ÚJ KORSZAK – RÉGI-ÚJ KIHÍVÁSOK

NEW ERA – OLD AND NEW CHALLENGES

KESZTHELYI ANDRÁS LÁSZLÓ egyetemi docens
Óbudai Egyetem, Keleti Károly Gazdasági Kar

ABSTRACT

The importance of the human factor in IT security increases day by day. As a cliché the weakest chain in the security, i. e. the human factor, is to be strenghened by different regulations, including the law and the different regulations, e.g. IT security regulations. These regulations contain a large number of rules, regarding the technical and organisational aspects as well as the supposed and forbidden activities in typical situations. In the background we can find trust: we believe that the regulations are good enough and that most of our fellow creatures will keep them well enough. The aim of this paper is to investigate the relationship between trust, security and publicity by analysing IT security incidents.

Bevezetés

A biztonságtechnikában egyre nagyobb szerepe van az emberi tényezőnek. A közhelyszerűen leggyöngébb láncszem erősítésére szolgálnak a különféle szabályok, az állami törvényektől a különféle – pl. informatikai biztonsági – szabályzatokkal bezárólag. Ezek számos előírást tartalmaznak a technikai, műszaki, szervezési kérdésekre vonatkozóan ugyanúgy, mint a típusos helyzetekben elvárt, illetve tilalmazott magatartási formákra vonatkozóan. Mindezek mögött meghúzódik azonban a bizalom: elhisszük, hogy a szabályok elegendően jók, és hogy embertársaink számunkra releváns részhalmazai azokat elegendően pontosan be is tartják. Ezen tanulmány célja a bizalom és a biztonság kapcsolatának vizsgálata különböző biztonságot érintő incidensek elemzésével, s ezek kapcsán a nyilvánosság szerepével.

Bizalom a mindennapokban

Mindennapi életünk, a legegyszerűbb hétköznapokban is egyszerűen élhetetlen lenne bizalom nélkül. Nem nehezen élhető, hanem élhetetlen. Egy totalitárius rendszerben vagy egy maffia-környezetben megtanulható (és igen gyorsan megtanulandó), hogy megválogassuk, kivel miről és hogyan beszélgethetünk, és hogy vannak olyan területek, amelyek az „ez nem telefontéma” halmazba tartoznak. Ez

a helyzet, ha messze is van az ideális állapottól, kezelhető. Többek között azért, mert csak az élet egy adott területét érinti. Nézzünk azonban további példákat.

Megbízom a szüleimnek vélt emberekben annyira, hogy elhiggyem: valóban az ő gyermekük vagyok, valóban abba a családba tartozom, anélkül, hogy genetikai vizsgálattal bizonyíttatnánk ezt a tizennyolcadik születésnapunkon. Ha kimegyek az utcára, többé-kevésbé megbízom a többi közlekedő embertársamban, hogy betartják a közlekedési szabályokat (ún. bizalmi elv). Használok bankkártyát, ennek során megbízom a bankban és a kereskedőben, hogy nem lopják el a pénzemet – pontosabban a bankrendszerben és annak felügyeletében. A példák sorát hosszasan lehetne folytatni.

A bizalom nélkül nemcsak egyénként nem tudnánk létezni, de társadalmunk is összeomlana. Ez az általános bizalom annak ellenére fennáll, hogy mindannyian ismerünk ellenpéldákat.

2013-ban a görög rendőrség nemzetközi segítséget kért egy, Falsala közelében lévő cigánytáborban talált gyermek személyazonosságának megállapításához, miután DNS-vizsgálat mutatta ki, hogy nem áll rokonságban az őt nevelő párral. (MTI, 2013.)

A józsefvárosi önkormányzat 2014-ben közel félmilliárd forint közlekedési bírságot rótt ki csak a Harminckettesek tere felől a körútra jobbra szabálytalanul bekanyarodó autósokra. (Zách, 2015.) A Rezesova-ügyről nem is beszélve.

2015-ben a Quaestor és a Buda-Cash botrányában többszáz milliárd forint tűnt el. (HVG, 2015/A.) Az „évszázad bankrablásában" nagyjából egymilliárd dollárt zsákmányoltak a leleményes netbűnözők. (Kaspersky, 2015.)

Az ellenpéldák sorát hosszasan lehetne folytatni.

