Peszleg Tibor
(informatikai szakértő)

Internetes önvédelem, avagy meddig terjedhet a passzív és az aktív védekezés a számítástechnikai rendszerek elleni támadások visszaverésére

1. Problémafelvetés

Ma hazánkban, de a fejlett világban is a legnagyobb veszélynek a leggyakoribb támadásoknak, ha csak a számszerűséget nézzük, akkor az informatikai rendszereket működtető személyek, szervezetek vannak kitéve. Ezek a támadások nem közvetlenül személyünket, életünket, testi épségünket fenyegetik, hanem vagyonunkat, személyes adatainkat, privátszféránkat. Az természetes, hogy ha valakit megtámadnak az utcán, életét, testi épségét, vagy vagyonát fenyegetik, akkor joga van az önvédelemhez, és ehhez akár eszközöket is igénybe vehet (önvédelmi fegyver, testi erő, stb.). Vagyonunk védelme érdekében passzív védelmet szokás kiépíteni (kerítés, megfigyelő-, beléptető rendszerek, stb.) és aktív védelemre, visszatámadásra nincs lehetőség. Az informatikában a technikai lehetősége megvan annak, hogy a rendszerünk ellen intézet támadást egy másik informatikai támadással megakadályozzunk. Dolgozatomban arra keresem a választ, hogy ez jogilag, illetve taktikailag megvalósítható-e, érdemes-e meglépni ezt a védekezési formát.

2. A támadások típusai

Az informatikai rendszerekbe épített védekezések kártékony programok, illetve gép és programhibák elleni védelmek. A támadásokat jellemzően ezek kihasználásával követik el. Honnan jöhetnek a támadások? Azt gondolhatnánk, hogy rendszerünket kívülről, az internet felől támadják meg. Statisztikák mutatják, hogy ez nem így van. A legveszélyesebb támadások általában nem az internet felől jönnek, hanem a belső hálózatunkból. Ezek lehetnek tudatos támadások, de lehet csak gondatlanság is. Gondoljunk arra, hogy hányszor helyezünk be egy hordozható memóriát a belső hálózat egy

gépébe, majd egy idegen számítógépbe, ezzel a kártékony programoknak lehetőséget adva megfertőzni a rendszert.

A támadásokat három kategóriába lehet sorolni. Az első és leggyakoribb az informatikai támadás, amikor is informatikai eszközökkel (programokkal) támadják meg az informatikai rendszert. Ezek a mindennapi gondolkodásunkban a hackereknek tulajdonított támadások, amikor valaki távolról, egy program vagy kód segítségével feltöri a számítógépünket. Nagy informatikai tudást igényel ennek a véghezvitele.

A következő, amikor a felhasználót tévesztik meg és ezáltal okoznak kárt a rendszerében. Ennek lényege, hogy a felhasználót veszik rá arra, hogy kiadjon olyan információt, mellyel kárt lehet okozni a rendszerében. Ennek egyik legtipikusabb példája az ún. adathalász támadás, amikor egy megtévesztő levéllel tudják meg a banki hozzáférési adatokat az ügyféltől és ezek felhasználásával lépnek be a számlájára és viszik el a pénzét.

A harmadik talán a legritkább, amikor magát az eszközt támadják, próbálják megsemmisíteni, megrongálni. Ezekben az esetekben nem képzett informatikusok végzik a támadást, és nem is az a céljuk, hogy információhoz jussanak, csak az eszköz működését akarják megakadályozni, az adatokat módosítani vagy éppen megsemmisíteni.

