Gyakorlati fenyegetettségelemzés és kockázatkezelés

Attól, hogy fenyegetettségelemzést végzünk, még nem fogunk nyugodtabban aludni, de segít abban, hogy felébredve helyesen cselekedjünk.

Aki már régebb óta olvassa ezt a rovatot, tapasztalhatta, hogy szeretem, ha a műszaki megoldásokhoz, eszközökhöz és technikákhoz elegendő háttéradat áll rendelkezésre.
A biztonság hatalmas témakör, és az egyetlen lehetőség, hogy eligazodjunk a változatok, módszerek és fekete mágia tengerében, az, ha megpróbáljuk megtalálni a közös pontokat ebben a biztonsági kirakójátékban.
Az egyetlen darabka, amely minden biztonsági feladatban közös, a fenyegetettség. Fenyegetettség nélkül ugyanis nincs értelme a biztonsági feladatokról beszélni. Csakhogy vajon mennyi időt töltünk a fenyegetettség felmérésével és értékelésével ahhoz képest, hogy mennyit szánunk a biztonsági megoldások telepítésére és (remélhetőleg) karbantartására? Valószínűleg igen keveset. Még ha így is van, ne keseredjünk el nagyon, hiszen még a biztonsági szaktanácsadók is túl keveset foglalkoznak a fenyegetettségelemzéssel.
Természetesen, nem azt mondom, hogy órákat töltsünk el vele. Álláspontom az, hogy eszményi esetben csak kritikus rendszereink sértetlenségét és elérhetőségeit kell rendszerezetten végigböngészni; végül a kevésbé szükséges, de fontos rendszerek fenyegetettségét is legalább egyszer szervezetten végig kell gondolni. Vagyis nekünk van valamink (vagyon), a Rosszfiúk pedig szeretnék ezt a valamit.
Mielőtt elmerülnénk a fenyegetettségelemzés rejtelmeiben, előbb érdemes lefektetnünk néhány fontos alapelvet és meghatározást. Először is, mit jelent egyáltalán a fenyegetettség? Nagyon egyszerűen: a fenyegetettség a vagyon, a sérülékenység és a támadó együttese.
A vagyon bármi lehet, amit csak meg szeretnénk óvni. Adatbiztonsági értelemben a vagyon legtöbbször adat, számítógépes rendszer vagy számítógépes hálózat. Ezen „vagyontárgyak" sértetlenségét (adatok esetében a bizalmasságukat) szeretnénk megőrizni.
A sértetlenség a jogosulatlan változtatások hiányát jelenti. A jogosulatlan változtatások eredményeképpen a számítógép vagy az adat sértetlensége megszűnik. Ez jelentheti azt, hogy hibás adatot szúrnak a valós adatok közé, a törvényes adatok egy részét törlik vagy megváltoztatják. Számítógépek esetében azt takarja, hogy a támadó a beállításfájlokat úgy változtatja meg, hogy a jogosulatlan felhasználók a rendszert képesek lesznek helytelen módon használni.
Adataink legalább egy részének a bizalmasságát is meg szeretnénk őrizni. Ez valamelyest más feladat, mint a sértetlenség, hiszen a bizalmasság passzív módon is károsítható. Hogy valaki megváltoztatja az adatainkat, könnyen felfedezhetjük és kivizsgálhatjuk – egyszerűen az eredeti és a károsított adat összehasonlításával. Amennyiben azonban a támadó adatainkat jogosulatlanul másolja le (azaz ellopja), a felderítés és a kárfelmérés sokkal nehezebb, hiszen az adat tulajdonképpen nem változott.
Tegyük fel, hogy ABC Társaság rendelkezik egy SMTP-átjáróval, amely a bejövő leveleket dolgozza fel. Ez az SMTP-átjáró két vagyonértéket képvisel. Az első maga a kiszolgáló, melynek tökéletes működése az ABC Társaság napi üzletmenetében igen fontos szerepet tölt be. Más szavakkal az ABC Társaságnak meg kell védenie SMTP-átjárója sértetlenségét, hogy az e-mail szolgáltatása ne szakadhasson meg.
Másodszor ez az SMTP-átjáró tárolja a rajta keresztül érkező leveleket. Így ha az átjáró rendszere megsérül, a bizalmas levelekbe beleolvashatnak, illetve fontos adatokhoz férhetnek hozzá. Az SMTP-átjáró védelme tehát az ABC társaság e-mail adatainak bizalmasságának és sértetlenségének megőrzésében is fontos szerepet játszik.
Az első lépés minden fenyegetettségelemzés esetében tehát a védendő vagyonértékek, illetve a vagyonértékek védendő minőségének, tulajdonságainak a meghatározása.

