DOI:10.38146/bsz-ajia.2012.v60.i.5pp5-21

LENGRÉ MÓNIKA

A XXI. század új típusú próbatétele: az informatikai biztonság

A csaknem két évtizeddel ezelőtt bekövetkező változások jelentős hatást gyakoroltak a nemzetközi kapcsolatok elméletére. Nagymértékű változások történtek a nemzetközi életben a hidegháború után, ennek következtében a politikai, gazdasági, társadalmi jellemzők is átalakultak. Ez a változás valójában egy korábban kezdődő folyamat következménye volt, és aligha lehet kötni egy megadott időponthoz, mégis jelképesen a hidegháború végéhez, a kelet-közép-európai rendszerváltozásokhoz szoktuk kapcsolni. A bipoláris rendszer felbomlása után unipolárissá vált az új világrend, ezzel együtt a globális biztonsági rendszer befolyása jelentősen csökkent, és ezáltal az egyes országok, régiók szabadabbá váltak.

Az országok, régiók szabadságát az is fokozta, hogy az Amerikai Egyesült Államok mint az egyik szuperhatalom, valamint a többi nagyhatalom – különösképpen gazdasági és pénzügyi okok miatt – nem akar minden egyes régióban szerepet vállalni. Így a magukra maradó régiók saját maguk alakíthatták ki a regionális rendszerüket és azon belül annak biztonsági dimenzióját.

A biztonság mind terjedelmi, mind tartalmi vonatkozásban felettébb összetett fogalom; politikai, külpolitikai, gazdasági, katonai, társadalmi, humanitárius és környezetvédelmi, katasztrófa-elhárítási, valamint informatikai dimenziói egyaránt vannak.

A biztonság nehezen meghatározható fogalom. A *biztonság* szó latin megfelelője, a „securitas – sine cura”, aggodalmat, félelemnélküliséget takar. A biztonság legegyszerűbb megközelítésben fenyegetettség nélküli életet, vagy bármiféle veszélyeztetettség, veszélyérzet hiányát jelenti.

Az, hogy egy társadalom biztonságban van, csak akkor válik nyilvánvalóvá, ha bizonyos próbatételek jelennek meg. Hosszú idejű, stabil, biztonsági kockázatoktól mentes korszakok elteltével a társadalom egészének veszélyérzete jelentősen csökken, hiszen az állampolgárok biztonságban érzik magukat mind a várható, mind a váratlan külső, illetve belső fenyegetések tekintetében, az állampolgároknak a biztonságpolitika hagyományos, katonai jellegű tevékenységét érintő érzékenysége elenyészik.

A gazdasági, az energia- és a környezetbiztonság mellett más területeken is beszélhetünk a biztonsági próbatételekről. A hidegháború végével a nemzetközi rendszer szereplői átalakultak, számuk jelentősen növekedett, horizontálisan és vertikálisan is kiszélesedett.

Ez egyrészt a széteső államok miatti több, kisebb állam kialakulását, másrészt új szereplők megjelenését jelentette a nemzetközi színtéren (multik megjelenése). Ez a kiszélesedés súlyos következményekkel járt, mivel a hidegháború után a nagyhatalmak már nem felügyelték saját érdekszférájukat. Ez olyan jelenségek megerősödéséhez vezetett, mint az államkudarcok, a belső polgárháborús helyzetek kialakulása, a nemzetközi terrorizmus fellendülése, az illegális fegyverkereskedelem szélesebb elterjedése, illetve a szervezett bűnözés megjelenése és terjeszkedése.

Valami megváltozott

A maguknak nyugalmat követelő egyének, állampolgárok és a nemzetközi közvélemény szemében 2001. szeptember 11. után a nemzetközi terrorizmus vált a legnagyobb ellenséggé, de korántsem tekinthetünk el a többi fenyegetéstől. Különösen azért, mert sokszor összefüggnek egymással. Az államkudarctól szenvedő gyenge és működésképtelen államok melegágyai lehetnek különféle, akár politikai indíttatású, akár gazdasági terrorszervezeteknek, illetve rossz biztonsági körülményeik miatt az illegális migráció, a fertőző betegségek kiindulópontjává, a szervezett bűnözés táptalajává is válhatnak.

Évekig a szervezett bűnözéssel kapcsolatba hozható – de annak sokrétűsége miatt hazánkban még nem kifejezetten idesorolt –, az egyik leginkább elterjedt és talán az egyik legnehezebben felderíthető és bizonyítható, de jelentős jövedelemforrást teremtő bűnözési forma, az információ-, illetve adatlopások, valamint az interneten elkövetett bűncselekmények felderítése volt egyebek között a feladatom.

Manapság kikerülhetetlen tényező a világhálót mindennap használóknak az informatikai biztonságról való gondolkodás és gondoskodás, hiszen biztonsági események tömege veszélyeztet minden informatikai rendszert és felhasználót.

Ahhoz, hogy egy nagyobb szervezeten belül a biztonsági nehézségek jól kezelhetők és megoldhatók legyenek, szükség van jól megtervezett, bevezetett, dokumentált és számon kért intézkedésekre.

Felgyorsult világunkban egyre fontosabb szerepük van a számítógépeknek, valamint az őket hálózatba kötő telekommunikációs rendszereknek.

Olyan információs társadalomban élünk, amikor is mindennapi életünkben, munkahelyünkön eddig soha nem tapasztalt információmennyiséget kell feldolgoznunk a lehető legrövidebb időn belül és a lehető legalaposabban.

Ennek következtében szinte minden háztartásban van számítógép, egy iroda pedig elképzelhetetlen nélküle, vagyis a számítógép mindennapos eszközzé vált.

