MŰSZAKI VAGY EMBERI TÉNYEZŐKTŐL FÜGG INKÁBB?

Adathalászat kontra adatvédelem

Kik fenyegetik az információt, mint a XXI. század legértékesebb vagyontárgyát? Az informatikai biztonság elsősorban nem is műszaki kérdés. Bár a legtöbb kiadványban főként ezeket tárgyalják, ki kell emelnünk, hogy a biztonság elsősorban az emberi tényezőtől függ. A legnagyobb fenyegetést a számítógépekre és az informatikai adatokra nem a külső behatolók, hanem a saját alkalmazottak jelentik.

Az Egyesült Államokban az informatikai bűnözés által okozott, felderített és közölt kár meghaladja az évenkénti 70 milliárd dollárt. A számítógépek nem követnek el bűnöket, azt az emberek követik el, akik bűnös célra használják azokat. Így tehát a rendszer védelmének hatékonyságát az emberi oldalra történő odafigyelés növelheti elsősorban, azaz „Soha ne feledkezzünk meg az emberről, amikor gépről beszélünk!"

Főként tehát a saját alkalmazottakra kell odafigyelni. A hálózatból kívülről behatolók és vírusterjesztők nagyobb publicitást kapnak, így jobban felhívják a figyelmet a gyenge pontokra (az interneten napi 72 000, a NASA hálózatába évi 7000 detektált betörési kísérlettel, és naponta 6 új vírus megjelenésével számolhatunk), de az igazi veszély az intézményen belül van. Nincs az a pitbull-mutációkkal védett páncélterem, titkosító-, vagy bármiféle biztonsági rendszer, amit kellő ismerettel, főleg belülről és csoportosan ne lehetne feltörni.

Az Egyesült Államokban külön országos központi, informatikai bűnözést nyilvántartó adatbank működik, amelynek néhány statisztikai adatát szemlélteti **1. ábránk**. Ezen érdemes elgondolkodni!

Közismert, hogy a nyomozói gyakorlatban a "motiváció, módszer és alkalom"-elvét alkalmazzák. A motivált elkövető, ha hozzáférhet a rendszerhez, akkor biztosan megtalálja az alkalmat, és kidolgozza a módszert a károkozásra. A kormányzati és üzleti számítógépekbe behatoló kamaszok többé-kevésbé véletlenszerűen lesznek bűnelkövetők. Egy jelszó kitalálása jó passzió. A külső elkövetőnek találgatnia kell, míg a belső alkalmazott tudja, hogy hol vannak a gyenge pontok és hol találja az érzékeny állományokat.

Az informatikai bűnözők gyakran a legokosabb és a legjobban képzett szakemberek közül kerülnek ki, akik úgy érzik, hogy a feladatukat képező rutinszerű munkánál jobbak a képességeik. Ez különösen a fiatalabbaknál fordulhat elő, akiknek még nincs professzionális felelősségérzetük. A motiváltság, a munkahelyi kihívás magas szintjének fenntartása elkerülhetővé teszi ezt a biztonsági problémát.

Az informatikai bűnelkövető azonban nem szükségszerűen jól képzett szakember, lehet egy kis beosztott is, aki egészen véletlenül jön rá a lehetőségeire: "Jé, a géppel ezt is meg lehet csinálni!" Amennyiben elégedett és lojális, akkor ezzel az újonnan megszerzett tudással nem fog ártani. Ha viszont sérelem éri, akár több hónappal később is — sőt, az intézménytől kilépve, sokszor pont a konkurencia kötelékében — felhasználhatja tapasztalatait.

Az informatikai bűnözők sokszor a bizalmi pozícióban lévők köréből kerülnek ki, akik az általuk jól ismert, normális munkarutinokat használva árthatnak a rendszernek. Bármely biztonsági terv esetén ezen egyének tevékenységét kell gondosan felügyelni szoros ellenőrzéssel és hatékony nyilvántartással.

A bűneseteket legtöbbször nem egyedül követik el, ezek felében bűntársak működnek közre, mivel az egyén rátermettségét meghaladó képességekre lehet szükség, sőt, egy intézményen belüli elkövetőnek külső partnerei is lehetnek (**2. ábra**).

