Betörések, betörési kísérletek II. avagy ki nevet a végén?

A sorozat előző tagjából megtudhattuk, pontosan milyen következményekkel jár az, ha valaki egy számítógépét vagy számítástechnikai rendszerét megpróbál feltörni. Most azokról a (jogi)eszközökről lesz szó, melyekkel egy ilyen csibészt (ckrackert) nyakon lehet csípni.

Mindenek előtt nem árt definiálni, hogy mit is ért a jog számítástechnikai rendszer alatt:

„Számítástechnikai rendszer minden olyan berendezés, amely közvetlen emberi beavatkozás nélkül (automatikusan) végez adatfeldolgozást, azaz adatok bevitelét, kezelését, tárolását, továbbítását látja el. A számítástechnikai rendszerek körébe tartoznak a számítástechnikai adatfeldolgozásra épülő, memóriával rendelkező olyan egységek is, amelyek megjelenésükben nem hagyományos számítógépet jelentenek.
A számítástechnikai rendszer fogalma azonban nemcsak az egyes berendezésekre terjed ki, hanem felöleli az azok összekapcsolása révén létrejött hálózatot, valamint az adattovábbítást, a kapcsolatfelvételt biztosító műszaki berendezéseket is." [1]

Ennek értelmében, ha mondjuk pár év múlva valaki betörve az intelligens hűtőszekrényembe rendel nekem 15 karton tejet, pontosan ugyanezt a bűncselekményt fogja elkövetni – feltéve persze, hogy addig nem változtatják meg a tényállás elemeket.

A betörés felfedezése

Függetlenül attól, hogy az elkövető a rendszerünkbe belépve milyen mértékű kárt okoz, azzal, hogy a rendszert feltörte, már megvalósította a számítástechnikai rendszer elleni bűncselekmény tényállásának valamennyi elemét. Feltétel persze, hogy a rendszerünknek legyen legalább valamilyen minimális szintű védelme (hardver- vagy szoftver-alapú tűzfal), hogy azt jogosulatlan belépéssel, kijátszással vagy más módon meg lehessen sérteni.

Alapszint

Rendszergazdaként belépve azt tapasztaljuk, hogy valaki az éj vagy a bitek leple alatt bejutott a rendszerünkbe, és tallózta a könyvtárainkat.[2] Annak nincs nyoma, hogy bármiféle változtatást eszközölt volna, vagy adatokat másolt volna le. Ilyenkor az eljárás, (azt követően, hogy a rendszerünket újra biztonságossá tettük például másik típusú tűzfal telepítése, trójai kereső program lefuttatása... stb.) hogy a korábban már begyűjtött naplóbejegyzéseket, illetve a visszakereshető ip címet lementjük (lehetőleg egy olyan gépre, ami nincs hálózatra kötve, hogy esetleg a visszatérő garázda ne leljen rá).
Az e módon kigyűjtött információkat – egy ismeretlen tettes elleni feljelentés keretében – eljuttathatjuk az illetékes ügyészhez vagy nyomozóhatósághoz.