Az államigazgatási, az oktatási, a gazdasági és a kereskedelmi szféra munkavégzése egyaránt a számítógépek használatán alapul, így a számítógépes rendszerektől való függés egyre nagyobb lesz.

A termelés, irányítás, oktatás, valamint a közigazgatásban végzett munka közben keletkező információk, adatok nagy részét már nemcsak papíron, hanem nagyrészt informatikai rendszerekben tároljuk és továbbítjuk. A világháló, az internet terjedésével a kommunikáció és a világban való tájékozódás módja is megváltozott.

Egy modern világ

Ebben az új világban az információ valódi értékké vált, így a védelme elengedhetetlen. De nemcsak az adatot, információt, hanem magát a számítógépes rendszert is védeni kell, hiszen e nélkül könnyen megbénulhat a számítógép által vezérelt életünk.

Az informatikai biztonság mint kedvező állapot elérése érdekében védelmi intézkedéseket kell alkalmaznunk. Ezeknek az intézkedéseknek át kell fogniuk az informatikai rendszer egészét, így annak létesítését, használatát, változtatását, megszüntetését, a védelemre fordított összegnek pedig arányban kell állnia az információ vagy a rendszer sérüléséből bekövetkezhető kárral.

Az informatikai rendszer védelme ki kell hogy terjedjen a fizikai, a logikai, a humánpolitikai védelem területére, valamint speciális eszközök és eljárások használatára is.

Ezt a védelmet nehezíti, hogy a számítógépes rendszerek is egyre bonyolultabbak. Manapság a legjobb szakemberek is nehéz helyzetben vannak, hiszen nem ismerhetik részletekbe menően a pontos működési mechanizmusokat, így rendkívül nehéz arról meggyőződniük, hogy egy rendszer tényleg úgy működik-e, ahogy kellene, illetve ez a rendszer valóban biztonságos-e.

Egy átlagos felhasználó, akinek kezében a számítástechnikai rendszer és szoftver csak használati eszköz, még ennyire sem ismeri a számítógépet. Párhuzamot vonhatunk például a mikrohullámú sütő vagy televízió működésé-

vel, hiszen egy átlagember ezeknek az eszközöknek sem ismeri pontosan a működési mechanizmusát, csak a használatuk módját.

Nehezen tudja eldönteni egy adott számítógépes rendszer használatakor, hogy mennyire van kiszolgáltatva rossz szándékú embertársainak.

A hétköznapi embernek a háztartási eszközök használatához nyújt segítséget a használati utasítás, amelyből megtudhatja, hogy az elvárt működés érdekében mit kell tennie, valamint hogyan tudja megóvni a saját és a környezete biztonságát.

Az otthoni számítógépek, valamint a világháló mindennapi használatakor a működésükre az egyes természeti tényezők (villámcsapás) és a hardvermeghibásodások is nagy veszélyt jelentenek, az adatok könnyen sérülhetnek, megsemmisülhetnek. Ez a bizonytalanság bizalmatlanságot okozhat, és a számítógépes rendszerek terjedését tekintve jelentős negatív hatása lehet. Ennek kiküszöbölése céljából az igazán fontos információkat gyakran több, akár öt vagy nyolc szerverre mentik le az informatikai szakemberek, így az adat pótolható vagy teljesen visszaállítható.

A számítógépek elterjedésével drámaian növekszik annak rosszindulatú felhasználása is: például hackerek feltörhetik a cég honlapját, egy sértődött munkatárs bizalmas adatokat tulajdoníthat el, régi barát vagy barátnő, esetleg volt házastárs bosszúból a rendszerben és a másik fél életében felbecsülhetetlen kárt okozhat. Az ilyen jellegű bosszút sajnos sokszor saját magunk is elősegíthetjük, hiszen, amikor még megvan a bizalom, könnyelműen megadjuk a jelszavunkat, vagy jelszó-emlékeztetőnket, erről aztán a későbbiekben megfeledkezünk. Az időközben haragossá váló fél pedig ezzel a bizalommal visszaélve, hozzájuthat olyan leveleinkhez, illetve egyéb fontos információkhoz, amelyeket már nem szándékoztunk megosztani vele. Jelszavunk megválasztásakor jó ha tudjuk, hogy minél nagyobb a választott jelszó bitértéke, illetve minél hosszabb, annál nehezebb feltörni, vagyis a feltöréséhez sokkal több idő szükséges.

Kérdések merülhetnek fel jogdíjas programok vagy zenei anyagok felhasználásával kapcsolatban, de az is előfordulhat, hogy egy szerződés elküldésének az időpontja vitatott. Számtalan olyan kérdés merülhet fel, amellyel kapcsolatban a számítógépen hagyott nyomoknak nagy jelentőségük lehet, polgári vagy büntetőpereket dönthet el. Ezek a nyomok a számítástechnikai adatok.

Lényegét tekintve a számítástechnikai adat nem más, mint az információknak, tényeknek, fogalmaknak olyan formában való megjelenése, amely informatikai feldolgozásra alkalmas, ideértve azt a programot is, amely vala-

mely funkciónak a számítástechnikai rendszer által való végrehajtását teszi lehetővé.

Az adatvédelem az adatok jogi értelemben vett, törvényekkel, szabályzatokkal való védelmét jelenti, míg az adatbiztonság fogalma magát a technikai védelmet.

Ezzel párhuzamosan adatbiztonságnak nevezzük az adatok jogosulatlan megismerése, megszerzése, módosítása és megsemmisítése elleni logikai (szervezési) és fizikai (műszaki) védelmi intézkedéseket, valamint a szervezési eljárások egységes rendszerét. Szokás még a számítógépes rendszerek és a bennük tárolt információk biztonságát informatikai biztonságnak is nevezni. Az informatikai biztonság két nagy területre osztható: információvédelem és megbízható működés.