A számos ismert ellenpélda dacára az általános bizalom többé-kevésbé fennáll. Ezt az teszi lehetővé, hogy az egyes területek biztonsága az egyének és a közvélekedés számára elfogadható mértékű. A komplex rendszerek, legyenek biológiaiak vagy társadalmiak, együttműködés nélkül hosszú távon működésképtelenek. Schneier (2013.) rámutat arra a logikus körülményre, hogy bár minden ilyen rendszerben vannak potyautasok, mind a rendszer működőképessége, mind a potyautasok túlélése szempontjából lényeges, hogy ezek nem lehetnek „túl sikeresek". Ha mégis, az a rendszer összeomlását eredményezi: a gazdaszervezet pusztulásával a rákos sejtek is elpusztulnak, ha egy piacon túl sok a tolvaj, akkor az emberek nem fognak odamenni vásárolni, és a tolvajoknak nem lesz kitől lopniuk.

Vegyük sorra napjaink ún. információs társadalmának néhány bizalmi kihívását az alábbiakban, az erre vonatkozó sajtóhírek – nyilvánosságot kapott esetek – alapján.

SSL/TLS tanúsítványok a böngészésben

Ahogyan a személyi számítógépek és az internet egyre inkább a mindennapok részévé vált, úgy merült föl az igény a biztonságos kommunikáció megvalósítására. Enélkül ugyanis az üzleti felhasználás – vásárlás a hálózaton, fizetés, net-

bank stb. – elképzelhetetlen. Az adatforgalom biztonsága azt jelenti, hogy nemcsak maga az adatforgalom kell titkosított legyen (ne lehessen lehallgatni és/vagy megváltoztatni az ügyfél és a netbank közötti adatforgalmat), hanem az ügyfélnek abban is biztosnak kell lennie, hogy valóban a saját netbankjának a honlapjával forgalmaz, nem pedig egy, arra teljes mértékben hasonlító kalózoldallal.

Az ehhez szükséges kétkulcsos (aszimmetrikus) titkosítás matematikai alapját az 1977-ben fölfedezett RSA-eljárás adja (Rivest, 1983.), ami lehetővé teszi az adatforgalom titkosításán túl a kiszolgáló hitelesítését is. Ezen az alapon fejlesztették ki az SSL-t (secure socket layer – biztonságos szoftvercsatorna réteg, 1996). Később átnevezték: TLS (transport layer security – biztonságos szállítási réteg), illetve gyakran SSL/TLS lett belőle.

Ennek lényege, hogy a hiteles kiszolgáló gépnek van egy tanúsítványa, ami nem más, mint egy szabványos szerkezetű dokumentum, ami tartalmazza – többek között – a gép nevét és nyilvános kulcsát, s ezt a dokumentumot digitálisan aláírta a tanúsítványkibocsátó (CA – certificate authority). A tanúsítványkibocsátó cég nyilvános kulcsa a böngészőkben gyárilag benne kell legyen, hogy digitális aláírásukat ellenőrizni lehessen.

Ezen a területen a bizalomnak számos vonatkozása van. Ezek közül a legfontosabb, hogy megbízom abban, hogy a tanúsítványkibocsátó a tanúsítvány kiadásakor elég gondosan ellenőrzi a tanúsítványt igénylő személyazonosságát és jogosultságát. Ellenkező esetben ugyanis ha Ambrus Attila igényelhet (és kaphatna!) tanúsítványt – mondjuk – a *.otpbank.hu kiszolgálónévre, akkor fölösleges lenne fegyverrel követelni egy-egy bankfiókban a pénzt.

Megbízom továbbá a böngészők fejlesztőiben, hogy csak „rendes” tanúsítványkibocsátók nyilvános kulcsait építik bele a böngészőjükbe. Meg kell bíznom a szoftverek fejlesztőiben, hogy elég alapos, jó minőségű munkát végeztek az e területen (is) használt programok tervezése és fejlesztése során. Megbízom a rendszer üzemeltetőiben, hogy az elvárható gondossággal üzemeltetik az érintett szolgáltatást, hogy a tanúsítvány védelmében végzett tevékenységemet és forgalmazott adataimat nem teszik ki veszélynek.

Előfordultak – és valószínűleg fognak is – olyan események, amelyek pont ezen bizalmat aknázzák alá. Ez olyasmi, mintha valaki képes lenne – illetéktelenül – közjegyzői szárazbélyegzővel és aláírással ellátni papírdokumentumokat.

2011-ben a Turktrust nevű török tanúsítványkiadó cégnél egy hibás üzleti folyamat eredményeképpen kerültek ki inkorrekt tanúsítványok. (Ducklin, 2013/A)

2013 elején a Google hamis tanúsítványokat fedezett föl, amelyeket a francia DG Trésor bocsátott ki a Google valamely doménnevére (Ducklin, 2013/B), lehetővé téve ezáltal azok megszemélyesítését illetéktelenek számára.