Sebezhetőségek

A második lépés az érték, illetve a vele közvetlen kapcsolatban álló rendszerek ismert és kézenfekvő sebezhető pontjainak meghatározása. Természetesen az ismert gyengeségekre sokkal könnyebb megoldást találni, mint a tisztán elképzeléseken alapulókra (legalábbis így gondolnánk, mégis jelentős számú számítógép fut az Interneten alapértelmezett, változatlan operációs rendszerrel). Ennek ellenére mindkét fajtát meg kell próbálnunk beazonosítani.
Az ismert gyengeségek programjavítások használatával, körültekintő beállítással, vagy a terjesztő hirdetőtábláin és a nyilvános fórumokon megjelenő utasítások betartásával könnyen javíthatók. Azok a gondok, amelyek ily módon nem enyhíthetők, további vizsgálatot és mérlegelést igényelnek, és vagy külső módszerekkel védhetők (például tűzfallal), vagy el kell őket fogadni, mint az adott rendszer tevékenységének velejáróját.
Az ismeretlen sérülékenységeket meghatározás szerint általánosan kell kezelni, de a jelentőségük ettől még cseppet sem csökken. Ezt a legkönnyebben egy példa segítségével tudjuk bemutatni.
Térjünk vissza ismét az ABC Társasághoz. A levelezés rendszergazdája a Sendmailt szereti futtatni az ABC Társaság SMTP-átjáróján, mivel jól ért a Sendmail beállításaihoz, és eddig jól megfelelt a céloknak. Ugyanakkor nem táplál ábrándokat a Sendmail biztonsági kérdéseit illetően; folyamatosan figyeli a biztonsági hirdetéseket, és minden javítást, frissítést azonnal felrak, amint megjelenik. Az ABC Társaság így az ismert Sendmail-kiskapuk ellen elég jól védett.
Az ABC igazán menő e-mail rendszergazdája azonban nem elégszik meg ennyivel. Igaz, biztos benne, hogy a Sendmail már biztonságosan javított és beállított, de azt is tudja, hogy korábban voltak veremtúlcsordulási kiskapuk, amelyek gondokat okoztak, különösen akkor, ha a Sendmailt rendszergazdaként futtatták (rendszergazdaként ugyanis a futó folyamat eltérítése a rendszergazdai jogosultság megszerzésével egyenértékű). Ezért aztán a Sendmailt `chroot jail` alatt futtatja (a teljes rendszer egy alhalmazán) root felhasználó helyett `mail`-felhasználóként, és ennek megfelelően állítja be a Sendmail `SafeFileEnvironment` és `RunAsUser` feldolgozási kapcsolóit. Ezáltal az SMTP-átjáró többszintű védelemre is szert tesz,

Leírás	Becsült ár
Helyreállítás: megbeszélés egy külső céggel (4 óra×150 dollár)	600 dollár
Kieső termelés (2 óra per 10 munkás x átlagosan 17.5 dollár/óra)	350 dollár
FAX-papír, hőalapú (thermal) (1 tekercs 16 dollár)	16 dollár
Távolsági FAX-kapcsolatok (20 x átl. 2 perc×0,25 dollár/perc)	10 dollár
Összes SLE egynapos SMTP-kiszolgáló elleni DOS-támadás esetén	***950 dollár***

1. táblázat Részletezett egyedi várható veszteség

és már nemcsak az ismert gyenge pontok ellen védett, hanem bizonyos ismeretlen kiskapuk ellen is, amelyek ugyan károsíthatják a Sendmailt, de egyúttal remélhetőleg nem okozzák a teljes rendszer károsodását.

Támadók

A fenyegetettség-kirakójáték utolsó darabkája, amit megvizsgálunk, mielőtt a fenyegetettségelemzés rejtelmeibe belevetnénk magunkat, maga a támadó. A támadók, vagy ahogy néha nevezik őket, a „művészek" (actors), igen változatosak lehetnek, a várhatóaktól (elégedetlen exalkalmazottak, csintalan fiatalok) kezdve egészen a „különös, de igaz" (kábítószerszövetségek, kormányzati ügynökségek, ipari kémek) típusokig. Ha a lehetséges támadókat számba vesszük, kiderül, hogy szinte minden típusuk előfordulhat; feladatunk ilyenkor, hogy megbecsüljük, vajon melyik támadó a legvalószínűbb.
Jó ökölszabály ilyen esetekre, ha számba vesszük, milyen támadók ellen tervezték is a fizikai biztonsági rendszereket, majd azokat a földrajzi korlátoknak megfelelően módosítjuk. A két dolog között párhuzam vonható: ha költséges zárat szerelünk fel a számítógépterem ajtajára, senki sem kérdezi meg tőled, hogy „tényleg azt hiszed, a karbantartók ellopják ezeket a gépeket, ha hazamegyünk?"
A számítógépes biztonság semmiben sem különbözik ettől. Gyakran hallani olyasmit, hogy „az én adataim érdektelenek; senki sem akarhatja feltörni a rendszeremet", pedig nincs más választásunk, mint feltételezni, hogy ha valamilyen támadás ellen sérülékenyek vagyunk, azt valaki ki fogja használni, még akkor is, ha el sem tudjuk képzelni, vajon miért teszi. Nyilvánvalóan nem az a fontos, hogy megértsük a támadó észjárását, hanem hogy beazonosítsuk és mérsékeljük a támadható gyengeségeket.

