dr. Parti Katalin

Úti jelentés

a **Current Issues in IT Security – An Interdisciplinary Conference** c. konferenciáról

2009. május 12. és 15. között Freiburgban a Max Planck Institut für ausländisches und internationales Strafrecht ismét megrendezte az informatikai biztonságról szóló, interdiszciplináris konferenciát, amelyen technikai szakemberek és kriminológusok vettek részt.

A konferencia négy fő tárgy köré összpontosított:

1. Az informatikai biztonság technikai kérdései (pl. notebook-biztonság, etikai hacking, a Max Planck Intézet számítástechnikai rendszerének felépítése és az adatok biztonsága, GSM biztonság – mobiltelefonok lehallgathatósága, laikusok IT biztonságért való felelőssége).
2. A jövő technikai vívmányai, lehetőségei (pl a jövő tűzfala)
3. A jövő cyber-bűncselekményei (pl. kritikus infrastruktúrák – közérdekű üzem, pl. közlekedés – elleni támadások, cybercrime mint szervezett bűnözés, vállalatok elleni támadások és statisztikai mérhetőségük, SMS-chat csalás).
4. Kriminológiai kérdések (pl. az állami büntető igény érvényesítéséhez fűződő érdek és a magánszféra tiszteletben tartásának határai, a morális pánik összetevői és a veszély-érzékelés megváltozása az internet-kommunikáció mindennapossá válásával, a jogalkotás túlreagálása a cyber-veszélyekre).

A konferencia fő tanulságai a következők:

- Továbbra is érvényes az a közkeletű megállapítás, hogy a vállalatok nagy része nem érzékeli az ellen indított támadásokat, ezekre csak utólag derül fény. A detektált támadásoknak is csak kb. 23-24%-át jelentik a CERT[1]-eknek. Ez megnehezíti, illetve lehetetlenné teszi a nyomozást, ill. a nemzetközi együttműködést. Gátolja a megelőző stratégiák kidolgozását és ilyen intézkedések megtételét is. További probléma, hogy a CERT-ek és a nyomozó hatóságok között kezdetleges, illetve véletlenszerű az együttműködés,

[1] CERT – Computer Emergency Response Team

egyedül Dél-Koreában ismeretes ilyen együttműködés, mégpedig az elkövető számítógépének azonosításában segít a CERT.

- Úgyszintén változatlanul érvényes a nemzetközi együttműködés buktatójaként ismert tény, amely szerint a nyomozó hatóság olyan banális kihívásokkal kell hogy megküzdjön, mint az elektronikus adatok lefoglalhatósága, vagy alternatívaként az adatok megőrzésére kötelezés. A nemzetközi együttműködés még mindig nem folyik olajozottan, első sorban a nehézkes ügyintézés miatt. Az államok igyekeznek megőrizni szuverenitásukat, ez akadályozza az együttműködés formális feltételeinek megteremtését, így a hivatalos megkeresési útvonalak járatlanok, lassúak.
- Marco Gercke (Kölni Egyetem) ötleteket adott arra, hogy a jövőben milyen sebezhető pontok ellen lehet elkövetni cyber-támadásokat. Ilyen a közérdekű üzem, mint pl. a közlekedés elleni támadás, ami jelentheti a közlekedési lámpák egyszerű működésképtelenné tételét. Felvázolt egy futurisztikus képet, amikor a személyautókban a fedélzeti számítógép szenzorja érzékeli majd az elsőbbséget élvező járművel közeledését és figyelmezteti a vezetőt a lehúzódási/lassítási kötelezettségre. Ebben a helyzetben, mivel több lesz a számítástechnika által vezérelt gép, több lehetőség adódik a közlekedés biztonságába való jogellenes beavatkozásra is. így pl. magukat a járműveket is irányítása alá vonhatja a hacker, ami könnyen közlekedési káoszhoz vezethet, mivel az emberek leszoktak a saját 5 érzékszervük használatáról és úgy hiszik, maximálisan megbíznak a gépben. Ehhez hasonló az a mai jelenség, amikor a személygépkocsi lopásérzékelője meghibásodik, ez blokkolja a zárakat és a kocsi indítórendszerét is. Tehát, elemi funkciók meghibásodása az egész járművet használhatatlanná teheti – ráadásul a tulajdonosa által (is). Gercke kiemelte, hogy mindenekelőtt statisztikai adatokat kell gyűjteni mind a sikeres, mind a sikertelen támadásokról, hiszen ez teszi lehetővé a számítástechnikai rendszerek hibáinak felfedését és kijavítását. David Wall (Leeds-i Egyetem) ezt annyival egészítette ki, hogy a szervezett bűnözés természetének megértéséhez nemcsak a technikai, de egyéb, pl. a szociológiai, a kriminológiai, a politikai biztonsági réseket is elemezni kell, mert csak így kaphatunk hiteles képet erről az összetett jelenségről.