Az emberi tényező adminisztratív szabályozásának igen jó, már az '50-es években kidolgozott irodalma van, álljon itt néhány általános fogás. Rendkívül fontosak az egyértelmű, és részletes munkaköri leírások, továbbá elengedhetetlen a kötelezettségek szétválasztása, hogy senkinek ne lehessen jogosultsága a teljes rendszer feletti felügyeletre. Nagygépes környezetben a rendszerelemzők, az operátorok és az adatbevivők külön posztokat töltenek be és mindegyikük csak a rendszer egy részével foglalkozik. Hálózatba kötött gépeknél viszont létezik egy központi rendszermenedzser. Főként a külföldi bankoknál bevett szokás a rövid, de váratlan és kötelezően kivett szabadságok elrendelése. A sikkasztási folyamatokat egy-egy rövid szabadságolás derékba törheti. Elengedhetetlen, hogy a cégek a kulcspozíciókban lévő alkalmazottakat tegyék elkötelezetté, s hogy rotálják a beosztottakat a műszakok, a számítógépek vagy projektek között. A rendszernek legyen alapvető szolgáltatása a programok és adatállományok használatának naplózása. Fent kell tartani a fizikai biztonságot. Létesíteni kell tehát olyan helyeket, ahova még a programozók és a rendszerelemzők sem léphetnek be. Fenn kell tartani olyan jelszórendszert, amely csak a jogosultakat privilegizálja. Kilépő dolgozók esetén a cégvezetőknek azonnal be kell gyűjteniük a kulcsokat, azonosító kártyákat és egyéb biztonsági eszközöket, s törölni kell az általuk használt jelszavakat.

Az internetes fenyegetésekről

Mivel az internet természetéből következően a szó szoros értelmében az egész világ számára nyitott, bizonyos alkalmazások — mint például üzleti tranzakciók lebonyolítása, vagy éppen államigazgatási ügyek intézése — számos problémát vetnek fel az információcsere titkosságát és a hozzáférés megfigyelését, ellenőrzését illetően. Ezek ugyan technikailag bizonyos mértékig megoldhatók a tárolt és a továbbított adatok titkosítását, rejtjelezését („kódolását") szolgáló eszközökkel, de mégsem hagyhatók figyelmen kívül. A biztonság és a kockázatelemzés szempontjából teljesen kockázatmentes állapot az interneten sem lesz soha elérhető!

Az interneten kétféle bűncselekményt lehet elkövetni. Az egyik a hagyományos bűncselekmény, melyhez az internet — hasonlóan más eszközökhöz — csupán egyszerű kommunikációs eszközül szolgál (nem informatikai bűncselekmény például az információátadás egy ékszerüzlet kirablásához). A másik, amelyben magát a hálózatot és a számítástechnikai eszközöket használják fel jogellenes célok érdekében (informatikai bűncselekmények, főképp csalások). Ez ugyanakkor nem jelenti azt, mintha a hálózat mentes lenne a nem informatikai bűncselekményektől. A kábítószer-kereskedelemmel kapcsolatos információk, valamint a terrorista cselekményekhez és a maffiatevékenységhez adott instrukciók mellett nagy mennyiségű pornografikus anyag is van forgalomban a hálózaton. Azon túl, hogy ezek támadást jelentenek a közrend és a közerkölcs ellen, felmerül a kiskorúak számára való hozzáférhetőség kérdése is. Jelen vizsgálatunk körén ez

1. ábra. A bűnelkövetők

utóbbiak ugyan kívül esnek, de az informatikai bűncselekmények nagy mennyisége arra késztet minket, hogy figyelmünket a „nem-hagyományos" kérdésre összpontosítsuk.

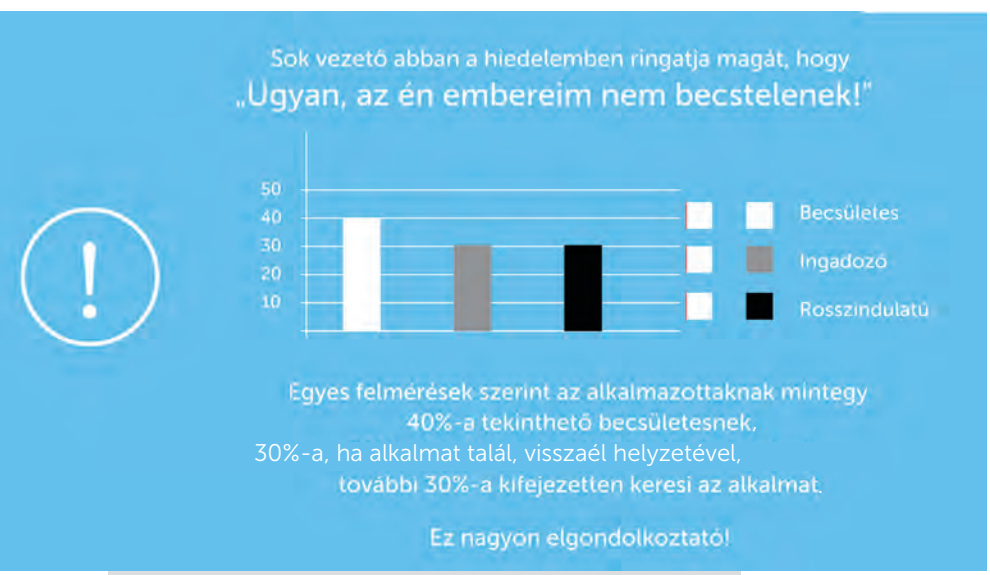
Az informatikai bűncselekmények vonatkozásában négy olyan magatartástípust érintünk, amelyek káros hatással lehetnek az internet-felhasználókra:

Engedély nélküli hozzáférés (csatlakozás): Gyakran a bűncselekmények első lépését alkotja, és olyan felhasználót feltételez, aki engedély hiányában tudatosan csatlakozik rá egy hálózatra, kiszolgálóra vagy fér hozzá egy fájlhoz (például egy email postafiókhoz), vagy olyat, aki véletlenül létesít csatlakozást, fér hozzá valamihez, de tudatosan úgy dönt, hogy fenntartja az engedély nélküli kapcsolatot.

Kárt okozó tevékenység vagy kárt okozó anyagok közzététele: Ha a bűnelkövető egyszer bejutott egy kiszolgálóba, lehetősége nyílik, hogy fájlokat tulajdonítson el,

azokat lemásolja, vagy kárt okozó információt terjesszen, mint például vírusokat vagy férgeket. Annak ellenére, hogy az ilyen magatartás nem sorolható be egyértelműen egyetlen pontosan meghatározott jogi kategóriába sem, gyakran minősítik szerzői jogi kalózkodásnak (az adatok eltulajdonítása, eltávolítása és használata az adatok tulajdonosának tudomása nélkül) vagy szabotázsnak (az adatok vagy a szoftverek megváltoztatása, módosítása vagy megsemmisítése, amelynek hatásaként megbénul a rendszer vagy a kiszolgáló tevékenysége az interneten).

Információ illetéktelen elfogása: Ebben az esetben a hacker, észlelve az (interneten) továbbított elektronikus impulzusokat, meg tudja szerezi a nem neki szánt információt. Amikor az ilyen törvénytelen információszerzés



2. ábra. Az „emberi tényező"

nem az illetéktelen hozzáférés keretében történik, rendkívül nehéz felderíteni. Megjegyzendő, hogy a fénykábelek egy-egy aknafedél alatt igen könnyen „tapperelhetők".

Előnyös szolgáltatás nyújtása közben adatlopás: A legközismertebb adathalászati tevékenységet bátran nevezhetjük a Facebook „Zuckerberg-cselének". Mi történt a közelmúltban? A kongresszusi meghallgatáson ötből kettőre csak kínos, elfogadhatatlan magyarázkodást kaptak a szenátorok.

Hiába a rengeteg figyelmeztetés, az elrettentő példák, sokan még mindig bíznak az ajánlkozásuk és leírásaik szerint csodatevő programokban. Ezek vagy totálisan feleslegesek, vagy kártékonyak — több a kár, mint a haszon, az viszont látványos...[1].

Álljon most példaként a Microsoft igen kiváló adatbázis-kezelője az MS Access, melynek van olyan kimeneti alakja, hogy az értékes szellemi tulajdont jelentő programot kódolva rejti el. Így az mdb (Microsoft Data Base) kiterjesztésű fájl mde (Microsoft Database Encryted) formában kerül forgalomba — az újabb verziók accdb illetve accde-ként. Na már most, ha rákérdezünk a keresőben a kulcsszavakra, hogy „convert accde to accdb" a negyvenkétezer találat alapján majdnem biztosan máris alkalmazhatunk egy trójai falovat!

A [2]-es publikáció szerint utánanéztek a fenti dolognak, de nagyon úgy tűnik, hogy ingyenes (és megbízható) megoldás erre nem létezik. Még a fizetős változatok sem képesek teljesen visszaállítani a forrásfájlt, legfeljebb arra van esély, hogy az adattáblákat importálhatják a titkosított fájlból.