Egyszerű kockázatelemzés: ALE-k

Miután összeállítottuk az értékek és a gyenge pontok listáját (és végiggondoltuk a lehetséges támadókat), a következő lépés a köztük lévő kapcsolat feltárása, illetve a mennyiséghatározás. Egy egyszerű módszer, amivel lemérhetjük a kockázat mértékét, az éves várható veszteség (annualized loss expectancies, azaz ALE-k) kiszámítása.
Az összes gyenge pontot minden egyes értékkel párosítva előbb megbecsüljük az adott érték pótlásának vagy helyreállításának költségét (egyszeri veszteséggel számolva), majd megállapítjuk a gyenge pont várható éves előfordulási gyakoriságát. Ezekután a kettőt összeszorozva kapjuk meg a sérülékenység éves várható veszteségét.
Más szavakkal: minden gyenge ponthoz kiszámítjuk a következő értéket: egyszeri várható veszteség (költség) × (várható) éves gyakoriság = éves várható veszteség.
Például egy kisvállalkozás, a Mommenpop Kft. ki szeretné számítani az SMTP-átjárójuk elleni DoS (denial of service) támadásokra vonatkozó ALE-értéket. Tegyük fel továbbá, hogy az e-mail szolgáltatás kulcsfontosságú az üzletmenethez; mind a tíz alkalmazottjuk e-mail alapján számláz az ügyfeleknek, így ad munkabecsléseket a jövendőbeli vásárlóknak, illetve más hasonlóan fontos üzleti kapcsolattartást folytat. Ugyanakkor a hálózatkezelés nem éppen a szakterületük, így egy helyi tanácsadócégre bízzák az levelezőkiszolgáló kezelését.
A korábbi, átlagosan egynapos kimaradások a termelékenységet körülbelül az egynegyedével csökkentették, amely visszaszámolva napi két órát ad ki alkalmazottanként. Tartalékrendszerük egy faxgép, de mivel székhelyük egy kisvárosban található, ez távolsági hívásokkal jár és meglehetősen drága.
Lehet, hogy kicsit talán bonyolultabban hangzik, mint amilyen valójában; táblázatban kifejezve azonban máris sokkal kevésbé elrettentő (lásd az *1. táblázatot*).
A következő lépés az adott gond várható éves előfordulásának (Expected Annual Occurrence avagy EAO) megbecslése. Ezt számként gond per év hányadosként szokás kifejezni. Példánkat folytatva tegyük fel, hogy a Mommenpop Kft. ez idáig még semmiféle kémkedésnek vagy más, a versenytársak által elkövetett támadásnak nem volt célpontja, és legjobb tudásunk szerint a levelezőkiszolgáló elleni DoS-támadások legvalószínűbb forrásai vandálok, gengszterek, zűrös emberek és más véletlenszerű idegenek lehetnek.
Elfogadhatónak tűnik az a becslés, miszerint ilyen támadás két- vagy háromévente körülbelül egyszer fordul elő; de legyünk óvatosak és mondjunk kettőt. Kétévente egy támadás átlagosan 0,5 gondot jelent évente, azaz az EAO 0.5. Illesszük be ezt az értéket az ALE-képletbe:

```
950 ($/problØma)   0.5 (problØma/Øv) = 475 ($/Øv).
```

A Mommenpop SMTP-átjáró elleni DoS-támadások ALE-értéke tehát 475 dollár évente.
Most tegyük fel, hogy valamilyen terjesztő megpróbálja rábeszélni a céget saját fejlesztésű Linux-tűzfalának kereskedelmi tűzfalra való cseréjére; ez a termék beépített SMTP-proxyval rendelkezik, ami segít csökkenteni, de nem szünteti meg az SMTP-kapu DoS-támadásokkal szembeni érzékenységét. Tegyük fel, hogy ez a termék 5000 dollárba kerül. Még ha a költségeket három évre osztjuk is el (10% kamattal számolva ez évente 2166 dollárt tesz ki), egy ilyen tűzfalfejlesztés nem tűnik igazán jogosnak egyetlen kockázatforrás kiküszöbölésére.
A *2. táblázat* a képzeletbeli cégünk SMTP-átjárójának fenyegetettségelemzését mutatja be kicsit teljesebb formában, ahol nemcsak az ALE-eket, hanem számos más, a vagyonértékeinket célzó számértéket is bemutatunk, illetve különféle biztonsági célokat is láthatunk. Ebben a példaelemzésben a vásárlói adatok bizalmassága minősült a legfontosabb kockázati értéknek; ha ugyanis ezeket fürkészik ki vagy ezekbe nyúlnak bele, a cég könnyen elveszítheti a vásárlóit (hiszen megrendül a Mommenpoppal szembeni bizalom), ami végsősoron a jövedelem megcsappanását jelenti. E veszteségek különböző jelentőségét mutatják az egyes gyenge pontokhoz tartozó egyszeri várható veszteségábrák. Hasonlóképpen a különféle becsült éves előfordulási mennyiségek az egyes gyenge pontok tényleges kihasználásának relatív valószínűségét mutatják.