A Stuxnet vírus is – amelyet az iráni urándúsítási program akadályozására fejlesztettek ki – hamis tanúsítványokat használt föl arra, hogy saját hiteles eszközvezérlő mivoltát bizonyítsa. (Cserháti, 2011), többek között a holland DigiNotartól szerzett digitális aláírásokkal (Kormányzati, 2012). A DigiNotar digitális aláírásait

felhasználva perzsa felhasználók Google-hozzáférését is sikerült feltörniük a tetteseknek – ennek esetleges következményei akár beláthatatlanok is lehetnek, lehettek.

Ezen titkosítási eljárás feltörhető a megfelelő kulcsok hiányában, legalábbis elméletileg. Azaz a matematikai eljárás ismert, a nehézséget az elvégzendő számítás mennyisége jelenti: túl nagy számok prímtényezős felbontása reménytelen mennyiségű erőforrást igényel. Ha azonban a támadónak pl. tudomása van arról, hogy a kulcsgenerálásnál alkalmazott véletlenszámok esetleg nem teljesen véletlenszerűek, az jelentősen javítja a hatékonyságát.

Az amerikai nemzetbiztonsági hivatal (NSA) évente hozzávetőleg 250 millió dollárt fordít a különféle titkosítási szabványok oly módon való alakítására, hogy a rendelkezésére álló számítási teljesítménnyel esélye legyen matematikailag törni a biztonságosnak hitt titkosításokat is. (Greenwald, 2013.)

Az Edward Snowden kiszivárogtatotta dokumentumokból megtudjuk, hogy az RSA vállalat egy, mindössze tízmillió dolláros üzlet fejében nem elég megbízható véletlenszámgenerátort épített be a termékeibe. (Gálffy, 2013.)

A tanúsítványok ellenőrzését végző programkódokbam is találtak olyan programozási hibát, amely jogosan veti föl azt a kérdést, hogy az lehetett-e egyáltalán hiba, nem volt-e esetleg szándékos cselekedet. (Ducklin, 2014.) (Goodin, 2014.)

Ilyen pl. a Heartbleed hiba, ami lehetővé tette a sérülékeny rendszerekből a titkos kulcs nyomok nélküli megszerzését. (CVE 2014.)

Az idei év elején került nyilvánosságra, hogy az amerikai és a brit titkosszolgálatok sikeresen betörtek a holland Gemalto rendszerébe, és ellopták a titkosításhoz használatos kulcsokat. (Scahill 2015.) A Gemalto a világ egyik legnagyobb SIM-kártya gyártó vállalata, amely évente kétmilliárd SIM-kártyát állít elő. Ez lehetővé teszi a mobilhívásokhoz való szabad hozzáférést az érintett szervek számára.

Jelszavaink

A felhasználók hitelesítésének ősidők óta ismert módja a jelszavak alkalmazása. A jelszó tudás alapú felhasználóazonosító, azon alapul, hogy csak a jogosult felhasználó ismerheti az adott jelszót. Sokan és sokat írtak a jelszavakkal kapcsolatos tudnivalókról, közöttük a jelen tanulmány szerzője is (Keszthelyi, 2013.) Ezek többnyire és elsősorban a felhasználókra vonatkozó szabályokat taglalják, azonban a szolgáltató felelősségét sem hagyhatjuk figyelmen kívül. Felhasználóként ugyanis – jó esetben – a felhasználói általános szabályokat betarthatjuk ugyan (jelszóhossz stb.), de nincs ráhatásunk arra, hogy vajon a szolgáltató az elvárható gondossággal jár-e el: meg kell bíznom benne, hogy igen. Talán a legalapvetőbb üzemeltetői szabály, hogy a felhasználói jelszavakat nem szabad tárolni még titkosított formában sem, csak a jelszavakból képzett ellenőrző összeget (hash, olyan függvény, amelynek nincs inverze), amelyekből az eredeti jelszavak nem állíthatók helyre.

Az Adobe Systems 2013-ban egy év alatt háromszor is elszenvedett jelentős (presztízs)veszteséggel járó eredményes támadást. Ezek során a vállalat felhasz-

nálói adatbázisa a támadók kezébe került. Mivel az Adobe sajnálatos módon a felhasználói jelszavakat titkosítva tárolta („sózott" hash helyett), így a támadók aránylag könnyen hozzájutottak a jelszavakhoz is. (Ducklin, 2013/C.) Ennek közvetlen következménye az egyes felhasználók jelszavainak megismerésén túl – a statisztikailag értékelhető felhasználói halmaz okán – az általános jelszóhasználati szokások megismerése és további, más támadások során való felhasználhatósága. Fokozatosan, több lépésben vált ismertté ugyanis, hogy valójában legalább 150 millió felhasználói adatot sikerült ellopniuk a támadóknak.