Míg az információvédelem az adatok sértetlenségével, bizalmasságával, hitelességével foglalkozik, addig az utóbbinak a célja a rendelkezésre állás és a működés fenntartása.

A rendszer védelmi célja az, hogy az információkhoz vagy adatokhoz csak az arra jogosultak és csak az előírt módon és ideig férhessenek hozzá. A bizalmasság követelményét a megfelelő hozzáférési jogosultságok beállításával lehet elérni. Ebből következik, hogy az információ vagy rendszer csak akkor lehet sértetlen, ha csak az arra jogosultak végeznek benne változtatást, vagy minden kétséget kizáróan megállapítható, hogy az előállítás óta változatlan maradt, abban senki semmit nem módosított.

A rendelkezésre állás követelménye pedig azt rögzíti, hogy egy adott rendszernek milyen megbízhatósággal kell ellátnia a feladatát a meghatározott időn belül. Mivel a rendelkezésre állást véletlen események (meghibásodás, tűz, víz, betörés) is fenyegetik, de akár támadók tevékenysége sem zárható ki, az előbbi jellemzők garantálása érdekében határozott védelmi intézkedéseket kell tenni.

Az informatikai rendszerek tökéletes biztonságát nehéz kivitelezni, hiszen a váratlan események köre nem behatárolható, közbejöhetnek olyan történések, amelyek kivédhetetlen, elkerülhetetlen veszélyt jelenthetnek, és amelyek ellen nagyon nehéz vagy egyáltalán nem lehet védekezni.

A tökéletes informatikai biztonság megvalósulásának lehetőségével kapcsolatban párhuzamot vonhatunk egy magánlakás vagy ház biztonsága között, hiszen mindkét esetben – bár a biztonsági, illetve biztonságtechnikai lehetőségek végtelenek – a tökéletes védelem kiépítését nehezíti az a tény, hogy az emberi és pénzügyi források végesek.

Alapvető hiba úgy gondolkodni a biztonságról, mintha az egyszerűen csak egy termék lenne, és ha egyszer megvásároltuk, akkor a későbbiekben már biztonságban érezhetjük magunkat.

A rendszerek egyre összetettebbek, így nem adhat teljes megoldást egyik vagy másik operációs rendszer, tűzfal vagy biztonsági beállítás alkalmazása sem, csak ha azokat megfelelő környezetben használjuk. A tűzfal önmagában nem old meg semmit, ha nem korlátozzuk a beállításokat, és minden hálózati forgalom engedélyezve van.

Célszerű a tűzfalat nem egyszeri biztonsági intézkedésként alkalmazni, hanem olyan eljárásként, amely átfogja a rendszer egész működését.

A tapasztalat azonban azt mutatja, hogy a hétköznapi ember általában csak akkor veszi komolyan a biztonságot, illetve annak hiányát, amikor egy váratlan esemény visszafordíthatatlan és helyrehozhatatlan anyagi és erkölcsi károkat okoz.

A legnagyobb biztonság eléréséhez elengedhetetlen az a folyamatosság, amely a biztonsági intézkedéseknek a rendszer egész működési idejét, életciklusát átfogja. Egy vírusirtó rendszeres és folyamatos frissítése legalább olyan fontos, mint annak telepítése. Ugyanígy hiába naplózzuk az eseményeket, ha soha nem ellenőrizzük, mi került a naplófájlba. Egy elhanyagolt, frissítetlen hálózat az idő múlásával egyre nagyobb és nagyobb veszélyt jelent. Sokszor nem is észlelhető a sikeres támadás, mert az elhanyagolt rendszereket ugródeszkának használják a támadók, ezért igyekeznek rejtve maradni a sikeresen támadott rendszerben. Ezek a tények pedig rendszerint az otthoni, a család által használt számítógépekre igazak, hiszen csupán minimális anyagi ráfordítással és kevés utánajárással próbáljuk meg a rendszereinket biztonságossá tenni.

Biztonságosan a világhálón

Nagyon sokan hajlamosak azt hinni, hogy a jelszavuk senkit sem érdekel, vagy az ő rendszerükön nincs semmilyen értékes információ vagy adat, amelyért azt érdemes lenne feltörni. A támadók sokszor automatikus eszközökkel keresik a gyenge pontokat, nem foglalkoznak az egyénnel, csak azzal, hogy egyszerűen kitalálható-e a jelszavunk, vagy sem. Egy gyengén védett gép nem kell hogy értékes adatokat tároljon, elég, ha átmenetnek használható egy már értékes adatokat tároló gép feltöréséhez, és így az eredeti támadó rejtve maradhat a feltört gép álarca mögött.

Sokan élnek ezzel a lehetőséggel, és gyakorlatilag sok-sok számítógép folyamatos üzemben kutat a világhálón lehetséges célpontok után.

Előfordulhat, hogy ha egy rendszerhez a gép által generált jelszó használatát teszik kötelezővé, akkor az emberek azért, hogy megjegyezzék, leírják egy papírra a jelszavukat, ami adott esetben kockázatosabb, mint ha egyszerűbb, de megjegyezhető, ezáltal más számára hozzáférhetetlen jelszót választottak volna. A biztonsági megoldásokat mindig lehet fokozni a teljes használhatatlanságig, de többnyire nem ez a cél. Az egyszerű megoldást könnyebb elfogadtatni és a beidegződése is gyorsabb, hatékonyabb, így sokkal hatásosabb védelem lehet.