Egy nagyobb, fontosabb informatikai rendszer tervezésénél, kivitelezésénél, üzemeltetésénél mind a három támadásra gondolni kell. Nem véletlen, hogy az ilyen rendszerek szerverei jól őrzött, biztonságos szervertermekben találhatók, ellátták vírusvédelemmel, tűzfalakkal, behatolás-érzékelőkkel, és egyéb szoftveres védelemmel, valamint nagyon szigorúan szabályozzák azt is, hogy ki, milyen adatokhoz és programokhoz férhet hozzá

3. Mi a támadás?

A támadást a számítástechnikai, illetve a jogtudomány különböző módon definiálja. Más az informatikai támadás fogalma és más a büntetőjog által meghatározott támadás-fogalom. A büntetőjogi támadásnak mindenképpen aktív emberi magatartásnak kell lennie. Neki kell létrehoznia a kártékony programot, azt feltelepítenie a támadó gépére, elkészítenie és eljuttatnia az áldozatnak az adathalász levelet, vagy neki kell pl. tüzet okozni a szerverteremben, hogy ezáltal működésképtelenné váljon a rendszer. Passzív magatartás is lehet nagyon káros, de nem minősíthető támadásnak.

Jogi értelemben a támadásnak a jogrendszer által védett érdek ellen kell irányulnia. Ez jelentheti a személyek testi épsége vagy élete ellen irányuló támadást, pl. egy kórházi rendszerben a véradatbázisban tárolt adat megváltoztatását és ezzel, bizonyos feltételek fennállása esetén akár halált vagy súlyos egészségügyi következményeket, vagy akár egy közmű működésének olyan megváltoztatását, mellyel szennyezett víz kerül pl. a lakosság nagy tömegeihez.

Személyek elleni támadásnak minősül az is, és talán ez a leggyakoribb, ha a megtámadott méltóságában, jó hírnevén esik csorba a támadás következtében. Gondoljunk arra, ha valakinek az állami vagy intézményi informatikai rendszerben a bűnügyi adatait változtatják meg, vagy egyszerűen csak olyan információkat tesznek róla közzé, az internetet mint médiumot használva, amely sérti emberi méltóságát.

A személyek javai elleni támadás az egyik leggyakoribb támadási forma ezen a területen. Ide kell érteni, ha becsapják őket és ezzel informatikai rendszerben tárolt vagy vezetett bankszámláikról szerzik meg vagyonuk egy részét, vagy a rendelt áru ellenértékét nem fizetik ki, és sok más elkövetési magatartással is találkozhatunk.

A közérdek is ilyen védett érdek. Gondoljunk csak arra, hogy mindennapjainkban mennyire támaszkodunk az informatikára, annak pozitív, minden esetben biztonságos működése mennyire befolyásolja az életünket. Ha egy-egy rendszer nem megfelelően működik, akkor nem tudjuk egymással tartani a kapcsolatot, vagy nem megfelelően működnek az életünkben megszokott dolgok. Ez a bizalom, amit ezeknek a rendszereknek a biztonságos működésébe vetünk, nagyon kihat az életünkre. Ennek elvesztése akár komoly, állami, társadalmi szintű problémákhoz vezethet. Egy ország, társadalom életét jelentősen befolyásolhatja, ha pl. a választási rendszerét hackelik meg.

A jogi értelemben vett támadásnak van egy nagyon fontos kritériuma, amely csak az informatikai támadásokra érvényes, ez pedig az, hogy az informatikai rendszert védelmi intézkedéssel kell ellátni. Ez azt jelenti, hogy ellentétben a fizikai élettel, ahol nincs jogi kötelezettsége a megtámadottnak, hogy védje magát, itt csak akkor valósul meg a bűncselekmény, ha valamilyen szintű védelemmel ellátta az informatikai rendszerét. Ez a védelem nem meghatározott a jogban. Vannak, voltak olyan nézetek, melyek azt mondták, hogy csak akkor valósul meg a bűncselekmény, ha az informatikai rendszert megfelelő, a védeni kívánt érdeknek elvárható