A nyár végén az Ashley Madison nevű szolgáltatót törték föl sikeresen, és mintegy negyvenmilliós felhasználói adatbázist szereztek meg a támadók. Tíz nap alatt tizenegy millió felhasználói jelszót sikerült helyreállítani, ugyanis a jelszavak egy részét ma már korszerűtlennek számító módon kezelte a szolgáltató. (Ducklin, 2015

Saját személyes tapasztalatom, hogy a Telenor Magyarország is tárolja az ügyfelek MyTelenor jelszavait. 2014 tavaszán egy üzemzavar kapcsán tévesen feltételeztem, hogy a jelszavamra vagy rosszul emlékszem, vagy esetleg azt valaki (jogosulatlanul) megváltoztatta. Az elfelejtett jelszó szolgáltatással legnagyobb meglepetésemre nyílt elektronikus levélben elküldték a korábban használt jelszavamat. Arra a levelemre, melyben fölhívtam a figyelmüket a problémára, érdemi választ mindmáig nem kaptam.

Szolgáltatók

A felhasználók joggal várnák el, hogy a különféle szolgáltatók tisztességesen, ügyfeleik alapvető érdekeit nem sértve és nem veszélyeztetve járnak el, még akkor is, ha maga a szolgáltatás ingyenes, vagy legalábbis nem pénzzel fizetünk érte. Megbízunk bennük, esetenként sajnos alaptalanul.

Legelső, és leginkább elgondolkodtató példa a Sony rootkit esete. 2005 októberének végén került napvilágra, hogy a Sony BMG Music Entertainment olyan zenei CD-ket hozott forgalomba, amelyek – ha a CD-t számítógépen hallgatták – egy olyan programcsomagot telepített a felhasználó gépére észrevétlenül, amely egyrészt adatokat küldött a Sonynak, másrészt pedig lehetővé tette, hogy a felhasználó gépének irányítását – ugyancsak tudta és beleegyezése nélkül – távolról valaki átvegye. Az igazi kérdés azonban nem az, hogy a Sonyban (vagy bármely más zenei, szórakoztató stb. cégben) megbízhatunk-e, hanem az, hogy a víruskeresők fejlesztőiben megbízhatunk-e. Ugyanis a világhírű víruskeresők egyike sem jelezte a kártékony szoftver jelenlétét, amíg Mark Russinovich nyilvánosságra nem hozta felfedezését, és utána is csak jelentős késéssel, továbbá elfogadhatatlan módon reagáltak: eleinte a kártevőt nem, csak annak álcázását távolították el. (Schneier, 2005.)

Nagy keresőcégek, a Google, a Yahoo, a Microsoft, továbbá a Vodafone 2007 elején nyilatkozatot adott ki arról, hogy a továbbiakban „egy bizonyos határ alá nem mennek a cenzúrát alkalmazó országokban" (Berta, 2007.) Ez különösen annak fényében érdekes, hogy korábban oly módon működtek együtt pl. a kínai

hatóságokkal, ami emberi jogi aktivisták bebörtönzéséhez is vezetett. Megbízunk-e bennük?

2014-ben bíróság elé állítottak egy ausztrál férfit, és „olyan szexuális bűncselekményért ítéltek el, aminek valójában nem volt áldozata. A férfi egy kilencéves kislánnyal, Sweetie-vel fajtalankodott webkamerán keresztül, ami bőven kimeríti a pedofília fogalmát – csak éppen ez a kislány soha nem is létezett. Sweetie nem létező személy, csak egy megtévesztésig élethű számítógépes modell, amit egy fiatal filippínó lányról mintáztak. Látszólag valódi, de operátorok csetelnek helyette. Sweetie mostanra körülbelül ezer pedofilt buktatott le; az üzemeltetők elküldték az adataikat a hatóságoknak." (Hegyeshalmi, 2014.) (Crawford, 2014.)

A Magyar Telekom Nyrt. bizonyítottan érdeklődött a Hackint Team nevű olasz cégnél különféle kémprogramok beszerzésével kapcsolatban (Gálffy, 2015.)

Egy ideje tudjuk, hogy a Facebookot a betörők is felhasznál(hat)ják célpontjaik kiválasztásánál. Újdonság, hogy komoly formában fölmerült a polgároknak a Facebookon adott kapcsolati hálójának értékelése a banki hitelbírálat során. (HVG, 2015.) A Facebook másik érdekessége, hogy a felhasználóinak ún. árnyékprofiljuk is van, illetve lehet – és ez olyan személyes adatokat is tartalmazhat, amelyeket maga a felhasználó sosem adott meg a Facebook számára. (Oravecz, 2012.)