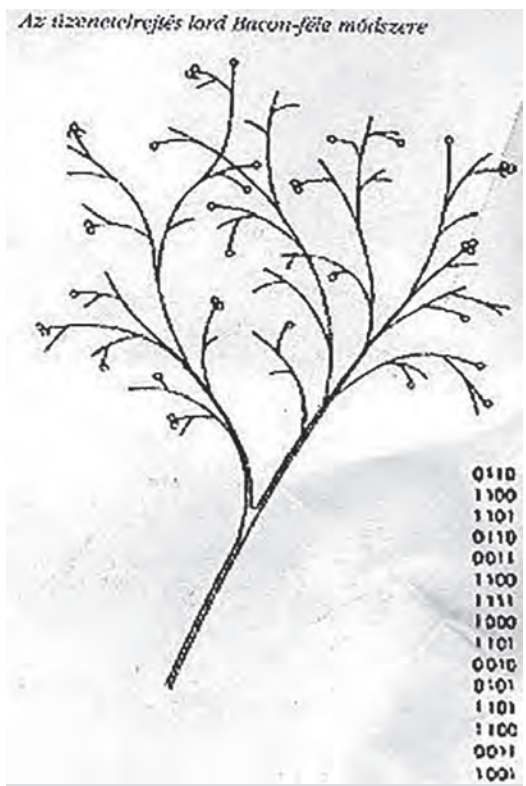
A kriminalitás napjainkban tapasztalt mértékű intenzitását részben az ellene folytatott küzdelem nehézségei magyarázzák; nemzetközi szinten általában, de az interneten különösen. Ezek közül az első a jogellenes cselekmény felderítésében és elkövetőjének megtalálásában áll. Az informatikai szabotázscselekményeket gyorsan végrehajtják, de a kiváltott funkciózavar következtében általában gyorsan fel is fedezik. Ugyanez nem mondható el az engedély nélküli hozzáférésről, az információ-elfogásról, vagy a kalózkodásról. Az interneten tevékenykedő szereplők sokfélesége használó, hozzáférés-szolgáltató, szolgáló, kiszolgáló-rendszeroperátor stb.) nem teszi egyszerűbbé annak meghatározását, kit terhel a büntetőjogi felelősség. Így megállapítható azon felhasználó büntetőjogi felelőssége, aki szándékosan terjeszt el egy vírust valamely kiszolgálón, de bizonyos esetekben a kiszolgáló büntetőjogi felelőssége is. A nemzetközi informatikai bűnözés együtt fejlődik az internettel. A használók a világ minden táján megtalálhatók, és így igen nagy a valószínűsége annak, hogy a bűnelkövető és az áldozat különböző országok eltérő törvényi szabályozása alá tartozik majd. Habár a nemzetközi jogi együttműködési megállapodások és a kétoldalú kiadatási szerződések igyekeznek orvosolni a nemzetközi bűnözés által okozott problémák egy részét, de ezen igyekezet gyakran ütközik korlátokba.

Ha modemed van, távozz!

A kívülről történő betörésekre hivatkozva — mint a belső hacking utáni második legnagyobb biztonsági kockázatra — az igazán profi cégek azonnali elbocsátással

büntetik, ha valakinek modem van az íróasztalán. Itt internet-hozzáférés csak a cég megfelelően (tűzfallal) védett hálózatán legális. Sok informatikai betörőprogram használ egy „háborús tárcsázásnak" nevezett technikát, amikor a gép kipróbál több ezer telefonszámot is egy tétlen modem megtalálása céljából. Ha a tulajdonos éppen nem használja a gépét, akkor a hacker hatásosan „el tudja fogni", és hozzá tud férni ahhoz a hálózathoz, amelyhez az adott számítógép kapcsolódik.

Magától értetődik, hogy a jog nem hagyja figyelmen kívül a nemzetközi bűnözés meredeken emelkedő tendenciáját. Az e tárgyban született nemzetközi kezdeményezéseken felül az amerikai és a kanadai jog az európai országok többségéhez hasonlóan kriminalizálta a fent említett háromféle informatikai magatartást, vagyis az engedély nélküli hozzáférést (csatlakozást), a kárt okozó anyagok terjesztését és az információ engedély nélküli elfogását. Itt és most nem bocsátkozhatunk a részletekbe, csak utalunk az [2]-től [4]-es publikációkra. Ez utóbbit **3. ábránkon** kiegészítjük a lord Bacon-féle másik — és meghökkentően egyedi — rejtjelező módszerrel.