védelemmel látják el. A mai joggyakorlat és a törvényszöveg ennek ellentmond és a legkisebb szintű védelmet is elfogadja. Úgy gondolom, hogy alapvetően el kell és lehet is fogadni ezt a hozzáállást és a megfelelő szintű védelmeket más jogszabályban kell előírni az üzemeltetők, felhasználók számára. (Ebben lehetne hasznos az előző kormányzat idején kidolgozott informatikai biztonsági törvény, mely öt szintben határozza meg az informatikai rendszerek biztonsági fokát és mindegyikhez megfelelő védelmi szintet ír elő. Kötelezően viszont csak a három legmagasabb szinten ír elő szabályokat. Az egyedi felhasználók és a következő szint számára viszont csak ajánlásokat fogalmaz meg.) Ez azt jelenti, hogy akár egy egyszerű jelszavas védelem feltörésével vagy megkerülésével is megvalósulhat a bűncselekmény.

Informatikai értelemben támadásról akkor beszélünk, ha úgy lépnek be egy informatikai rendszerbe, hogy annak a programnak a hibáját kihasználják, kártékony programkódot juttatnak a rendszerbe, vagy az adatokat manipulálják, illetve működését akadályozzák, vagy szabotázst követnek el a rendszer ellen.

A leggyakoribb hackertámadások mögött a programhibák kihasználása rejlik. Köztudomású, hogy tökéletes programot nem lehet készíteni, mivel a szoftverfejlesztők gazdasági érdeke az, hogy minél gyorsabban és költségkímélőbb módon készítsék el a programjaikat. Ez azzal jár, hogy bizonyos szükséges tesztelési fázisokat lerövidítenek vagy kihagynak. Természetesen nem feledkezhetünk meg arról sem, hogy ezek a programok nagyon sokszor több százezer vagy akár több millió sorból, kódból állnak, melyeket sok ember készít és ezekek a részeknek az összehangolása, tesztelése sem megoldható hiba nélkül. Napjainkban a világon sok ember foglalkozik azzal, hogy a különböző szoftverekben programhibákat találjon, és ezen emberek egy nagy része ezeket a megtalált hibákat nem a fejlesztőknek jelenti, hanem saját bűnös céljaira használja fel. Az interneten rákeresve nem egy oldalt találunk, ahol közzéteszik ezeket a hibákat, hogy azt bűnös szándékú emberek felhasználhassák. Ma már az interneten megtalálhatók olyan előre programozott eszközök, amelyek ezeket a programhibákat kisebb informatikai tudással is ki tudják használni, ezáltal a kezdő vagy az informatikában kevésbé jártas elkövetők kezébe eszközt adnak, hogy feltörhessenek rendszereket. Ezeket az eszközöket természetesen nem csak a hackerek használják, hanem az informatikai rendszert üzemeltető

személyek is, hogy teszteljék, biztonságosabbá tegyék az általuk üzemeltetett rendszereket.

Talán a legnagyobb veszélyt napjainkban a kártékony kódok informatikai rendszerbe való bevitele jelenti. Gondoljunk csak arra, hogy régebben, a '90-es évek elején még nem volt része az operációs rendszernek semmiféle védelmi program, míg napjainkban már vírusvédelmi program vagy kártékony programfelderítő szoftver is az operációs rendszer tartozéka. A számítógépes vírusok és azok különféle mutánsainak egyre gyakoribb megjelenése oda vezetett, hogy egy védelem nélküli számítógépet, ha az internetre kiteszünk, akkor kevesebb mint 20 perc alatt megfertőződik valamilyen vírussal, vagy kártékony programmal, még ha nem is használjuk, csak elérhető az internet felől. Ezek a vírusok, kártékony programok vagy a gép működését befolyásolják, annak erőforrásait akarják az elkövetők rendelkezésére bocsátani, pl. egy *bot*[137] hálózat részévé tenni, vagy adatokat gyűjtenek a számítógépről. Automatikusan felismerik, ha bankkártya-adatokat, bankszámla-adatokat tárolunk vagy küldünk a gépünkről, összegyűjtik a gépünkön lévő elektronikus levélcímeket és ezt továbbítják az elkövetőknek. Ezáltal lehetővé válik, hogy ezekre a postafiók címekre kéretlen elektronikus leveleket küldjenek, ezáltal is terhelve az informatikai hálózatokat, vagy a bankszámla-, bankkártya-adatainkkal visszaélve ellopják pénzünket. Természetesen ezeket a cselekményeket nem saját számítógépükről követik el, hanem a kártékony programokkal kiépített bot-hálózatuk segítségével.