Emberi tényező

Közhely, de igaz: minden biztonsági rendszer leggyöngébb láncszeme az ember. Ezen belül legalább három területet különböztethetünk meg, és mindegyik különböző módon és mértékben érinti a bizalom és a biztonság problémáját.

Az első terület a hétköznapi élet rutinja. A megszokott napi tevékenységeinket begyakorolt automatizmusok irányítják. Kocsinkban a lámpa és az ablaktörlő ki-bekapcsolója (vagy akár a pedálok sorrendje) megszokott dolog: használatuk nem igényel előzetes töprengést. Ez így normális, enélkül nem tudnánk létezni sem. Viszont éppen ezért ez hatékonyan kihasználható a biztonságot érintő (megkerülő) célok esetében. Ha egy reflexszé vált tevékenységsorban valaki egyetlen elemet ügyesen és nem túl feltűnően megváltoztat, jó esélye van arra, hogy a célszemély, vagy akár nagy tömegek is átsiklanak fölötte. Jó példája ennek a Kurnyikova-vírus, ami azt használta ki, hogy a „pont-jpg" végződésről mindenkinek a képek jutnak eszébe.

Ezen reflexszerűségek kihasználásának általánosítása és tudományos szintre emelése az ún. „social engineering" – általánosan elfogadott magyar fordítása nincs, a legegyszerűbben az „átverés" szó fejezi ki a lényegét. Igen tanulságos példája, amikor Stavridis tengernagy beosztottjainak adatait a tengernagy nevében egy hamisított Facebook-profillal szerezték meg. (Lewis, 2012.)

A már érintett programozási (és esetleg egyéb, szakmai területeket érintő) hibákat (Ducklin, 2014.) (Goodin, 2014.) (CVE 2014.) az emberi tényező kapcsán is említeni kell.

Mivel ez a terület alapvető emberi tulajdonságokra alapoz, jóval nehezebb általános érvényű állásfoglalást megfogalmazni. Iránymutatásként, kiindulásként abban talán egyetérthetünk, hogy más a felelőssége egy „mezei" felhasználónak és egy rendszergazdának.

A mindenkori hatalom

A mindenkori hatalom a számára adott és elérhető lehetőségekkel élve törekedett és törekszik saját polgárainak a megfigyelésére. Napjainkban a terrorizmus elleni harc zászlaja alatt próbálja meg elfogadtatni azt az álláspontot, hogy a biztonságért cserébe a magánélet, általában a szabadság egy részével kell fizessünk. Hogy ez mennyiben érinti a mindenkori hatalomba vetett állampolgári, személyes bizalmunkat, azt mindenkinek saját magának kell megválaszolnia.

A telefonok lehallgatása, lehallgathatósága már a vezetékes telefonok korában is közismert gyakorlata volt az akkori hatalomnak. A mobiltelefonok korában sincs ez másképpen. „Az NSA globális lehallgatási gyakorlatát nyilvánosságra hozó 32 éves IT-szakember szerint semmit nem tehetünk az ellen, hogy a telefonjaink a titkosszolgálatok eszközeivé váljanak, akár a tudtunk nélkül is (...) Az NSA például egymilliárd dollárt költött erre..." (NYG, 2015.) A mobiltelefonok lehallgatásának egy másik eleme a fentebb már említett tanúsítványlopás a Gemaltótól.

Ugyancsak a mobiltelefonok lehallgatását (is) érinti az olasz Hacking Team nevű, kormányzati felhasználásra kémprogramokat fejlesztető cég, illetve a Gamma International feltörése: nyilvánosságra került rengeteg részletes adat arról, hogy mely kormányok milyen szoftvereket rendeltek ezen cégektől, s ezen szoftverek milyen eszközöket adnak a szóban forgó kormányok kezébe a mobiltelefonok lehallgatásához. (Voith, 2015.)

Visszatérően tesz kísérleteket az amerikai kormány arra vonatkozóan, hogy a különféle titkosításokat megvalósító programokba a fejlesztők kötelesek legyenek olyan hátsó kapukat beépíteni, amelyek felhasználásával a kormányzati szervek könnyen hozzáférhetnek az elvileg titkosított adatokhoz, adatforgalomhoz. (Bolcsó, 2015.)

A Skype hosszú időn keresztül híres volt arról, hogy erős titkosítással védetten biztonságos kommunikációt tesz lehetővé P2P alapon két számítógép között. Aztán 2011-ben a Microsoft megvette a Skype-ot, mintegy 8,5 milliárd dollárért, s evvel vége is lett a lehallgathatatlanságnak. „A német Heise Security szerint a Microsoft beleolvas a Skype-on keresztül zajló beszélgetésekbe és a redmondi cég szerverei meglátogatják a chaten küldött URL-eket is." (Bodnár, 2011.)