Meg kell említenünk a hazánkban is egyre elterjedtebb módszert, a jelszavak feltörésére használt brute-force-t, azaz a nyers erőszakot. Az ilyen jellegű támadás a teljes kipróbáláson alapszik, amelynek a lényege, hogy minden lehetséges betű, szám, illetve speciális karakter lehetséges kombinációját kipróbálja, amíg meg nem találja a kérdéses jelszót. Az ilyen jellegű feltörések általában elég sokáig tartanak, a támadási idő hosszúsága függ a támadást indító számítógép erősségétől és a jelszó összetettségétől is. Értelemszerűen minél hosszabb, bonyolultabb egy jelszó, annál nehezebb feltörni. A jelszó kiválasztásánál célszerű váltogatni a kis- és nagybetűket, számokat, illetve egyéb, speciális karaktereket.

Meg kell említeni a különböző közösségi oldalakat, hiszen ezeken az oldalakon külön csoportként megjelölhetjük a közvetlen hozzátartozóinkat, családtagjainkat, legjobb barátainkat. Sokan beleesnek abba a hibába, hogy ha a jelszót nem is, de a biztonsági kérdésre vagy a jelszó-emlékeztetőre adott válaszokat felteszik a saját adatlapjukra, vagy azok a megadott csoportok információjából kikövetkeztethetők (például a szerelmem neve, majd a fényképek között megtalálhatjuk a Szerelmemmel, Gáborral című fotót). De ugyanezt el lehet játszani kutyanévvel, vagy barát, barátnő, születési hely, illetve egyéb, a közösségi oldalakra meggondolatlanul feltett információ felhasználásával is.

A mindennapi életben használt modern információs és informatikai rendszerek nemzetközi jellegéből adódóan mára az egyik legelterjedtebb bűnözési formává vált az internet útján, illetve az internet felhasználásával elkövetett bűncselekmény.

Ennek legelterjedtebb formája, az adathalászat, azaz *phishing (password harvesting fishing)* az utóbbi időben Magyarországon is egyre nagyobb gondot okoz. Az adathalászok (identitástolvajok) célja, hogy minél rövidebb idő alatt a lehető legtöbb adatot szerezzék meg. Mivel a csalók általában megbíz-

ható személynek vagy cégnek adják ki magukat, és az interneten keresztül – személytelenségbe burkolódzva – lépnek kapcsolatba a sértettekkel, így nagy esélyük van arra, hogy tettüket sikeresen vigyék véghez.

Nézzünk egy példát: látszólag a számlavezető bankunktól érkezik az e-mail címünkre egy elektronikus levél, amelyben arra szólítanak fel, hogy valamilyen banki átalakítás vagy fejlesztés miatt egyeztessük az adatainkat. Ehhez csak arra a megadott linkre kell kattintani, amely látszólag a bankunk oldalára mutat. Megnyitva a hivatkozást a bankunkéval látszólag tökéletesen megegyező honlapra kerülünk, ahol kérik a bejelentkező nevünket vagy azonosítónkat, a jelszavunkat és az elektronikus belépéshez szükséges egyéb adatainkat. A honlap azonban csak látszólag a pénzintézetünké. Az eredeti banki oldalhoz a megtévesztésig hasonló oldalra navigálnak át a csalók, így a felhasználók közül sokan bejelentkeznek és meg is adják a kért adatokat. Ezeket az adatokat azután a csalók elektronikus vásárláshoz vagy pénzátutaláshoz használják, természetesen a saját céljaikra, ezáltal akár milliós károkat is okozhatnak. A bankok és a média rendszeresen közzé tesz tömeges és látványos, a veszélyre figyelmeztető felhívásokat, ennek ellenére még mindig eurómilliárdokra tehető a phishinggel okozott kár Európában. A banki informatikai szakemberek sem ülnek tétlenül, igyekeznek felvenni a versenyt az internetes bűnelkövetőkkel szemben, ezért érdemes a pénzintézetek honlapjain tájékozódni és kihasználni a bankok által nyújtott szolgáltatásokat, valamint megfogadni a biztonsági intézkedésekre történő felhívásokat. Ha a banki tranzakcióinkat interneten keresztül intézzük, célszerű igénybe venni a webszámlát és egyéb, például csak az interneten használható kártyák szolgáltatásait, illetve az e célból sms-ben történő értesítéseket a csalások megelőzése érdekében.

Az interneten elkövetett bűncselekmények sajátosságai közé tartozik, hogy a csalások érintettjei, károsultjai csak utólag és sokszor nagy veszteségek árán értesülnek a történtekről.

Az adathalászat – mint az egyik bűnözési forma – célja ma már egyértelműen az anyagi haszonszerzés, a hétköznapi ember bizalmára építő támadás. A módszerről az 1990-es évek közepén az egyik legnagyobb amerikai internetszolgáltató, az AOL ellen elkövetett adatlopáskor értesült a világ. Magyarországon az első ismertté vált phishingtámadás az Inter-Európa Bankot érte, 2003-ban. A veszély ma globális szinten folyamatosan növekszik, a technika pedig a személyi számítógépek és szoftverek fejlődésével egyidejűleg tökéletesedik. Az interneten a mind olcsóbbá váló és egyre nagyobb sávszélességet elérő szolgáltatások lehetővé teszik a felhasználók számára, hogy nagy-

méretű médiafájlokat, népszerű programokat és más adattípusokat viszonylag gyorsan letöltsenek, ez növeli a bűnözők lehetőségeit is. Míg 2005-ig a világméretű számítógépes vírus- és féregtámadások voltak a jellemzők, ez a trend az elmúlt évek folyamán erőteljesen megváltozott.