Mind az államigazgatás, mind a cégek életében nagyon nagy veszélyt jelent, ha informatikai rendszerükbe nem megfelelő adatokat visznek be vagy az ott tárolt adatokat megváltoztatják. Gondoljunk csak arra, hogy egy-egy hamis átutalási megbízás egy bank rendszerében milyen károkat tud okozni. Ezt meg tudja tenni egy alkalmazott is, akinek jogosultsága van ilyen adatokat bevinni a rendszerbe, de megtehető kívülről is, ha megszereznek a korábban vázolt módon egy ilyen jogosultságot. Ezzel a módszerrel megváltoztatható akár egy jól működő rendszer tevékenysége és a hibás adatok miatt gazdasági vagy akár más kár is keletkezhet.

Ma már szinte háborús eszköznek tekinthetjük azokat a technikákat, amivel egy-egy informatikai rendszer működését akadályozhatjuk meg vagy

---

[137] A *botnet* csoportosan vezérelhető botok hálózata. A botok (vagy zombik) olyan számítógépek, amelyek a tulajdonos tudta nélkül távolról irányíthatók. Az irányítás egy csatornán keresztül történik, amely lehet IRC, web vagy P2P alapú. Forrás: Hun-CERT (http://www.cert.hu/index.php?option=com_content&task=view&id=34&Itemid=205)

szabotálhatjuk. Gondoljunk csak a pár évvel korábban Észtország ellen végrehajtott DDos[138] támadásra, melynek következményeként az észt közigazgatás és a nagybankok elektronikus működése több napra megbénult. Ugyanezzel találkoztunk az orosz-grúz konfliktus idején is. Ilyenkor tulajdonképpen önmagukban szabályos műveleteket hajtanak végre a az informatikai rendszerek, de olyan nagyságrendben, hogy azt már nem tudják kezelni és túlterhelődnek, lelassulnak, majd végül leállnak, működésképtelenné válnak. Ezekkel a technikákkal találkoztunk már nem csak államok közötti „hadviselésben", hanem a mindennapi életben is. Gazdasági társaságok, akár hitelrontás, akár egy-egy akciós időszak miatt is szenvedtek el ilyen támadásokat. Ilyenkor csak az a támadók szándéka, hogy akár véglegesen, akár csak egy-egy időszakra megbénítsák az adott informatikai rendszer működését. Hazánkban is nem egy alkalommal találkozhattunk már ilyen támadással, akár az üzleti szférában, akár az államigazgatás ellen.

Mint láthatjuk, az informatikai rendszerek nagyon kiszolgáltatottak ezen támadásoknak, és az ellenük való védekezés nagyon nehéz, jelentős károkat tud okozni. A problémát fokozza az is, hogy ellentétben a való életbeli támadásokkal, itt az elkövetők felderítése és elfogása sokkal nehezebb. Gondoljunk csak arra, hogy az internet nemzetközisége miatt mennyi jogi és technikai nehézséggel kell szembenézni, azokat megoldani, hogy az elkövetőt azonosítsuk. Arról nem is beszélve, hogy azok az adatok, amelyekkel dolgoznánk, a felderítés során mennyire változékonyak: nem is percről percre, hanem a másodperc tört része alatt megsemmisülhetnek, megváltozhatnak.

