenleg kutatási fázisban vannak. A megoldás hatásfokát az befolyásolja, hogy nem lehet egyértelműen megállapítani azt a normális viselkedést, amelyhez a rendszer az éppen aktuális aktivitást viszonyítja. Például, ha a felhasználói profilban a rendszerbe való belépés ideje reggel nyolc és kilenc óra időintervallumra van beállítva, akkor az ettől eltérő (például reggeli hét óra) bejelentkezést az IDS támadó magtartásnak értékeli, még akkor is, ha csak egy szorgalmas dolgozóról van szó.

A minta alapú és az anomálisérzékelő technikák összehasonlító kompetenciáit a 6-4. ábra szemlélteti.



6-4. ábra: A két technika kompetenciája

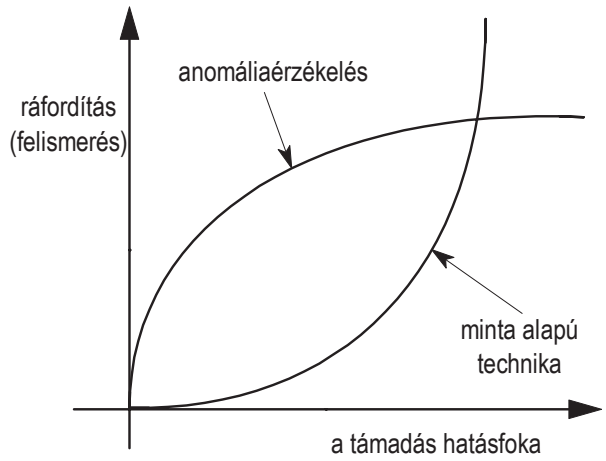
IRS automatikus reakció

Mihelyt a támadó elér egy számítógéprendszert vagy annak egy részét az elérés keretei között tetszőleges károkat okozhat. Az IRS feladata elsősorban a támadó azonosítása (IP-címének meghatározása), és csak másodsorban a támadási magatartással dimetrális viselkedés tanúsítása, azaz a további károktól való védelem. Ez például az alábbi tevékenységsorozatot jelentheti:

- az érintett TCP/UDP port leválasztása, a programok és szolgáltatások terminációja,
- azon IP-datagrammok visszautasítása, amelyek a támadó IP-címével érkeznek, adott esetben a felhasználói account zárolása, ha a támadás a belső hálózatról érkezik, valamint
- a keletkezett károk megszüntetése, például a biztonsági másolatok felhasználásával.

A rendszer bevezetési költségei

Mint ahogy sok, ma kapható biztonsági eszköznél, úgy az IDS-rendszereknél is nehéz megbecsülni a ráfordítási és az üzemeltetési költségeket. Bár az inicializálási költségek (termékvásárlás és installáció) a beszerzési ár alapján meglehetősen jól becsülhetőek, addig elég nehéz feladat a trainingphase költségek becslése anomáliaérzékelés alkalmazása esetében, különösen akkor, ha az instabil környezet mellékköltségeket okoz (lásd 6-5. ábra).



6-5. ábra: Különbségek a ráfordításban, az egyes technikákat tekintve

Egy biztonságos rendszer érdekében felmerült költségek a következő faktoroktól függnek:

- Mennyibe kerül a szakvélemény?
- Milyen eszközök állnak rendelkezésre a minták modellezéséhez?
- Mennyire ügyesek és hatásosak a kezelendő támadások?
- Mely operációs rendszerek érintettek?
- Milyen alkalmazásokat használnak az adott rendszeren? Sok programot ismerünk ugyanis immanens biztonsági gyengeséggel.
- Milyen információforrásokat kell megvizsgálni az új támadások felderítése céljából? Egyes mail-listák (mint például az NTSEC Windows NT Security) sok redundáns és lényegtelen információt tartalmaznak.
- Mennyire megbízhatóak a rendelkezésre álló információk? Egyes listák moderáltak (például a bugtraq), ezáltal az előfizető többnyire releváns információhoz jut.