Érték	Biztonsági cél	Sérülékenység	SLE$/konfliktus	ARO konfliktus/év	ALE$/év
SMTP-átjáró	Rendszerintegritás	Sendmail-hibák	2400 dollár	0,5	1200 dollár
		Egyéb rendszerhibák	2400 dollár	0,5	1200 dollár
	Rendelkezésre állás	DOS-támadás	950 dollár	0,5	475 dollár
Bizalmas e-mail (ügyfél számlaadat)	Adatbizalmasság	Kémkedés az Interneten vagy az ISP-nél	50 000 dollár	2	100 000 dollár
		SMTP-átjáró feltörése	50 000 dollár	0,5	25000 dollár
		Rossz szándékú belsős	150 000 dollár	0,33	49500 dollár
	Adatintegritás	Hamisított levél a vásárlónak/-tól	10 000$ dollár	1	10 000 dollár
		Továbbítás alatti változtatás az Interneten vagy az ISP-n	10 000 dollár	0,25	2500 dollár
		SMTP-átjáró feltörése	10 000 dollár	0,5	5000 dollár
Nem bizalmas e-mail (művelet-adatok)	Adatintegritás	Továbbítás alatti változtatás az Interneten vagy az ISP-n	3000 dollár	0,25	750 dollár
		SMTP-átjáró feltörése	3000 dollár	0,5	1500 dollár

2. táblázat ALE-alapú példa fenyegetettségmodell

Minthogy a 2. *táblázatban* látható példaelemzést táblázat formájában adtuk meg, a sorokat tetszés szerint könnyen rendezhetjük. A 3. *táblázat* ugyanezt az elemzést mutatja be sérülékenység szerint rendezve.

Hasznos lehet, ha az azonos sérülékenységekhez tartozó ALE-ket összeadjuk. A leveleknek az Interneten töltött idő alatt vagy az ISP-n történő megváltoztatásának eredménye: 2500 dollár és 750 dollár, összesen tehát 3250 dollár ALE-érték. Ha a képzést feladó tanácsadó például 2400 dollárt kér három félnapos tanfolyamért, ahol a dolgozóknak azt mutatják be, hogyan kell az ingyenes GnuPG programot a dokumentumok aláírására használni, akkor a kiképzési díj ezzel a veszélyforrással arányban áll. Azt is láthatjuk, hogy bizonyos ALE-k egyes sérülékenységekkel kapcsolatban állnak. A 3. ábrán megfigyelhetjük, hogy az alsó három ALE az SMTP-átjáró károsítása miatt bekövetkezett veszteségeket gyűjti össze. Más szavakkal az SMTP-átjáró sérülése nem csak a termeléskiesés és a vaskos helyreállítási költségek miatt okoz veszteséget (1200 dollár bármelyik ALE esetében, a 3. táblázat tetején), hiszen a levéladatok károsodásának kockázata további 31 500 dollár veszteséggel is fenyegeti a céget, így az ide tartozó ALE értéke összesen 32 700 dollár. Látható, hogy a levelezés kikémlelésének vagy módosításának veszélye igen magas. A Mommenpop Kft. jobban tenné, ha máris hívná azt a 2400 dolláros oktatót.

Az ALE-n alapuló elemzőeszközök egyik nagy hátránya a részrehajló szemléletmód (figyeljük meg, a fenti leírásban milyen gyakran szerepeltek a „valószínű” és a „megfelelő” szavak), és épp emiatt a végeredményt a gyakorlati adatok helyett alapvetően a tanulmány készítőjének tapasztalata és tudása határozza meg.

Ez módszer ráadásul nem ad igazán jó lehetőséget az ALE-k összehasonlítására (az olyan rövidke listáktól eltekintve, mint a 2. és a 3. táblázat).

Az ALE-módszer előnye egyszerűségében és rugalmasságában rejlik. Bárki, aki elegendő ismerettel rendelkezik a saját rendszerének felépítéséről és működtetési költségeiről, és nagyjából tisztában van a jelenlegi főbb IT-s (információtechnológiai) biztonsági irányvonalakkal (például olvassa a CERT jelenlegi és korábbi tanácsadó és az összetűzésekről szóló jelentéseit), a környezetről már könnyedén hosszú ALE-listát képes készíteni. Ha ezt a listát táblázatos formában jelenítjük meg, a különféle költségek és gyakoriságok megbecslése különösen könnyű. Annak ellenére, hogy ez a módszer valóban erőteljesen elfogult (amit a kockázatvizsgálatokban teljes mértékben nem is lehet kizárni), igen fontos és hasznos eszköz a kockázati tényezők összeszámlálásában, mennyiségi becslésében és a kockázatok súlyozásában. Az éves várható veszteségek jól szerkesztett listája sokat segíthet nekünk abban, hogy IT-s biztonsági kiadásainkat arra gyenge pontra költsük, amely a leginkább számít.

Egy másik megoldás: Schneier támadási fadiagrammja

Bruce Schneier, az Applied Cryptography (Alkalmazott kriptográfia) szerzője a kockázatelemzés egy másik formáját vezette be: a támadási fákat. A támadási fa nagyon tömören egy adott célpont elleni támadási lehetőségek szemléletes megjelenítése. A támadási célpontot (target) gyökércsomópontnak nevezzük (root node), a cél eléréséhez szükséges alcélokat pedig levélcsomópontoknak hívjuk (leaf nodes).