Ilyenkor sok esetben a sértett fél, nem minden alap nélkül úgy gondolja, hogy nem érdemes eljárást kezdeményeznie, mert úgy sem tudják felderíteni a hatóságok az elkövetőt, neki viszont nagyobb anyagi, erkölcsi kára származik az eljárásból, mintha titokban tartaná az ügyet. Egyesek megpróbálnak egy-egy ilyen támadás első jelére jogos önvédelemre

---

[138] A DDoS az angol *Distributed Denial of Service*, azaz *elosztott szolgáltatás-megtagadással járó támadás* rövidítése. A DoS-támadások alkalmával egy szervert olyan sok kéréssel bombáznak, hogy a rendszer a feladatokat egyszerűen nem képes ellátni, és legrosszabb esetben összeomlik. Ilyen módon támadtak már ismert szervereket, mint az Amazon, Yahoo, eBay, a normális adatforgalom több mint négyszeresével, és így egy bizonyos időre a normális kérések számára üzemen kívül helyezték. Forrás: biztonsagosbongeszes.hu
(http://www.biztonsagosinternet.hu/node/42)

hivatkozva a támadó eszközeit felhasználva megállítani a támadást, vagy annak kárát minimalizálni, csökkenteni, a támadást visszaverni.

4. Az ellentámadás feltételei

Ezen visszatámadásnak milyen feltételei vannak? Először a technikai feltételeket nézzük meg. A visszatámadás legelőször is nagyfokú és speciális szaktudást igényel. Bár az ilyen nagy rendszerek üzemeltetői között nagyon sok a jó biztonsági szakember, de nem azonos oldalon állnak az elkövetővel. Egész más a mentalitásuk, gondolkodásuk, máshogyan, más oldalról ismerik a programokat. Ide, erre a feladatra olyan szakemberekre van szükség, akik támadni tudnak, nem pedig védekezni. Gondoljunk csak a focira. Ott is vannak külön támadó játékosok és védők. A jégkorongban egész sorokat cserélnek le a feladatnak megfelelően. Mások játszanak, ha védekezni kell és mások, ha támadni. Nagy rendszerek üzemeltetésénél megoldható, hogy ilyen szakembereket is foglalkoztasson a megrendelő, de gazdaságilag már nem biztos, hogy költséghatékony lenne ez a megoldás.

Szintén hasonló a gond a másik technikai alaptételnél, a gazdaságossági szempontnál. Ez a technikai feltétel pedig az, hogy a támadáshoz egy másik a védekezőhöz se jogilag, se technikailag vissza nem vezethető, csak a támadásokra használt informatikai hálózatot kellene fenntartani, üzemeltetni. Ez önmagában is már egy vagy több büntetőjogi tényállás megvalósulását jelentené, mert a gyakorlatban ehhez egy *bot*-hálózatot kellene létrehozni. Ezt sem jogi, sem gazdasági, sem presztízs-érdekből nem teszik meg a nagyobb üzemeltetők.

Amit megtehetnek jogilag és technikailag is, és véleményem szerint meg is kell tenniük, az az, hogy folyamatosan figyelik a támadásra utaló informatikai és nem informatikai jeleket és felkészülnek azok elhárítására. Minden támadásnak lehetnek előjelei. A legegyszerűbb *portscan*-től[139] kezdve a komolyabb hálózati puhatolásokon át, egészen az adathalász támadásoknál

---

[139] A *port scanning*-et hackerek alkalmazzák annak felderítésére, hogy milyen szolgáltatások futnak a gépünkön. Sok rendszerellenőrző program is használja ezt a technikát az elemzéshez. A scannelő valószínűleg arra kíváncsi, melyik szolgáltatást kihasználva tudna betörni gépünkre. Forrás: Linux szerverek biztonsága.
(http://dvhc.uw.hu/php/article.php?artid=f515fa3b407aebbf&rovat=Hack&rovat_sub=Linux:)

használt *strómangyűjtésig*[140] nagyon sok minden. Ezeket a biztonsági szakemberek már ismerik és használják. Nem véletlenül beszélek itt már biztonsági szakemberekről és nem informatikai szakemberekről. Ez a fajta védekezés már nem csak informatikai ismereteket, hanem ennél komplexebb biztonsági ismereteket jelent. Itt már nem csak a hálózatot, hanem az alkalmazottakat, a humán erőforrást, a gazdasági helyzetet is figyelni, elemezni kell, de akár egy társadalmi esemény, vagy politikai helyzetbeli változás is figyelmet érdemel.