Következtetések

Az IDS-technikát magában hordozó kereskedelmi termékek utáni igény egyre növekvő tendenciát mutat. A védtelen rendszerek kiszolgáltatottságával kapcsolatos ismeretek folyamatos bővülése és a fokozott biztonságra való törekvés megköveteli az IDS-piac gyors fejlődését. Valószínűnek tűnik, hogy az IDS-fejlesztők a jövőben a tervezésnél több szempontot fognak figyelembe venni, így például a többi biztonsági eszközökkel (tűzfal, víruskereső, biometrikus azonosítás, titkosítási eljárások, vulnerability scanner stb.) való együttműködési képességet, a felhasználóbarátság követelményét, az internetes alkalmazások támogatottságát és a populáris operációs rendszerek, mint a Windows támogatását.

Jelenleg még számos korlátja van az elvárásoknak megfelelő teljes funkcionalitású IRS-rendszerek széleskörű forgalmazásának és alkalmazásának, hiszen a kapható eszközökben az IRS-funkció még csupán részfeladatként jelentkezik, és sok az ellenvetés az automatikus IRS-intézkedések bevezetése tekintetében is.

Az egyik égető megoldás az IDS-szabványosítás, amelyre már vannak kezdeményezések. Ezek közül a legmeghatározóbbak az alábbiak.

- *Common Intrusion Detection Framework Projekt (CIDF):* A CIDF az amerikai DARPA által támogatott projekt, amely definiálja az egyes komponenseket (eseménykiválasztó, eseménykiértékelő, adattároló és reakció), illetve az egyes komponensek közötti kommunikáció protokollját. A kiértékelendő eseménnyel való szabványos kapcsolatot a „Common Intruction Specification Language" (CISL) határozza meg.
- *IETF Intrusion Detection Working Group (IDWG)* Az IDWG révén kifejlesztett „Intrusion Detection Exchange Format" (IDEF) a támadási minták formátumát definiálja. 2000. 06. 05-én hozták nyilvánosságra „Internet Draft" néven.
- *Common Content Inspection (CCI) API, OPSEC (Check Point)* A CCI API egy szabványos portot határoz meg, amelyen keresztül a vizsgálatot igénylő gyanús aktivitások a kiértékelő állomásba továbbíthatók. Az OPSEC (www.opsec.com) egy sor API-t és protokollt definiál, amelyek lehetővé teszik a releváns adatok rendszerek közötti cseréjét. Kérdés, hogy amely gyártók építik termékükbe a megoldásokat.
- *Common Vulnerabilities and Exposures (CVE)* A CVE (cve.mitre.org) célja az összes támadásminta és sebezhetőség egységes névvel és számmal való ellátása.
- *ISO Technical Support* Az ISO/IEC elkészített egy technikai összefoglalót Intrusion Detection témában, amely áttekintést nyújt az alkalmazásában.

A CIDF csak a szerkezetet határozza meg, az IDEF kizárólag a támadási formák szabványos leírását, a CVE pedig egyedül a szabványos megnevezéssel foglalkozik. A CIDF és IDEF a jelenleg kapható és a gyártók által támogatott termékben nem kerültek megvalósításra, a CVE számozást viszont szinte mindegyik produktum figyelembe veszi.

Hivatkozások

[1] Benjamin H.: *Intrusion Detection System in Firewalls* – Uni.Hamburg, 2002.

[2] *Das Erkennen von Angriffen auf Rechner und Rechnernetze* – BSI, 2002.

[3] *Einführung von Intrusion Detection System* – ConSecur Gmbh, 2002.

[4] Kőrös Zsolt.: *Betörésdetektáló eszközök, Az informatikai biztonság kézikönyve* – Verlag Dashöfer, 2002.

[5] Paul E. P.: *The Practical Intrusion Detection Handbook* – Prentice Hall, 2001.

[6] Roland B.: *Transaction-based Anomaly Detection* – USENIX, 1999.

[7] Stephen N.: *Network Intrusion Detection* – New Riders, 2000.

[8] Venesz B.: *Támadásérzékelés és kezelés hálózatos környezetben* – SZE-TMDK dolgozat, 2002.