Az adathalászat egyik elterjedt változata a csalilevél. Csali használatával könnyű halat fogni. Adathalászatkor az internetes tolvajok is csalikat vetnek be. Az „eljárás" során a csaló csali-e-mailt vagy azonnali üzenetet küld a felhasználónak, mint az előbbi példában is látható, akár egy bank vagy egyéb pénzintézet nevében, a feladó azonban csak álca. A levélben szereplő hivatkozás (link) egy az eredetihez nagyon hasonló vagy akár ugyanolyan oldalra mutat. Olyan érzékeny adatok kiszolgáltatására kérik, mint a bankszámlaszám, jelszó vagy PIN kód, amelyeket aztán a csalók az illető bankszámlájának elérésére használhatnak fel.

A másik fajta adathalászati módszer az úgynevezett trójai program, amely a levélhez csatolt vagy egy honlapról az áldozat tudta nélkül települő billentyűzetfigyelő *(key logger)* „kémprogram", amely a leütött billentyűket továbbítja az interneten keresztül, és ellopja a begépelt bizalmas adatokat. Ezek a billentyűzetfigyelő programok nyomon követhetik a banki, e-mail- és egyéb internetes fiókokba való belépéseket, és elküldhetik a jelszavakat a vonal másik végén lévő szélhámosnak. Ő a felhasználónév és jelszó birtokában a számítógépes kalózokra jellemző trükkök révén nemcsak a veszélyeztetett számítógéphez, hanem akár a teljes vállalati hálózathoz hozzáférhet.

Az adathalász áldozatául eső állampolgár anyagi helyzetét, megbecsülését vagy akár kilétét is veszély fenyegetheti. Egy cég vagy vállalkozás azonban még ennél is többet veszíthet.

Ha az internetes tolvaj a biztonsági szempontból sérült számítógépen hacker módszerrel bejut egy multinacionális cég hálózatára, bizalmas adatokat lophat el, például levelezőlistákat és egyéb szellemi javakat. Ha a vásárlók bizalmas adatai eltűnnek, az katasztrofális következményekkel jár a cégre nézve, hiszen elvész a cégbe és a márkába vetett bizalom is.

A csalás egy másik formája a DNS-fertőzés (más néven eltérítéses adathalászat, angolul *pharming*), amikor is a csalók az internetes forgalmat irányító rendszert módosítják, feltörik. Egy hamis, hasonmás webhelyet hoznak létre, és az internet sebezhetőségét kihasználva átirányítják a felhasználók eredeti adatforgalmát egy másik, az eredeti célhelyhez hasonló tartalmú, hamis weboldalra.

Az előbbiekből látható, hogy a veszélyeztetettek köre igen széles, hiszen bárki lehet áldozat, aki internetet használ, illetve azon levelez. Nemcsak ma-

gánszemélyek, hanem akár egy cég vagy vállalat adatai is megszerezhetők. Gyakran az áldozat nem is tudja, hogy csalás áldozata.

Magyarországon nyolc-tíz éve az internethasználók több mint nyolcvan százaléka informatikai szakember volt, akik nem elsősorban szórakozásra, hanem a munkájuk miatt használták a világhálót. Köztudomású tény, hogy maga az internet kifejezetten a hírszerzés számára lett életre híva, időközben azonban internetboom következett be, és a magánszféra mint fő felhasználói réteg lett a célcsoport. A felhasználói kör struktúrájának változásától a felhasználók száma is ugrásszerűen megnövekedett. Manapság az internetes technológiákat körülbelül kétmilliárdan használják személyes, illetve üzleti célokra, például információkeresésre, szolgáltatások és áruk megrendelésére, kapcsolattartásra, szórakozásra stb.

Ezzel párhuzamosan a világhálót felhasználó csalók által elkövetett bűncselekmények száma is évről évre jelentősen nő, hiszen az internet

– olcsó,
– gyors,
– könnyen hozzáférhető,
– egyszerre nagy tömegekhez juttatható el,
– nehezen nyomon követhető,
– a károsultak gyakran nem is tudnak arról, hogy áldozatok,
– a tettesek nagyon ritkán és nehezen keríthetők kézre.

A világhálóhoz történő hozzáféréshez és annak használatához viszonylag könnyű út vezet. Először is előfizetői szerződést kell kötni azzal a céggel vagy társasággal, amely az ilyen jellegű szolgáltatást nyújtja. Az internethez kapcsolódáskor az előfizető számítógépe telefonvonal vagy más hálózat használatával kapcsolatba lép a szolgáltató szerverével, majd az előfizető számítógépe megadja az azonosításhoz szükséges adatokat (például az előfizetői azonosítót, felhasználónevet, jelszót stb.), majd a szolgáltató szervergépe ellenőrzi és azonosítja az előfizetőt, és ha megállapítja a jogosultságot, engedélyezi a hozzáférést a világhálóhoz. Ehhez az azonosításhoz a szolgáltató minden kapcsolódáskor egy négytagú, egymástól pontokkal elválasztott számsort rendel, ezt nevezzük IP-*(Internet Protokol)* címnek, amely nem más, mint egy hálózati azonosító.

Az internetszolgáltatókon keresztül a világhálóra kapcsolódó lakossági számítógépek IP-címe gyakran változó, de ugyanazt az IP-címet az interneten egy időben csak és kizárólag egy előfizető használhatja, és ez nem változik meg addig, amíg a kapcsolat fennáll a felhasználó és a szolgáltató szer-

vere között. Ezek alapján a szolgáltatók tájékoztathatják a nyomozó hatóságokat arról, hogy egy adott időben a megadott IP-cím kinek lett kiosztva, és akár az előfizetői szerződést is a rendelkezésükre bocsáthatják. A gyakorlatban azonban ez nem ilyen egyszerű, az IP-cím és a pontos időpont ellenére nem minden esetben lehet egyértelműen azonosítani az internet-előfizetőt. Előfordulhat, hogy az internet-előfizető tudta és beleegyezése nélkül valaki más használja az előfizetését, mivel hamis vagy lopott személyazonosító okmányokkal, vagy az előfizetői azonosító, a felhasználónév, illetve a jelszó megszerzésével lép fel az elkövető a világhálóra.