Ahhoz, hogy ez az állandó készenlét és helyzetelemzés használható legyen egy visszatámadásnál, az is szükséges, hogy a visszatámadáshoz folyamatosan készenlétben legyenek azok az eszközök, melyeket alkalmazni szeretnénk. Ez pedig elég nehéz és költséges, mivel egyszerre több támadásra is fel kell készülnünk. Gond az is, hogy ha azt akarjuk, hogy ezek a visszatámadások hatékonyak legyenek, akkor még időben kell azokat alkalmazni.

A technikai feltételek után nézzük meg a jogi feltételeket is egy ilyen visszatámadáshoz. Első és legfontosabb feltétel, hogy csak azonosított támadóval szemben alkalmazhatjuk ezt a módszert. Itt nem arra kell gondolni, hogy ismerjük a támadó személyazonosságát, vagy azt, hogy ki áll a támadás mögött, ki annak a „megrendelője", hanem hogy konkrétan azonosítjuk, milyen gépekről, IP-címekről érkezik a támadás. Ezekben az esetekben soha nem személy ellen támadunk vissza, soha nem az a cél, hogy a támadó személyét tegyük ártalmatlanná, hanem az, hogy a támadó gépeket kiiktassuk, azok működését tegyük lehetetlenné, illetve szerezzünk a gépekről olyan információt, bizonyítékot, mely a konkrét személy beazonosításához segíthet minket. Technikai értelemben könnyű ezeket a gépeket azonosítani, de a tapasztalat azt mutatja, hogy a támadók szinte minden esetben bot-hálózatokat használnak fel, hogy saját magukat elrejtsék. Ilyen esetekben nem az elkövető gépeit tennénk működésképtelenné, hanem ezeket a bitként használt, ún. zombi-gépeket.[141] Csak egy példa arra, hogy ez

---

[140] A csalók által gyűjtött személyek, akik a csalásról nem tudva segítik az elkövetőket a számláikra átutalt összeg kézpénzben való felvételben és azt más, jellemzően westernunion csatornán külföldi személyeknek átutalni. Ők a magyar törvények szerint a pénzmosás gondatlan alakzatát követik el.

[141] Az on-line bűnözők egy vírus segítségével egyszerre számos számítógép felett átvehetik az irányítást; ezek „zombikká" alakulnak, melyek együttesen „botnetként" végzik a káros tevékenységet. Az akár 100000 „zombiszámítógépből" álló botnet hálózatok levélszemetet és vírusokat terjesztenek, vagy megtámadhatnak más számítógépeket és kiszolgálókat és mást kárt is okozhatnak. Forrás: Microsoft Corporation
(http://www.microsoft.com/hun/protect/computer/viruses/zombies.mspx)

mennyire veszélyes lehet. A 2006 telén több magyar bankot is érintő adathalász-támadásnál az egyik beazonosított számítógép, amelyet felhasználtak a támadásnál, a New York-i metró egyik szervergépe volt. Elképzelhetjük, milyen problémát okozott volna, ha ezt a gépet működésképtelenné tette volna valamelyik bank biztonsági szolgálata.

Ezzel el is jutottunk a következő jogi feltételhez, mégpedig ahhoz, hogy a visszatámadás csak akkor lehet jogszerű, ha a támadót érinti és nem egy másik kívülálló személyt, informatikai rendszert. Ez sajnos technikailag szinte megvalósíthatatlan, mert csak a visszatámadott számítógépéről szerezhetők be olyan adatok, melyek bizonyítják, hogy ki volt a tényleges támadó. Természetesen nagyobb kárt nem okozhatunk, mint amekkora kára keletkezne megtámadottnak.