A bizalom, a biztonság és a nyilvánosság

Jogosan merül föl a kérdés, hogy a nyilvánosság milyen szerepet játszik a fenti, vagy azokhoz hasonló esetekben. Vajon elősegíti a nagyobb biztonságot, ennélfogva erősíti a bizalmat, avagy épp ellenkezőleg: a bizalom megrengetésével

gyengíti azt. Ezen a ponton Edward Snowden neve merül föl elsősorban, s az a kérdés, hogy szerepe vajon pozitív, vagy ellenkezőleg: elítélendő.

A biztonság ugyanis gazdasági-pénzügyi kérdés – is. A vállalatok alapvető, általános célja profitot termelni: növelni a bevételeket, és csökkenteni a kiadásokat. Ezért a vállalatok általános esetben a piaci környezet által elvárt minimumot áldozzák a biztonságra. Nem azért fog a vállalat – példának okáért – tűzfalszoftvert vásárolni és üzemeltetni jelentős költséggel, mert annyira eltökélt ügyféladatainak a védelmében, hanem mert ha nem teszi, az esetleg bekövetkező biztonsági incidenst követő kártérítési pereket el fogja veszíteni, hiszen nem követte az iparági legjobb gyakorlatot, nem az adott helyzetben általában elvárható gondossággal járt el.

Mi a teendő akkor, ha valaki kihasználható sebezhetőséget talál egy programkódban? Általános esetben a tisztességes eljárás az, ha értesíti a szoftver fejlesztőjét felfedezéséről, elősegítve így a hiba mielőbbi kijavítását, végső soron a biztonság erősítését. Mi a teendő akkor, ha az értesített fejlesztő úgy gondolja, hogy neki nem éri meg a hiba kijavítására áldozni? Ilyen esetre példa a közelmúltból, amikor a HP Zero Day Initiative javítatlan hibát találtak az Internet Explorerben. A sebezhetőség feltehetően elég súlyos lehet, ha a Microsoft 125 ezer dollárt fizetett az azt felfedező szakembereknek. Mivel gazdasági megfontolásokból a Microsoft nem tervezte a hiba javítását, a ZDI nyilvánosságra hozta azt. (Woody, 2015.)

Egy ilyen lépés vagy rákényszeríti a fejlesztőt arra, hogy eredeti szándékát megmásítva mégis javítsa a feltárt hibákat, vagy pedig lehetővé teszik, hogy a felhasználók védekezhessenek ellene, aminek a legegyszerűbb módja, hogy nem használják az adott szoftvert, szolgáltatást.

A Sony rootkit (l. fentebb) esetében is döntő szerepe volt annak, hogy nyilvánosságra került annak léte, különösen annak fényében, hogy a nagy hírű víruskeresők egyike sem mutatta ki annak jelenlétét, eltávolításáról nem is beszélve.

Ha jobban belegondolunk, a nyilvánosság hiteles tájékoztatása általában bizalomerősítő hatású, legalábbis ha követi a hibák kijavítása, a problémák elhárítása. Ha a vállalatok erre maguktól nem hajlandók, akkor a törvényhozásé lehet a döntő szó. Kalifornia az első állam, amelyben törvény kötelezi a vállalatokat, hogy személyes adatok (bármilyen módon történt) elvesztése esetén tájékoztassák erről a nyilvánosságot. (Schneier, 2010.)

Schneier úgy érvel (Schneier, 2010.), hogy a biztonság, így a bizalom irányába tehető igen jó lépés a teljes körű nyilvánosságra hozatala a biztonsági hibáknak. A szoftvercégek számára a programjaik sebezhetősége ugyanis externália. Csak akkor fog erőforrást áldozni a javítására, ha a helyzet kezelésének ez a legolcsóbb módja (pl. mert az eltitkolás lehetetlen). A felelősségteljes közzététel (amikor a fejlesztő cég időt kap a hiba javítására a nyilvánosság tájékoztatása előtt) alapja pedig az, hogy a nyilvánosságra hozatal és a tényleges tájékoztatás veszélye ugyanakkora. (Schneier, 2010.)

A nyilvánosság mellett van egy másik, igen hatékony tényező is. Vegyük példának a tanúsítványok fentebb részletezett problémáit: miért is merünk netbankolni,

ha a technológia végül is sérülékeny? Azért, mert a szabályok szerint az esetleges károkért a bank felel (hacsak nem az ügyfélnek felróható módon következett be). A bank választja ki és üzemelteti az alkalmazott technikát, a körülmények folytán a bank van abban a helyzetben, hogy érdemben javíthatja a biztonsági szintet: a felelősség és a hatékony cselekvés lehetősége együtt jár.