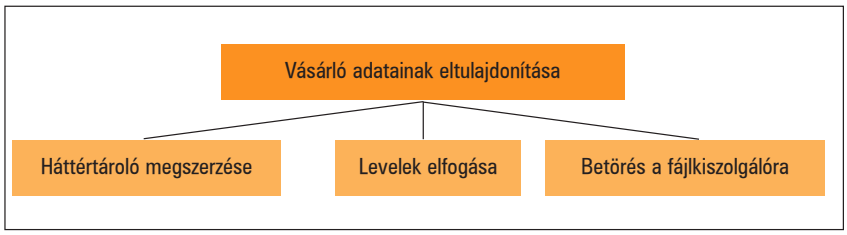
A támadási fa elkészítéséhez először is meg kell neveznünk egy gyökércsomópontot. Támadási cél lehet például az „ellopni a Mommenpop Kft. vásárlóinak bejelentkezési adatait”. Ennek közvetlen módozatai a következők lehetnének:

1. A Mommenpop-fájlkiszolgáló szalagjainak megszerzése,
2. A Mommenpop Kft. és a vásárlói közti e-mailforgalom elfogása és
3. Interneten keresztüli betörés a Mommenpop-fájlkiszolgálóra.

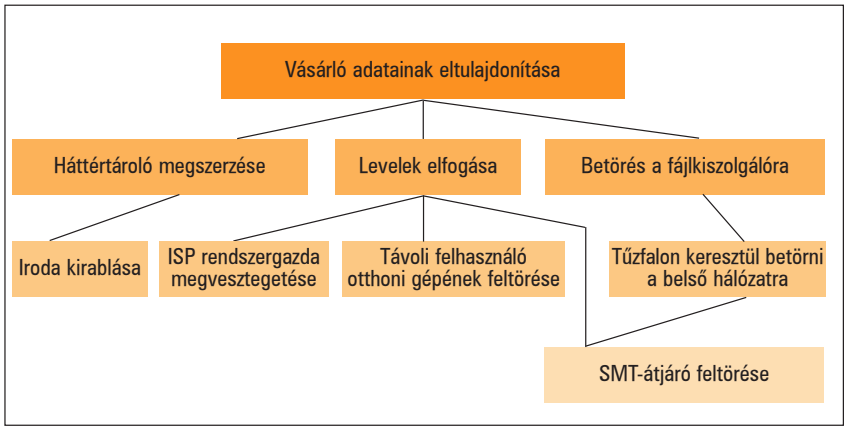
Érték	Biztonsági cél	Sérülékenység	SLE $/konfliktus	ARO konfliktus/év	ALE $/év
SMTP-átjáró	Rendszerintegritás	Sendmail-hibák	2400$	0,5	1200$
SMTP-átjáró	Rendszerintegritás	Egyéb rendszerhibák	2400$	0,5	1200$
Bizalmas e-mail (ügyfél számlainformáció)	Adatbizalmasság	Rossz szándékú belsős	150000$	0,33	49500$
Bizalmas e-mail (ügyfél számlainformáció)	Adatintegritás	Továbbítás alatti változtatás az Interneten vagy az ISP-n	10000$	0,25	2500$
Nem bizalmas e-mail (művelet információk)	Adatintegritás	Továbbítás alatti változtatás az Interneten vagy az ISP-n	3000$	0,25	750$
Bizalmas e-mail (ügyfél számlainformáció)	Adatintegritás	Hamisított levél a vásárlónak/-tól	10000$	1	10000$
Bizalmas e-mail (ügyfél számlainformáció)	Adatbizalmasság	Kémkedés az Interneten vagy az ISP-nél	50000$	2	100000$
SMTP-átjáró	Rendelkezésre állás	DOS-támadások	950$	0,5	475$
Bizalmas e-mail (ügyfél számlainformáció)	Adatbizalmasság	SMTP-átjáró feltörése	50000$	0,5	25000$
Bizalmas e-mail (ügyfél számlainformáció)	Adatintegritás	SMTP-átjáró feltörése	10000$	0,5	5000$
Nem bizalmas e-mail (műveletinformációk)	Adatintegritás	SMTP-átjáró feltörése	3000$	0,5	1500$