A fentiek figyelembevételével milyen visszatámadási módok jöhetnek szóba? Elsősorban a támadó gépének működésképtelenné tétele, ellene egy DoS- vagy DDoS-támadás lefolytatása. Ez igen gyors és hatékony megoldás lehet, csak nagyon nehéz, szinte lehetetlen időben megtalálni azokat a számítógépeket, melyekről a támadásokhoz felhasznált bot-hálózatokat irányítják. Azokban az esetekben lehet ez célravezető és jogilag is elfogadható, ahol nagyobb, komolyabb hálózatot támadnak meg és az elkövetők semmiféle, vagy csak nagyon egyszerű álcázást használnak, viszont az ilyen támadások más módszerekkel egyszerűbben és költséghatékonyabban is kivédhetők.

A másik ötlet az, hogy a megtámadott a támadó számítógépét feltörve, arról adatokat, programokat töltsön le, majd állítsa le a támadó gépet, hogy így bizonyítékokat nyerjen az elkövetésre nézve, egyben megakadályozva a támadást. A fenti probléma itt is megállapítható: szinte lehetetlen egy komolyabb támadásnál az elkövető beazonosítása, vagy ha mégis beazonosítható a támadó, akkor a támadás más módszerekkel sokkal könnyebben kivédhető lenne.

Ezek után nézzük meg, hogy milyen előnyökkel és hátrányokkal járna egy ilyen visszatámadás. Előnyei közt kell mindenképpen említeni, hogy ha sikeres és pontos a visszatámadás, akkor megelőzhetünk vele nagyobb károkozást. Ha időben hajtjuk végre, akkor szinte minimális kárt szenved a megtámadott rendszer, vagy akár az egész támadást megelőzhetjük vele. Szintén nagy előnye még a jól végrehajtott ellencsapásnak az is, hogy ezzel bizonyítékokat tudunk szerezni a támadóról, annak céljairól, indítékairól, valamint a saját védeni kívánt rendszerünk gyenge pontjairól, amit a támadó

ki akart használni. Ezzel is fokozni tudjuk a jövőbeni biztonságunkat, valamint ezeket az adatokat átadva a hatóságoknak az elkövető felkutatása és elfogása is biztosabbá válik. Ennek nem csak a mi esetünkben van jelentősége, hanem az egész informatikai biztonság szempontjából preventív hatása van.

Hátrányai közt kell megemlíteni, hogy drága és kockázatos. Drága abból a szempontból, hogy nagy humán- és technikai erőforrásokat kell folyamatosan készenlétben tartani. Kockázatos abból a szempontból, hogy az egyre felkészültebb támadók egyre jobban rejtik magukat és nem tudhatjuk, hogy nem okozunk-e nagyobb kárt és ezzel követünk-e el mi magunk is bűncselekményt annak anyagi kockázatát is a nyakunkba véve, mint ami minket ért, vagy érhetne. Kockázatos abból a szempontból is, hogy ha nem időben alkalmazzuk, vagy túl későn, akkor nem tudjuk minimalizálni a kárt. Mindenképpen meg kell említeni, hogy az általunk megbízott rendszerbiztonsági szakemberek a mi rendszerünket is megismerik, és a rendszer gyenge pontjainak kiszivárogtatásával nagyobb veszélynek is kitehetjük magunkat, ha mások jobban megfizetik a rendszertesztelésre megbízott „szakembereinket", hackereinket. Legvégül azt az erkölcsi kockázatot említeném meg, amelynek veszélye fennállhat akár egy jól kivitelezett visszatámadás, akár egy balul elsült visszatámadás során, ha ezek a visszatámadások nyilvánosságra kerülnek. Ezeket a módszereket nagyon nehezen tolerálják még a törvénytisztelők is, még ha a kiváltó okot meg is értik. Nem szabad elfeledkezni arról, hogy ilyenkor mi magunk is megvalósítunk egy-két törvényellenes magatartást, mely a Btk.-ban megfogalmazásra került. A civilizált világban a visszatámadás csak törvényi felhatalmazás alapján, nagyon szigorú szabályok szerint tehető meg, és csak kivételes esetben adatik meg magánszemélynek, vagy szervezetnek. A védekezési célú visszatámadás jellemzően állami monopólium.