Összegzés

Mint láttuk, a biztonság és a bizalom egymást feltételezik, egymás nélkül nem léteznek.

A bizalmat, következésképp a biztonságot tehát erősíteni kell. Ebben az oktatás (szakmai ismeretek) és a nevelés (etikai ismeretek) szerepe, végső soron a biztonság kultúrája (Lazányi, 2015/A., 2015/B.) megkérdőjelezhetetlen, a kívánt eredmény elérésében a nyilvánosság szerepe pedig legalább annyira hatékony eszköz, mint a felelősség. A költő és hadvezér Zrínyi Miklós mondja: „Bízzál, de nézd meg kiben, mert szépen szól, esküszik (...) ez mind cselfogás lehet az te fejedre és a tieid veszélyére.” (Pilch, 1936.)

FELHASZNÁLT IRODALOM

A honlapok elérhetőségét 2015. október 14-20. között ellenőriztem.

Berta, J. (2007). Google, Yahoo, Microsoft – közösen az emberi jogokért, SG, 2007.01.20., https://sg.hu/cikkek/49877/google_yahoo_microsoft_kozosen_az_emberi_jogokert

Bodnár, Á. (2011). A Microsoft megvette a Skype-ot, HWSW, 2011.05.10., http://www.hwsw.hu/hirek/46667/microsoft-skype-voip-telefon-felvasarlas.html

Bolcsó, D. (2015). Nincs olyan, hogy biztonságos hátsó ajtó, Index, 2015.07.29., http://index.hu/tech/2015/07/29/titkositasi_haboru_megfigyeles_terrorveszely_szemelyes_adatok/

Crawford, A. (2014). Webcam sex with fake girl Sweetie leads to sentence, BBC, 2014.10.21., http://www.bbc.com/news/technology-29688996

CVE database (2014). 2014.04.08. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160

Cserháti, A. (2011). A Stuxnet vírus és az iráni atomprogram, in: Fizikai Szemle, 2011/5. p/pp. 150-155.

Ducklin, P. (2013/A). The TURKTRUST SSL certificate fiasco – what really happened, and what happens next?, Naked Security – Award-winning computer security, news, opinion, advice and research from SOPHOS, 2013.01.08., https://nakedsecurity.sophos.com/2013/01/08/the-turktrust-ssl-certificate-fiasco-what-happened-and-what-happens-next/

Ducklin, P. (2013/B). Serious Security: Google finds fake but trusted SSL certificates for its domains, made in France, Naked Security – Award-winning computer security, news, opinion, advice and research from SOPHOS, 2013.12.09., https://nakedsecurity.sophos.com/2013/12/09/serious-security-google-finds-fake-but-trusted-ssl-certificates-for-its-domains-made-in-france/

Ducklin, P. (2013/C). Anatomy of a password disaster – Adobe’s giant-sized cryptographic blunder, Naked Security – Award-winning computer security, news, opinion, advice and research from

SOPHOS, 2013.11.04., https://nakedsecurity.sophos.com/2013/11/04/anatomy-of-a-password-disaster-adobes-giant-sized-cryptographic-blunder/

Ducklin, P. (2014). Anatomy of a „goto fail" – Apple's SSL bug explained, plus an unofficial patch for OS X!, Naked Security – Award-winning computer security, news, opinion, advice and research from SOPHOS, 2014.02.24., https://nakedsecurity.sophos.com/2014/02/24/anatomy-of-a-goto-fail-apples-ssl-bug-explained-plus-an-unofficial-patch/

Ducklin, P. (2015). 11 million Ashley Madison passwords cracked in 10 days, Naked Security – Award-winning computer security, news, opinion, advice and research from SOPHOS, 2015.09.10., https://nakedsecurity.sophos.com/2015/09/10/11-million-ashley-madison-passwords-cracked-in-10-days/

Gálffy, Cs. (2013). Szándékosan gyengíthetett az RSA, hwsw.hu, 2013.12.23. http://www.hwsw.hu/hirek/51525/rsa-nsa-dual-ec-drbg-veletlenszam-generator-biztonsag-snowden.html#kommentek

Gálffy, Cs. (2015). Hacking Team: a magyar vonatkozások, hwsw.hu, 2015.07.10., http://www.hwsw.hu/hirek/54243/hacking-team-magyar-nemzetbiztonsagi-szakszolgalat-digital-forensics-magyar-telekom.html

Goodin, D. (2014). Critical crypto bug leaves Linux, hundreds of apps open to eavesdropping, Ars-Technica, 2014.03.04., http://arstechnica.com/security/2014/03/critical-crypto-bug-leaves-linux-hundreds-of-apps-open-to-eavesdropping/