2.táblázat Ugyanez a példa sérülékenység szerint rendezve

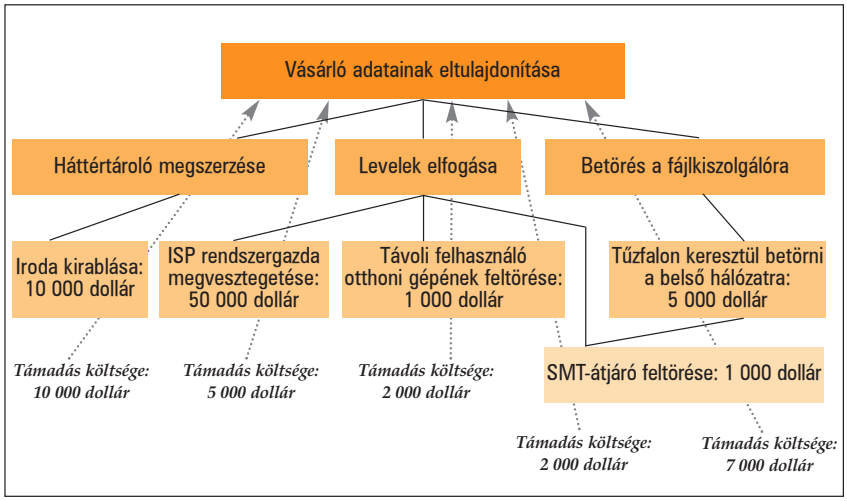
Ez a három alcél (levélcsomópont) helyezkedik el közvetlenül a gyökércsomópont alatt. (Lásd a *4. ábrát*)
Most minden egyes levélcsomóponthoz meg kell keresnünk azokat az alcélokat, amelyek az adott levélcsomópont eléréséhez feltétlenül szükségesek. Ez lesz a következő levélcsomópont-rétegünk. Ezt a lépést addig ismételgetjük, amíg a kívánt mélységet és összetettséget el nem érjük. Az *2. ábra* egy egyszerű, de többé-kevésbé teljes támadási fát mutat be a Mommenpop Kft. esetében.
Kétségtelen, hogy további kiegészítő leveleket is kitalálhatnánk az *5. ábrán* jelölt két réteghez, sőt akár új rétegeket is készíthetnénk. De tegyük fel, hogy a jelen környezet meglehetősen jól biztosított a belső támadásokkal szemben (elég ritka, hogy valóban így is van), illetve hogy egy kívülálló számára ezek a leginkább keresztülvihető támadási metódusok.
A példából sok minden kiolvasható: a háttér adathordozó megszerzése legkönnyebben az irodába történő behatolással oldható meg; a belső fájlkiszolgáló feltörése a tűzfal keresztültörését foglalja magába, az elfogott levelek segítségével pedig három különféle módon férhetünk hozzá az adatokhoz. Azt is leolvashatjuk róla, hogy bár a tűzfal támadása a legjobb módszer a Mommenpop Kft. SMTP-kiszolgálójának feltöréséhez, egy másik, közvetlenebb módszer is adódik: az elfoglalt átjárón keresztül haladó levelek elolvasása.
Ezek nagyon fontos adatok. Lehet, hogy a cég több pénzt szándékozik a tűzfalra költeni, de megeshet, hogy úgy dönt, jobban megéri neki, ha a pénzt és az időt az SMTP-átjáróra fordítja. Legalább ilyen fontos az is, hogy láthatjuk az egyes támadási célok közötti kapcsolatokat, amit ezzel a fával még nem végeztünk el. Ha a támadási fát a kívánt mélységig felrajzoltuk, elkezdhetjük felbecsülni az egyes leveleket. Például minden egyes levélhez árcédulát kapcsolhatunk, amely az adott cél eléréséhez szükséges becsült pénzösszeget jelképezi. Ha minden támadási vonalat árcédulákkal jelöltünk meg, könnyen megbecsülhetjük a különféle támadási módok egymáshoz viszonyított költségét. A *3. ábra* az árcédulákkal kiegészített támadási fát mutatja be (a pontozott vonalak a támadási utat jelölik).
A 3. ábrában úgy találtuk, hogy a betörés elég költséges támadási forma, hiszen az elfogatást és a börtönt is megkockázatja. Senki sem fogja ezt a munkát nekünk megfelelő ellenszolgáltatás nélkül elvégezni. Ugyanez igaz az ISP rendszergazdájának megvesztegetésére; még egy megvásárolható ISP-alkalmazott is kétszer meggondolja, érdemes-e elvesztenie a munkáját és priuszt szereznie.
A feltörés egy kicsit más – bár éppúgy törvénytelen, sokkal kevésbé tartják kockázatosnak, mint a betörést. Továbbá a legtöbb szervezet számítógépes védelmét sokkal kevésbé nehezebb áttörni, mint a fizikai védelmet.
Azt mondják, egy tűzfal keresztültöréséhez egy kicsit nagyobb tudás kell, mint amennyivel egy átlagos script-kiddie rendelkezik, továbbá némi időt és erőfeszítést igényel; így aztán ez is viszonylag drága cél. Az SMTP-átjáró feltörése már sokkal könnyebb, és ha már beazonosítottunk egy vagy több távoli felhasználót, akkor az adott felhasználó otthoni gépe jó eséllyel könnyedén feltörhető. Ezért ezt a két célt olcsóbbnak minősítettük.
A támadástípusoknak megfelelő képzettségű bűnözők bérlési költsége alapján e példában a legígéretesebb támadási forma az SMTP-átjáró feltörése és a távoli felhasználók gépeinek elfoglalása. A Mommenpop Kft. úgy tűnik, jobban teszi, ha hálózata peremvidékét, az SMTP-kiszolgáló biztonságát és a távoli elérési lehetőségeket kicsit jobban megvizsgálja.
Természetesen a levelekhez nem csak költséget rendelhetünk. Beilleszthetünk kétértékű (boolean) mennyiségeket is, mint például kivitelezhetőeket és nem kivitelezhetőeket; a „nem



1. ábra Gyökércsomópont három levélcsomóponttal



2. ábra Egy részletesebb támadási fa



3. ábra Támadási fa költségbecsléssel

kivitelezhető" a támadási fa bármely pontján egyúttal azt is jelenti, hogy az egész ág kivitelezhetetlen.
Írhatunk ide befektetett munkamennyiséget is, órában vagy percben. Röviden: egyazon támadási fát többféle módszerrel is megvizsgálhatunk, és rendszerünk gyengéiről olyan felbontású képet alkothatunk, amilyet csak akarunk. A *6. ábrában* látható költségbecslések mind azt feltételezték, hogy a támadás kivitelezéséhez a támadónak fel kell bérelnie valakit. Ezeket az értékeket egészen másképpen kellene számítani, mint ha a támadók maguk is tapasztalt rendszerkalózok – ilyen esetben az időbecslés minden csomópontra hasznosabb a költségbecslésnél.