Hátránya mindezek mellett, hogy hatásosan csak kevés és kis súlyú támadással szemben lehet alkalmazni, melyek más módszerekkel olcsóbban és kockázatmentesen kivédhetőek.

A fentiekből megállapítható, hogy csak kivételes esetekben lehet ezt a fajta védekezést használni eredményesen és törvényes keretek között.

5. Hogyan védekezzünk?

A legfontosabb a folyamatos felkészülés, amelyet az informatikai biztonsági szakma is hangsúlyoz. Mindig napra, sőt percre készen tartsuk karban az általunk használt informatikai rendszer minden elemét. Úgy a hardver-elemeket, mint a szoftvereket, de ne feledkezzünk meg a humán erőforrás, vagyis az ember naprakészen tartásáról sem. Folyamatosan frissítsük a programokat, tűzfalakat, vírusirtókat, kártékony programok elleni védelmünket. Készítsük el és folyamatosan aktualizáljuk a szabályzatokat, amelyekben lefektetjük a hozzáférési jogosultságokat, a biztonsági teendőket.

A következő nagyon fontos teendőnk, hogy fejlesszük informatikai rendszereinket anyagi lehetőségeinkhez és az általunk védett rendszerben lévő adatok értékéhez képest. Ne feledjük el, hogy a technika, az emberi tudás fejlődik, és a másik oldal is folyamatos fejlődésen megy keresztül, úgy technikailag, mint tudásban fejleszti magát.

Nagyon fontos, hogy ha elkészítettünk egy jó informatikai rendszert, a hozzá való szabályzatokkal, illetve felkészítettük azokat a személyeket is, akik használják ezt a rendszert, ezeket folyamatosan ellenőrizni kell és az így kapott eredményeket ki kell értékelni és beépíteni a további munkánkba.

Nagyon fontosnak tartom az együttműködést is, amely előre jelezheti a támadásokat, vagy ha már bekövetkezett a baj, akkor annak elhárításában tud segíteni. Ennek egyik jó példája a CERT-ek[142] együttműködése, amelynek segítségével törvényesen meg tudunk oldani olyan feladatokat is, amelyeket egyébként önállóan csak a fent említett visszatámadással tudnánk. Nem egy adathalász támadásnál, vagy DDoS-támadásnál a CERT-hálózatok nemzetközi együttműködése segítségével lehetett a támadó számítógépek működését leállítani.

Legfőképpen viszont az oktatást tartom szükségesnek minden területen: az informatikai biztonsági szakemberek és a felhasználók körében is, és tapasztalatom szerint jogalkalmazók (bűnüldözők, ügyészek, bírák) kiegészítő oktatására is nagyon nagy szükség lenne.

---

[142] A Computer Emergency Response Team (CERT) Feladata, hogy a tagszervezeteinél (internet-szolgáltatók) előforduló hálózati incidensek felderítésénél, elemzésénél és kezelésénél segítséget nyújtson. További célja a biztonsági tudatosság növelése. Ez utóbbi tevékenység nem elsősorban nem a hivatásszerűen számítástechnikával foglalkozókat célozza meg, hanem az ISZT tagok nagyszámú felhasználóinak kíván olyan információt nyújtani, amely képessé teszi őket az Internet használatával együttjáró kockázatok minél teljesebb megértésére és a sikeres védekezésre. Lapjainkon rövid ismertetők, hosszabb tanulmányok is megtalálhatók, valamint a különböző rendszerek, alkalmazások sebezhetőségéről olvashatnak híreket. Forrás: Hun-CERT (http://www.cert.hu/)