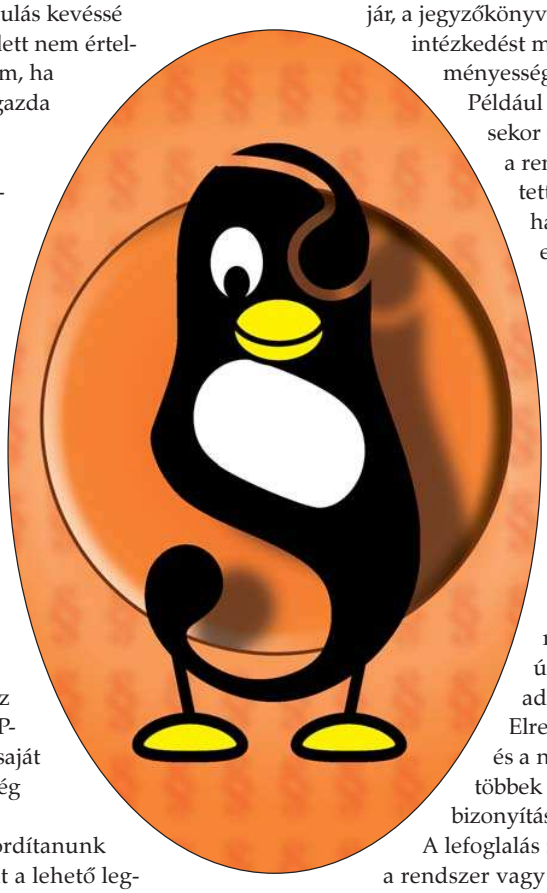
Középszint

A betörő jogosulatlanul belépett, jelenleg is bent tartózkodik, és éppen a ***szupertitkos*** feliratú mappánk tartalmát próbálja meg letölteni. A probléma leggyorsabb megoldásaként válasszuk le a gépet a netről. Ez esetben az elkövető észre fogja venni, hogy jelenlétére felfigyeltek, és talán soha többé nem próbálkozik meg a rendszerünkkel.
Ha a szupertitkos felirat azonban csak mindenféle kacatot rejtett, melyeket épp csalinak helyeztünk el ezen a gépen, akkor a helyzet persze merőben más. Amennyiben a rendelkezésünkre álló adatok alapján megtudtuk az elkövető ip címét, megkereshetjük a cím szolgáltatóját, és megkérdezhetjük, az előfizető nevét. Ezzel akár a későbbiekben eljáró nyomozó hatóság munkáját is segíthetjük, hiszen ebben az esetben már nem ismeretlen tettes ellen kell nyomozást folytatniuk.
Fontos tudni, hogy a párbajok ideje a XIX. századdal lejárt, nem megoldás az, ha a betörő kilétének felderítése érdekében mi is megpróbáljuk feltörni a minket ostromló rendszerét, hiszen akkor ugyanúgy jogosulatlan belépésre teszünk kísérletet vagy adott esetben, ha az akció célravezető, mi is elkövetővé válunk. Figyelemmel arra, hogy a Büntető

[1] Complex CDJogtár Btk. 300/F§ Kommentár részlet.
[2] Linuxos rendszerben ennek is marad nyoma, windows használata esetén pedig tételezzük fel, hogy így tett.

törvénykönyv nem nevesíti a „hirtelen felindulásból elkövetett számítástechnikai rendszer védelmét biztosító technikai rendszer kijátszását," mint tényállást – így e bűncselekmény elkövetésénél az erős felindulás kevéssé beszámítható. Jelen feltételek mellett nem értelmezhető jogos védelemként az sem, ha a büszkeségében sértett rendszergazda bosszút áll.

A nyomozóhatóságnak azonban – szemben a haragos rendszergazdával – lehetősége van rá, hogy külön engedély keretében titkos adatszerzést végezzen, ennek érdekében meghatározott számítástechnikai rendszer védelmét biztosító technikai intézkedéseket kijátsszon.



„Hajjaj" szint

Az elkövető belépve a gépünkre – azon kívül, hogy garázdálkodott az adataink között, – megnyitott pár portot, melyeken át a mi gépünk ip címét használva ostromol már hálózatokat.

Ez az eset mind közül a legsúlyosabb, itt mindenképpen javasolt az internetszolgáltatók (a kiderített IP-cím szolgáltatója csakúgy, mint a saját szolgáltatónk) valamint a rendőrség értesítése.

Itt különösen nagy gondot kell fordítanunk arra, hogy a betörés körülményeit a lehető legprecízebben dokumentáljuk (Adott esetben tanúk jelenlétében készített jegyzőkönyvekkel, melyeket a betöréssel kapcsolatosan tudtunkra jutott információhoz mellékelünk.)

Miért van mindez?

1. Értesíteni kell a betörő ip címét adó szolgáltatót a betörés körülményeiről is, hogy adott esetben saját hálózatán belül megpróbálhassa visszakeresni az elkövetőt.