- Wall felhívta a figyelmet a cyber-bűncselekmények mértékének eltúlzására, ugyanakkor alulbecslésére is („cybercrime is overreported and underreported at the same time"). A feljelentett támadásokat a média megszellőzteti, így lesz a kevés, nyilvánosságra hozott bűncselekményből óriási botrány-légballon.
- Ehhez kapcsolódott az előadásom, amely arról szólt, hogy az információs forradalmak hatására közelebb érezzük magunkhoz a veszélyt. De a morális pánik nemcsak az egyéni percepciókból és a média hírközpontú természetéből táplálkozik. Összetevői között van a tudomány, amely a pánikhelyzetet – annak létét, ontogenezisét, következményeit stb. – kutatja és maga a jogalkotás is, amely mindenkor megpróbál megfelelni a társadalom és a politika elvárásainak. A közelmúlt nemzetközi jogalkotási gyöngyszemeit hoztam fel annak szemléltetésére, hogy a büntetőjog egyre inkább olyan jelenségek ellen kíván védelmet nyújtani, amelyre tudottan nincs, nem lehet hatással. Ilyen pl. a gyermekpornográf weboldalak elérésének kriminalizálása, amelyre az Európa Tanács Lanzarote egyezménye (CETS. No. 201) hív fel, és amelynek bevezetésére legújabban a német törvényhozás tett kísérletet.[2]
- Ales Zavrsnik (Ljubljanai Egyetem) megerősítette az igazságszolgáltatás „túlreagálását" a cyber-bűncselekményekkel kapcsolatban. Megjegyezte, hogy nem célszerű olyan törvényeket hozni, amelyek szembe mennek az általános mértékkel, hiszen ez már nem a prevenciót szolgálja, hanem teljes társadalmi csoportok (pl. a file-letöltők) kriminalizálásához vezet.
- Az SMS-chat csalás manapság igen elterjedt meggazdagodási lehetőség. Könnyű munka és nehezen deríthető fel, tehát valószínűleg igen nagy a látencia az ilyen típusú cselekményeknél. Ez egy randi-SMS-szolgáltatás, amely emeltdíjas. Egy számítógépre futnak össze az SMS-ek és mindegyikre egy személy – az elkövető – válaszol, különböző álneveken. Fontos a változatosság, hiszen egyes „randizók" több különböző potenciális partnert is megkeresnek. Hogy hány különböző stílusban képes randi-SMS-hirdetést feladni, majd pedig a beérkező ismerkedő SMS-ekre válaszolni az elkövető, az az egyéni kreativitásától függ. Az SMS-chat működési elve hasonló a phishinghez, amikor a megtévesztett felhasználók adatait egy távoli szerver – botnet – gyűjti össze, majd a felhasználók bankszámláiról leemelt összegek

[2] http://de.news.yahoo.com/2/20090325/tts-eckpunkte-zur-bekaempfung-von-kinder-c1b2fc3.html

„megtisztítására” ismeretlen személyeket toboroznak az interneten, aki aztán az általuk továbbított – „mosott” – pénzösszeg egy részét megtarthatják. Az előbb ismertetett esetek rámutatnak a cyber-csalások ún. hosszú farok természetére („long tail effect”), aminek lényege, hogy sok kis összeg különböző személyektől kicsalva nehezebben érzékelhető és felderíthető, mintha egyetlen nagyösszegű csalást követnének el.

- A jövő biztonságtechnikájában egyre nagyobb szerepet játszanak a laikusok, az egyszerű felhasználók. Minél bonyolultabb egy biztonsági rendszer, valójában annál inkább a laikus felhasználókon múlik a biztonság megőrzése. A vállalatnak azonban, amely egy ilyen bonyolult biztonsági rendszert épít ki, tekintettel kell lenni e a felhasználók befogadó kapacitásának végességére. Pl. egy bank nem építhet ki szuperbiztonságos online beléptetőrendszert, mert ez elrettenti az egyszeri felhasználókat (bonyolult kezelhetőség, a „kelleténél” több felhasználóazonosító). Éppen ezért a bankoknak a nagymama-tesztet kell alkalmazniuk beléptetőrendszereik teszteléséhez. („The granny-test”: ha a nagymamád megérti a rendszert – és képes megjegyezni is – akkor alkalmazható, egyébként felhasználóellenes és a felhasználók elhagyják az online bankfiókot.)
- Ugyanakkor kérdés, hogy manapság ki számít laikusnak és ki az igazi szakember – a kérdést úgy is feltehetnénk, hogy mit kell tudni a laikusnak (is) a biztonság megőrzéséhez? Ez a dilemma az igazságügyi informatikai szakértő és a nyomozó vonatkozásában is felmerül. Mi az, amit egy nyomozónak minimálisan el kell tudnia végezni a lefoglalt számítástechnikai adathordozón és milyen munkát kell már a szakértőre bíznia? Egyre speciálisabb területei fejlődnek ki a számítástechnikának, így nem mindegy, hogy az egyes kérdések vizsgálatára milyen IT-szakértőt rendelnek ki. Ez a kérdés annak ellenére feltehető, hogy a Be. mindenhol hitelességet kíván meg a bizonyításhoz, ehhez pedig okvetlenül szükséges valamely IT-szakértő bevonása a büntetőeljárásba, hiszen a bíróság csak azt fogadja el bizonyítékként, amit IT-szakértő vizsgált. A szakértői vizsgálat egyfajta garancia az adatok és az adathordozóról tett megállapítások hitelességére.

Budapest, 2009. május 27.

Dr. Parti Katalin