Védekezés

A fenyegetettségelemzés végső célja az lenne, hogy meghatározzuk, milyen szintű védelmet kell felhasználnunk azokon a területeken, amelyeken rendszerünk gyengének tűnik.

Háromféleképpen csillapíthatjuk a kockázatot. A védelmi stratégiákat aszerint csoportosíthatjuk, hogy a támadó számára csökkentjük a vagyon értékét , mérsékeljük az adott gyengeségeket, illetve semlegesítjük vagy megelőzzük a támadásokat. A vagyon értékének csökkentése nem tűnik túl járható útnak, de gondoljunk csak bele: a vagyon értékét a támadó számára kell csökkentenünk, és nem a jogos felhasználók/tulajdonosok számára. A legjobb példa a titkosítás: az alkalmazott támadástípus a cikkben említett példák mindegyikében nagyjából semlegesíthető, amennyiben megfelelő levéltitkosító programot alkalmazunk. Az adatvédelem másik stratégiája a gyengeségek megszüntetése vagy mérséklése. A programjavítások, foltok jó példák erre: minden egyes Sendmail-hiba évek óta arra ösztönözte a fejlesztőket, hogy foltokat adjanak ki, amelyek az adott hibát kijavítják.
A gyengeségek csökkentésére még jobb példa a védekező kódolás. Ha forrásfájljainkat olyan szűrőkön futtatjuk keresztül, amelyek mondjuk megtalálják a hibás határvizsgálatokat, akkor elősegíthetjük, hogy programunk ne legyen sérülékeny a veremtúlcsorduláson alapuló támadásokkal szemben. Ez a módszer sokkal hatékonyabb, mintha egyszerűen, minden ellenőrzés nélkül kibocsátanánk a programot, és várnánk a hibajelentéseket.
A legtöbb figyelmet érdemlő védelmi stratégia azonban a következő: el kell űzni a támadót, mielőtt még hozzáférhetne a sérülékeny rendszerekhez. Nyilvánvaló megoldás erre a tűzfal. A tűzfalakat azért készítjük, hogy megakasszuk a támadást. Az elérést korlátozó szerkezetek – mint a felhasználónév–jelszó sémák, az azonosító nyelvi egységek (token) és az intelligens kártyák (smart cards) – úgyszintén ebbe a csoportba tartoznak, hiszen feladatuk a megbízható és a nem megbízható felhasználó (azaz a lehetséges támadó) közti megkülönböztetés. Nem árt azonban tudni, hogy az azonosítási módszereket a gyenge pontok megerősítésére is felhasználhatjuk (például SecurID nyelvi egységeket használunk egy nem megfelelő jogosultságrendszerrel rendelkező webalkalmazás azonosítási rétegéhez). Mára legyen elég ennyi.

További érdekességek találhatók a 30. CD Magazin/Gyakorlati könyvtárban.

Mick Bauer (mick@visi.com) hálózati biztonsággal foglalkozó szaktanácsadó. 1995 óta a Linux elkötelezett híve, 1997 óta pedig OpenBSD-prófétaként tevékenykedik. Mick minden kérdést és megjegyzést szívesen fogad.

A Linux és a Samba egy országos laboratóriumban

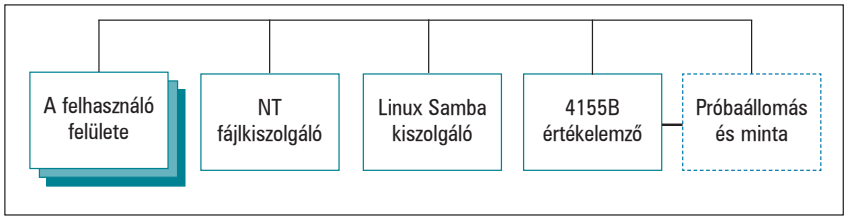
Az alábbiakban a Linuxnak és a Sambának a VCSEL-nek nevezett rendkívül kis méretű lézerek kutatásában történő felhasználásáról olvashatunk.

Nemrégiben a Linux és a Samba adott választ a marylandi Adelphiben található Hadi Kutatólaboratórium (ARL) igényeire. Intézetünk csúcstechnológiai kutatást végez a lézerek egy különleges fajtájánál, és ezen eszközök teljesítményének kipróbálása közben rendkívül nagy mennyiségű adatot gyűjtünk össze. A próbához használt felszerelésünket a hálózaton át rá tudtuk egy Samba kiszolgálóra kötni. Ennél a módszernél az a csel, hogy a beállítások miatt a felhasználók úgy látják, mintha az intézet NT-n futó fájlkiszolgálóján levő adatokat érnék el. Részletesen is el fogom magyarázni a felállást, de a kulcs az, hogy az NT-gépen egy hálózati parancsikont hoztunk létre, mely a Samba-megosztásra mutat, a linuxos gépet pedig a hálózaton láthatatlanná tettük. Az *ábra* a hálózat felépítését mutatja be.