2. Értesíteni kell a saját szolgáltatónkat, illetve azokat a szolgáltatókat akik felé a gépünkről kísérletet indítottak, hogy felhívhassák ügyfeleik figyelmét a veszélyre.

3. Értesíteni kell a rendőrséget, mert jó eséllyel előfordulhat, hogy a tőlünk indított kísérletet valaki más bejelenti az ügyészségen vagy a nyomozóhatóságnál, elkövetőként a mi ip címünket jelölve meg.

A feljelentés sorsa

A feljelentést elsődlegesen nyilvántartásba veszik. ***Megvizsgálják, hogy a*** történeti tényállás bűncselekmény gyanújának megállapítására alkalmas-e, ***a*** büntetőeljárás megindításának van-e akadálya, szükséges-e halaszthatatlan nyomozási cselekmény vagy más intézkedés foganatosítása, a bűncselekmény nyomozására van-e hatásköre, illetékessége.

A nyomozó szerv a Büntető eljárásról szóló törvény szerint köteles már a feljelentés vételekor, illetőleg a nyomozó szerv tagjának észlelésekor – ha a késedelem veszéllyel jár, a jegyzőkönyv felvétele előtt is – minden olyan intézkedést megtenni, amely a nyomozás eredményességét, gyors teljesítését elősegíti. Például amennyiben a betörés észlelésekor és bejelentésekor az elkövető a rendszerben tartózkodik, és tettenérhető, helye lehet azonnali házkutatásnak. Indokolt lehet ezen „gyorsított eljárás" azért is, mert ennek későbbi elvégzése az eljárás eredményességét károsan befolyásolhatja.

Lefoglalás

A lefoglalás jogászi nyelven: a bizonyítás érdekében a dolog birtokának elvonása a birtokos rendelkezése alól. Külön érdekes részlet, hogy a lefoglalás kapcsán a törvény már külön nevesíti a számítástechnikai rendszernek vagy ilyen rendszer útján rögzített adatokat tartalmazó adathordozónak a lefoglalását. Elrendelésére a bíróság, az ügyész és a nyomozóhatóság jogosult, többek között akkor, ha az adott tárgy bizonyítási eszköz.

A lefoglalás menete a következő: először is a rendszer vagy adathordozó birtokosát illetve az adat kezelőjét fel kell szólítani, hogy a keresett dolgot adja át, illetőleg a számítástechnikai rendszer útján rögzített adatot tegye hozzáférhetővé. (Tehát a nyomozóhatóság az internetszolgáltatót is kötelezheti valamennyi általa ismert információ kiadására). Amennyiben ezt önként nem teszi meg, rendbírsággal (általában 1000-200.000 forint közötti összeg) sújtható, kivéve a terheltet és azt, aki a tanúvallomást megtagadhatja, illetőleg aki tanúként nem hallgatható ki. (Tehát ha az elkövető takarítónőjét találják otthon a házkutatásra érkező rendőrök, aki makacs módon nem akarja átadni a gépét, rá kiszabhatnak rendbírságot, de ha maga az cracker van jelen, akkor ő, mint terheltet nem lehet megbírságolni). Fontos azonban tudni, hogy az átadás megtagadása egyik esetben sem lesz akadálya annak, hogy a keresett dolgot, illetőleg a számítástechnikai rendszer útján rögzített adatot házkutatással, illetve motozással megszerezzék.

A nyomozást általában annak megindulását követő 2 hónapon belül befejezik. Ez alatt az idő alatt vagy lehull a lepel vagy a tettes örökre ismeretlen marad.

Dr. Dudás Ágnes (dudas.agnes@abend.hu) ügyvédjelölt, az FSF egyik aktivistája. 2004-ben végzett az ELTE Jogtudományi Karán. Szakdolgozatát a szoftverek szerzői jogi védelméről írta, a 2003-as évet pedig e terület kutatásával a berlini Humboldt Egyetemen töltötte.