Mivel az internetszolgáltató csak annyit rögzít, hogy a szolgáltatást az azonosítóval rendelkező előfizető használta, gyakran csak akkor derül fény a megtévesztésre, amikor egy esetleges házkutatás és lefoglalás után a teljesen ártatlan előfizető számítógépe semmilyen adatot nem tartalmaz a bűncselekménnyel kapcsolatban.

Vezeték nélküli internetelérést lehetővé tevő berendezés *(router)* használata esetén általánosságban csaknem száz méteren belül szabadon elérhető az internet abban az esetben, ha valaki egy arra alkalmas számítógéppel megkeresi és csatlakozik nem védett, vezeték nélküli elérést nyújtó berendezéshez. Ha a rendszer nincs ellátva megfelelő védelemmel, például az előfizető nem védi jelszóval, vagy a jelszavát megszerzik, feltörik, ekkor már bárki más a tudta és belegyezése nélkül szabadon használhatja a világhálót, ezáltal az előfizetőre terelve a bűncselekmény gyanúját. Azon felül, hogy a routert jelszóvédelemmel célszerű ellátni, MAC-cím-szűrőt is tehetünk rá, amellyel az SSID-et el tudjuk rejteni.

A MAC- *(Media Access Control)* cím nem más, mint egy általában 12 karakterből álló számsor, amelyet a gyártáskor gyakorlatilag fizikailag beleégetnek a hálózati kártyába. Hardvercímnek is szokták hívni, a hálózat meghatározott pontjainak azonosítására alkalmas. Az SSID *(Server Set Identifier)* pedig a vezeték nélküli hálózat azonosítására szolgál.

A védelem és biztonság tekintetében gondot jelenthet továbbá az is, ha a világháló-elérést egyszerre sok számítógép használja. Ilyen lehet például, amikor az internet-előfizetést nem egy magánszemély, hanem például egy munkahely, egy iskola vagy kollégium, illetve irodaház használja. A szolgáltatónak ezekben az esetekben is meg tudja adni, hogy egy adott IP-cím, adott időpontban melyik előfizetőnek lett kiosztva, de ilyenkor jellemzően az előfizetők IP-tartományokat kapnak. Így azt, hogy a megadott IP-címet konkrétan melyik számítógép vagy munkaállomás használta, nem a szolgáltató, hanem az előfizető tudja megválaszolni, ha a számítógépes hálózata rögzítette

és tárolta ezeket az adatokat. Abban az esetben, ha a szerver nem tárolta ezeket az adatokat, akár több száz számítógép ellenőrzésére lenne szükség az elkövető által használt számítógép megtalálásához.

Gondot okozhatnak továbbá a szabad internet-elérési pontok, a nyilvános hálózatok, internetkávézók. Ilyenkor az IP-cím kiosztására vonatkozó adatokból csupán annyit lehet megállapítani, hogy az adott IP-cím egy étterem, kávézó, szálloda részére lett kiosztva, amelynek közelében akár szabadon, akár díjfizetés ellenében hozzáférhető a világháló vezeték nélküli hálózat segítségével. Budapesten is nagyon sok helyen vannak ilyen szabad elérési pontok. Ilyenkor természetesen szinte lehetetlen megállapítani, hogy az adott időpontban ki használta a rendelkezésre bocsátott számítógépet, és akkor még nem is beszéltünk a vezeték nélküli kapcsolatról, az úgynevezett wifit kihasználó laptopokról, illetve az egyre elterjedtebb okostelefonokról, egyéb modern mobilkészülékekről.

Napjainkban az egész világra kiterjedő gazdasági válság számos új internetes támadáshoz ad alapot, ezek között adathalász-támadások is lehetnek (például egy-egy bank bezárása körüli pletykák terjesztése), illetve olyanok, amelyek könnyű jelzáloghitelt vagy újrafinanszírozást ígérnek.

Várhatóan azokat is megpróbálják becsapni, akiknek nehézségei vannak a hitel visszafizetésével, vagy például végrehajtás alá vonják ingatlanát vagy egyéb nagyobb értékű, de a hitel fedezeteként felajánlott ingóságát, amely lehet akár gépjármű, műkincs vagy ékszer.

Az online feketegazdaság hatékony, világméretű piaccá nőtt, ahol milliárd dolláros értékben, rendszeresen adnak-vesznek lopott adatokat és csalásokhoz kapcsolódó szolgáltatásokat. A kutatások azt bizonyítják, hogy míg korábban csak néhány kártékony kódot terjesztettek tömegesen, napjainkra átálltak a nagy veszélycsaládok küldésére.

Ez praktikusan azt jelenti, hogy a telepített kártékony programok a terjedés során gyorsan átalakulnak, és ezért nehéz ellenük védekezni. A nemzetközi pénzügyi válság a bankszámlaadatok megszerzésére irányuló internetes bűncselekmények szaporodásával járhat.

Az Amerikai Szövetségi Kereskedelmi Bizottság és egy brit parlamenti bizottság egyaránt arra hívta fel a figyelmet, hogy a pénzügyi válság hatására az online adathalászat területén elmozdulás várható az identitástolvajlástól a banki ügyféladatok megszerzésére irányuló kísérletek irányába.