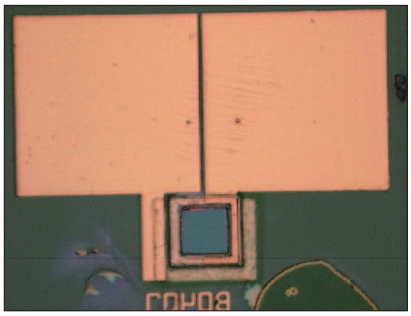
Intézetünk VCSEL-nek (felületi üreges függőlegesen sugárzó lézer) nevezett, rendkívül kis lézereket fejleszt, melyek a fénytani kutatás általános területébe tartoznak. Könnyen megesik, hogy egy négyzetmilliméternyi felületen több mint 60 lézert helyezünk el, és előfordul, hogy a lézereket tartalmazó lapka teljes átmérője mindössze 7,5 centiméter. Így hát megeshet, hogy egyetlen lapkán több ezer alkatrész található. A *1. képen* egy jellegzetes VCSEL látható. A legfőbb próbát, amelyet minden VCSEL teljesítményének ellenőrzéséhez lefuttatunk, az áramerősséget, a fényerőt és a feszültséget mérő ILV-görbének nevezik. Alapjában véve azt vizsgáljuk, hogy a befektetett energia mennyi fényt eredményez. Mivel az elemzőprogramok többsége a felhasználók asztali gépén található, szükségük van rá, hogy a feldolgozatlan adatokhoz onnan férjenek hozzá. A felhasználók a szokások rabjai. Az intézettel kapcsolatos adatok elérése mindig is azt jelentette, hogy el kell menni az NT-kiszolgálóra. Mivel a felhasználók hozzászoktak, hogy az adatokat az NT-s gépről kapják meg, nem akartuk rákényszeríteni őket, hogy mással kísérletezzenek. Igyekeztünk számukra mindent áttekinthetővé tenni, és azt a látszatot próbáltuk kelteni, mintha az NT-kiszolgálóról kapnák az adatokat. Azért, hogy a felhasználóknak az NT-s gépen keresztül kelljen menniük, a linuxos gépet a hálózatról nézve láthatatlanná tettük. Az adatokat elérő felhasználók azonosításában az NT-gép biztonságára támaszkodunk.

A kipróbálás beállításai

A VCSEL-ek jellemzésében két készüléknek jutott kulcsfontosságú szerep. Az első a mintavételező állomás, amely tulajdonképpen néhány apró szondával és egy fénymérővel egybeépített mikroszkóp. A szondák energiát bocsátanak az eszközre, mi pedig a fénymérővel megmérjük az áramot. A második készülék az Agilent gyártmányú 4155B típusú értékelemző. Az elemző úgy lett programozva, hogy pásztázza végig az áramerősség szintjét, valamint mérje meg a feszültséget és a fényerőt. Alapvetően két módon lehet vezérelni: a készüléken található kezelőszerveken és a GPIB-csatolón keresztül. Noha teljesen igaz, hogy a GPIB-kapu a tudományos berkekben népszerű csatoló, és mutatósabb tesztek elvégzését teszi lehetővé azáltal, hogy a próbabeállításokat számítógép vezérli, és az adatok összegyűjtésére is képes, azonban vezérlő számítógépünk a laboratóriumi helyszíntől mintegy ötlábnyira helyezkedik el, és nem lehet közelebb hozni. Emiatt nehéz elkezdeni a próbát, amikor a szondák a helyükre kerültek. Szerencsére fő tesztünket egyszerűen a készülék kezelőfelületén be lehet állítani. A próbát úgy szoktuk végrehajtani, hogy a szondákat a mikroszkóp nézőkéjének segítségével helyezzük el, óvatosan odanyúlunk és az értékelemzőn megnyomjuk a próbát indító gombot, majd pedig mentjük az adatokat. A *2. képen* a laboratórium felszerelése látható.



A hálózat felépítése



1. kép Jellemző VCSEL: a nagy téglalapok a próbát végző szondák érintkező felületei, a lézerrel besugárzott tényleges terület a kis szürke négyzet alul középen

Működés

Ha a próbát sikerült rendben lefuttatnunk, mentenünk kell az adatokat. A 4155B háromféle módon képes menteni az adatokat: GPIB, hajlékonylemez és TCP/IP. Az elemzőt nem GPIB-vel vezéreljük, ezért ez szóba sem jön. A hajlékonylemez támogatja a 3,5" lemezeket, de ezek a lemezek hamar megtelnek, és hurcolászni kell őket. Több laboratóriumi területen is dolgozunk, ezért előfordult már, hogy egy lépést újra kellett kezdenünk, mert épp eltűnt egy hajlékonylemez. Az általunk összeállított válasz a TCP/IP-támogatás alapján működik.

Linux

Az értékelemző támogatja a TCP/IP-t, pontosabban az NFS-t. Az elemzőt még pingelni is lehet. Be van jegyezve a laboratórium DNS-ébe, ezért IP-cím és