Greenwald, G. (2013). Revealed: how US and UK spy agencies defeat internet privacy and security, The Guardian, 2013.09.06. http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

Hegyeshalmi, R. (2014). Virtuális szex, valódi börtönbüntetés, Index, 2014.10.21., http://index.hu/tech/2014/10/21/virtualis_szex_valodi_bortonbuntetes/

HVG (2015/A). A Wall Street Farkasa elbújhat a Buda-Cash és Quaestor mögött. HVG, 2015.03.19., http://hvg.hu/gazdasag/20150319_A_Wall_Street_Farkasa_elbujhat_a_BudaCas

HVG (2015/B). Ha ezt tényleg bevezeti a Facebook, annak sokan nem fognak örülni, HVG, 2015.08.07., http://hvg.hu/tudomany/20150807_facebook_bankok_hitelfelvetel

Kaspersky (2015). The greatest heist of the century: hackers stole $1 bln. Kaspersky Lab Daily, 2015.02.16., https://blog.kaspersky.com/billion-dollar-apt-carbanak/7519/

Keszthelyi, A. (2013). About passwords, ACTA POLYTECHNICA HUNGARICA 10:(6) pp. 99-118., http://www.uni-obuda.hu/journal/Keszthelyi_44.pdf

Kormányzati Eseménykezelő Központ (2012). Újabb hamis digitális aláírást használó káros szoftverre bukkantak, 2012.03.19. http://tech.cert-hungary.hu/tech-blog/120319/ujabb-hamis-digitalis-alairast-hasznalo-karos-szoftverre-bukkantak

Lazányi, K. (2015/A): A biztonsági kultúra, TAYLOR Gazdálodás- és szervezéstudományi folyóirat VIKEK –Taylor Vezetéstudományi Brand, 2015/1-2. szám VII. évfolyam 1-2. szám No 18-19, Szeged 2015

Lazányi K. (2015/B): Mire jó a biztonsági kultúra?, VIKEK –Taylor Vezetéstudományi Brand, közlésre elfogadva.

Lewis, J. (2012). How spies used Facebook to steal Nato chiefs' details, The Telegraph, 2012.03.10., http://www.telegraph.co.uk/technology/9136029/How-spies-used-Facebook-to-steal-Nato-chiefs-details.html

MTI (2013). Szőke kislányt találtak egy görög cigánytáborban. Index, 2013.10.18., http://index.hu/kulfold/2013/10/18/szoke_kislanyt_talaltak_egy_gorog_ciganytaborban/

NYG (2015). Snowden: Titkosszolgálati törpök hemzsegnek az okostelefonjainkon, Index, 2015.10.05., http://index.hu/kulfold/2015/10/05/snowden_titkosszolgalati_torpok_hemzsegnek_az_okostelefonjainkon/

Oravecz, E. (2012). Árnyékkapcsolatok titkai, NOL, 2012.06.11., http://nol.hu/tud-tech/20120611-arnyekkapcsolatok_titkai-1313047

Pilch J. (1936). A hírszerzés és a kémkedés története. I-III. Franklin-Társulat, Budapest, 1936. Reprint kiadás: Kassák, Budapest 1998.

Rivest, R. et al. (1983). Cryptographic communications system and method, US 4405829 A, 20-09-1983. https://www.google.com/patents/US4405829

Scahill, J., Begley, J. (2015). The Great SIM Heist -- How Spies Stole the Keys to the Encryption Castle, The Intercept, 2015.02.19., https://theintercept.com/2015/02/19/great-sim-heist/

Schneier, B. (2013). Carry on: Sound Advice from Schneier on Security. John Wiley & Sons, 2013.

Schneier, B. (2005). Real Story of the Rogue Rootkit, Wired, 2005.11.17., http://www.wired.com/2005/11/real-story-of-the-rogue-rootkit/?currentPage=all

Schneier, B. (2010). Schneier a biztonságról. HVG Kiadó Zrt., Budapest, 2010.

Voith, H. (2015). Teljesen kirámoltak egy állami kémszoftverfejlesztőt, HWSW, 2015.07.06., http://www.hwsw.hu/hirek/54216/hacking-team-kormanyzati-kemprogram-adatvesztes-megfigyeles.html

Woody, L. (2015). HP's ZDI discloses 4 new vulnerabilities in Internet Explorer, InfoWorld, 2015.07.23., http://www.infoworld.com/article/2951738/patch-management/hp-s-zdi-discloses-four-new-vulnerabilities-in-internet-explorer.html

Zách D. (2015). 150 ezer forint bírság, öt perc alatt. Totalcar, 2015.06.25., http://totalcar.hu/magazin/kozelet/2015/06/25/150_ezer_forint_birsag_ot_perc_alatt/