A bizottság szerint a zavarosban halászó csalóknak kiváló lehetőséget nyújt a bankszférában végbemenő viharos változás, amelynek során számos pénzintézetnek hirtelen megváltozott a tulajdonosi szerkezete. A bűnözők a

megroggyant bankházak élére kinevezett állami válságmenedzserek vagy az új tulajdonos nevében léphetnek fel, és adategyeztetésre kérhetik a gyanútlan ügyfeleket.

A testület azt javasolja az internetező bankszámla-tulajdonosoknak, hogy ne reagáljanak az olyan e-mailekre vagy felugró ablakokon elhelyezett üzenetekre, amelyek számlaadatok megadására szólítanak fel, még akkor sem, ha ezek látszólag a banktól érkeztek.

Az identitástolvajlással *(ID Theft)* kapcsolatos ügyekkel foglalkozó brit parlamenti bizottság éves beszámolója szerint a krízis miatt szigorodó hitelfeltételek hatására gyakoribbá válhatnak a számlatulajdonosok elleni támadások.

„Hitelt szerezni lopott identitással is egyre nehezebb, a bűnözők ezért aktívabban törekedhetnek a már létező számlák megcsapolására" – áll a bizottság éves beszámolójában.

Mindeközben a brit bankrendszer fizetési iparágát összefogó szervezet, a Fizetési Klíringszolgáltatók Szövetsége arról számolt be, hogy az adathalásztámadások száma már a világ pénzügyi rendszerét megrázó válság kirobbanása előtt is meredeken emelkedett.

A visszaéléseket nehéz lenne megakadályozni, ha nem lennének büntetőjogi következményei a szabálytalanságoknak. Mindazonáltal a törvényalkotók sincsenek könnyű helyzetben, hiszen olyan törvényeket kell létrehozniuk, amelyek a lehető legnagyobb mértékben függetlenek a technológiától, így a technikai fejlődés ellenére is hosszú távon alkalmazhatók maradnak. Ezért tapasztalhatjuk a hatályban lévő törvények esetében is azt, hogy a technológiához kötődő elnevezések helyett igyekeznek általánosabb, inkább a funkcionalitást meghatározó fogalmakat használni. Ezen kívül a törvényeknek nem szabad gátolniuk a technikai és gazdasági fejlődést, és szabályozást csak ott kell létrehozni, ahol erre valóban szükség van. Az informatikai tárgyú jogalkotás ma elsősorban a magánjog területén jelenik meg, de a büntetőjoggal való kapcsolata sem elhanyagolható.

A világhálón elkövetett bűncselekmények kapcsán az információ által hordozott tartalom és annak jogsértő volta a domináns elem. Idetartoznak az információ, az információtárolás és -továbbítás biztonságosságát, bizalmasságát sértő bűncselekmények, valamint a szellemi tulajdon tárgyát adó adatok ellen irányuló cselekmények.

Lényegét tekintve az internet lehet az elkövetés eszköze, az itt keringő adatok pedig azon bűncselekmények tárgya, amelyek szoros összefüggést mutatnak az informatikával.

Büntetőjogi értelemben a vagyon elleni bűncselekményekre vonatkozó rendelkezések e cselekményeknél korábban nem voltak alkalmazhatók, ezért iktatta a jogalkotó a büntető törvénykönyvbe (1994. évi IX. törvény 22. §-a) 1994. május 15-i hatállyal a számítógépes csalás tényállását, amely azóta többször módosult.

Hazánk csatlakozott az Európa Tanács 2001. november 23-án, Budapesten elfogadott, a számítástechnikai bűnözésről szóló egyezményéhez *(Convention on Cybercrime)*, amely a belső jogunkba a 2004. évi LXXIX. törvénnyel került.

Az értelmező rendelkezés az informatikai egyezményben foglaltaknak megfelelően határozza meg a számítástechnikai rendszer fogalmát. A számítástechnikai rendszerek körébe tartoznak a számítástechnikai adatfeldolgozásra épülő, memóriával bíró olyan egységek is, amelyek megjelenésükben nem hagyományos számítógépek.

A törvény szerinti fogalom így átfogja a közcélú távbeszélő-szolgáltatás, illetve mobiltelefon-szolgáltatás igénybevételére szolgáló elektronikus kártyákat, a mobiltelefont vezérlő mikroszámítógépeket, valamint a számítástechnikai berendezések felhasználásával működő hírközlési, telekommunikációs rendszereket is.

A számítástechnikai rendszer fogalma nemcsak az egyes berendezésekre terjed ki, hanem felöleli az azok összekapcsolása révén létrejött hálózatot, valamint az adattovábbítást, a kapcsolatfelvételt lehetővé tevő műszaki berendezéseket is. Az egyes berendezések közötti kapcsolat nem jelent feltétlenül fizikai összekapcsoltságot.

A számítástechnikai rendszerek között az összeköttetés létrejöhet elektronikus vagy optikai jeleket továbbító kábelek vagy vezetékek útján, valamint rádióhullámok, infravörös, illetőleg rövidhullámok segítségével, vagy műholdas sugárzás igénybevételével is.

A 2001-ben elfogadott, majd 2004-ben módosított 2001. évi XXXV. törvény az elektronikus aláírás jogi szabályozásának alapjait teremti meg. A törvény más fejlett országokhoz képest későn jelent meg (az Európai Unióban 1999-ben jelent meg a 99/93/EC jelű direktíva, de ekkorra már több tagállamban is volt elektronikus aláírási törvény). De így is hatalmas a jelentősége, hiszen elektronikus aláírás nélkül nincs hiteles elektronikus ügyintézés. A törvény nagyon sok területen lehetővé teszi a papíralapú dokumentumok helyett elektronikus aláírás, illetve dokumentum használatát, de azért még korántsem az élet minden területén (például az anyakönyvvezetés hivatalos, papíralapú formáját továbbra sem váltja fel csak elektronikus dokumentum).

A 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szól, szintén többször módosított, aktualizált. A törvény összhangban van egyebek között az Európai Unió 2000/31/EK jelű, azonos témájú irányelvével, célja az elektronikus kereskedelem és más elektronikus szolgáltatások feltételeinek megteremtése, ezáltal a magyar gazdaság versenyképességének javítása, valamint a fogyasztók jogai védelmének szabályozása. A törvény hatálya nem terjed ki a magánjellegű kommunikációra.

Az informatikai biztonsággal kapcsolatban megemlíthetők még egyéb speciális területekre vonatkozó rendelkezések, mint például az államtitokról és a szolgálati titokról, az üzleti titokról vagy banktitokról szóló egyéb rendelkezések, amelyek mind fokozott és speciális biztonsági előírások betartását vonják maguk után.

A világhálón továbbított adatok ellenőrizetlensége miatt az egyes országok erőfeszítései ellenére nagy mennyiségben lehet fellelni a gyerekek és a fiatalok számára veszélyesnek és károsnak tűnő anyagokat, oldalakat.

Vannak olyan portálok, amelyek felnőtteknek szóló tartalmakat közvetítenek. Ezek használata előtt meg kell hogy jelenjen egy figyelemfelhívó panel, amely korhatár-ellenőrzést végez. Ez azonban teljesen hatástalan, mivel a felhasználó bármilyen születési dátumot beírhat. A gyerekekre és a fiatal felhasználókra további veszélyt jelentenek a különböző chat-, illetve közösségi oldalak, valamint az üzenetváltások esetében a megtévesztés, fenyegetés. A naiv, tapasztalatlan gyermekeket könnyűszerrel elcsalhatják az elkövetők, vagy olyan dolgokra, cselekedetekre kényszeríthetik, amelyek akár súlyos következményekkel járó bűncselekmények is lehetnek, vagy a további testi és lelki fejlődésükre, életükre is káros hatással lehetnek.

Számos hátránya mellett azonban az internet több olyan módszert is közvetít, amellyel a szülők, tanárok kiszűrhetik a világháló veszélyes anyagait. Ilyenek például a Net Nanny Parental Controls, valamint a McAfee Parental Controls, noha ezek sajnos fizetős és angol nyelvű oldalak.

Magyarországon elindult az úgynevezett Biztonságos Böngészés Program, amelynek keretében már 260 iskola 13 ezer munkaállomásán használhatják a nebulók biztonsággal a világhálót. Bármely magyarországi iskola csatlakozhat a programhoz, költségek nélkül. A Magyarországi Tartalomszolgáltatók Egyesületének ajánlásával készült gyermekvédelmi szűrőszoftver letöltése a nyilvános oldalról ingyenes, és ami nem elhanyagolható, magyar nyelvű.

Összegzés

Összegzésképpen elmondhatjuk, hogy a hackerek a számítógépek feltörésénél az emberi hibákat használják ki. A hétköznapi felhasználót ritkábban éri hackertámadás, mint a bankokat, illetve olyan cégeket, amelyeknél nagyobb esély van használható információhoz jutni. Az otthon használt rendszerek esetében az előfizető nem is észleli, hiszen jobb esetben sem anyagi, sem erkölcsi kára nem keletkezik.

Ha valaki szeretné elkerülni, hogy áldozat legyen, azaz a személyes adataival visszaéljenek, gondosan válassza meg a jelszavát, válasszon úgynevezett alfanumerikus jelszót, azaz kis- és nagybetűket, valamint számokat kombináló jelszót. A levelezésnél a SPAM-szűrőt érdemes erősre állítani, idegen, nem ismert vagy gyanús oldalakon pedig nem szabad megadni e-mail címet, egyéb személyes adatot, illetve ezeket az oldalakat célszerű meg sem nyitni. A telepített tűzfalakat, spy ware-eket, illetve vírusirtókat rendszeresen frissíteni kell, hiszen ezek a legtöbb problémára megoldást kínálnak.

A hackereknek is célszerű odafigyelniük, hiszen az általuk indított támadások közben az ő gépükre is települhetnek vírusok, egyéb trójai programok, így a támadókból gyakran áldozatok is lehetnek.

IRODALOM

Belovics Ervin – Molnár Gábor – Sinku Pál: Büntetőjog. HVG-ORAC Lap- és Könyvkiadó Kft., Budapest, 2007

Fischer Ferenc: A kétpólusú világ 1945–1989. Dialóg Campus Kiadó, Budapest–Pécs, 2005

Gazdag Ferenc (szerk.): Biztonságpolitika. SVKH, Budapest, 2001

Magyar Értelmező Kéziszótár. Akadémiai Kiadó, Budapest, 1975

Matus János: A jövő árnyéka. A Pesti Csoport Kft., Budapest, 2005

Szabó József – Gabriel Győző – Horváth Ferenc (szerk.): Hadtudományi Lexikon. Magyar Hadtudományi Társaság, Budapest, 1995

INTERNETES FORRÁSOK

www.cert.hu

www.microsoft.com

www.nbh.hu

www.zybex.org

www.antiphising.org

www.fraud.org

www.ic3.org
www.nw3c.org
www.itb.hu/ajanlasok
www.symantec.hu
www.magyarorszag.hu
www.honvedelem.hu
www.kulugyminiszterium.hu
www.hm.hu
www.biztostu.hu
www.complex.hu
http://net.jogtar.hu