3. ábra. Lord Bacon második rejtjelező módszere

Az IT-biztonság komplex fogalma akkor valósul meg, ha a szervezet az újnál újabb fenyegetések ellen dinamikusan kezeli az informatikai rendszerrel kapcsolatba kerülő humán erőforrásokat (vezetők, fejlesztők, kezelők, adminisztrátorok, biztonsági szakemberek, stb.); az informatikai folyamatokat megvalósító konkrét számítástechnikai eszközöket, rendszereket; az informatikai rendszerek környezetét (objektumok elhelyezése, tápellátása, kommunikációs kapcsolatai, stb.); s a rendszerekre, üzemeltetésre vonatkozó törvényeket, szabályozásokat, előírásokat, dokumentációkat, biztonsági elveket (koncepció, stratégia, „politika").

A legtöbb intézménynél a védelem több okból is távol áll attól, hogy kielégítőnek nevezhessük. Egyrészt a felső vezetők nincsenek teljesen tisztában azzal, hogy a biztonság elsősorban az ő felelősségük és annak ki kell terjedni az egész szervezetre (tisztelet a kivételnek, amint jelen vizsgálatunkban észleltük), másrészt úgy gondolják, hogy a biztonság csupán műszaki kérdés, pedig a legbonyolultabb biztonsági rendszert is egy célratörő, főleg megfelelő pozícióban lévő egyén fel tudja törni. A biztonság a munkahelyeken kezdődik és nem csupán a nagy központi feldolgozó csarnokokra vonatkozik. A védekezés kényelmetlenséget okoz, mivel a nem jogosult felhasználók kiszűrésére alkalmazott eljárások a legitim felhasználókat is meggyanúsítva, hátráltatják a munkát. Az intézmények pedig azt szeretnék, hogy a róluk kialakult kép kedvező legyen, ennélfogva nagyon sok informatikai bűneset azért nem kerül a nyilvánosság elé, mert a felső vezetők félnek a cég „imázsvesztésétől".

A jó védelmi rendszer az intézmény működésének veszélyeztetését minimalizálja; különböző jogosultságot biztosít a felhasználók igénye és felelőssége szerint; a felhasználókat egyértelműen felelőssé tudja tenni az informatikai akciókért; szétválasztja a felhasználókat, a programokat, az adatállományokat és a forrásokat; s azonosítja a visszaélési kísérleteket, és védekező lépéseket tesz.

A piacgazdaság új, komplex követelményeket támaszt és kínál — elég csak gondolnunk az elektronikus postára, vagy (a hazánkban ugyan egyelőre nem túlzottan terjedő) elektronikus kereskedelemre. Ezekhez elengedhetetlenek a szigorú azonosítási eljárások, a hozzáférés-szabályozás és a szervezet adott infrastruktúrájával való együttműködés képessége. Vegyünk ehhez az olyan műszaki követelményeket, mint az adatok megbízható vétele és tárolása, a tartalomvédelem, a frekvenciasáv hatékony használata, az inter-operativitás, a minimális fogyasztás igénye, stb. Az államigazgatás további igényeket támaszt: megbízható, ugyanakkor hatékony rejtjelezést! Az USA-ban ehhez a Szövetségi Adatfeldolgozási Szabvány (Federal Information Processing Standard — FIPS) 140-2 jelzésű, hiteles, minősített eszközöket ír elő.

Tökéletes biztonság nincs, az mindig viszonylagos: azzal jellemezhető, hogy a rendszer mennyire képes ellenállni a fenyegetéseknek. Egy adatkezelő rendszer tehát akkor mondható biztonságosnak, ha a fenyegetések nyomán jelentkező kockázat (risks) megfelelő

intézkedések révén elviselhető mértékűre csökkent. Ezért mindenekelőtt a következő kérdést kell megfogalmaznunk: milyen szigorú biztonsági követelményeket kell teljesítenünk ahhoz, hogy vagyonunkat biztonságban tudhassuk? A követelmények megfogalmazását követően arra kell választ találnunk, hogy milyen vagyonunk tényleges biztonsági helyzete. Végezetül bizonyosságot kell szereznünk; hogy nyugodtan alhassunk, meg kell tudnunk: mennyire bízhatunk abban, hogy vagyonunk a meghatározott színvonalon biztonságban van. Lényegében ezek a biztonság menedzselésének alapkérdései.

A biztonság tanúsítása során elfogulatlan, független tanúsító megvizsgálja a kívánt rendszert vagy terméket és igazolja, hogy az az előírt követelményrendszernek, a meghatározott biztonsági szintnek megfelel-e vagy nem. A tanúsítás akkor értékes, ha nemcsak önmagában értelmezhető, hanem összehasonlítható; azaz, ha nem eseti, hanem általánosan elfogadott, egységes, szabványos követelményrendszer az alapja. A tanúsítás értékét tovább növeli, ha azt az állam által erre felhatalmazott, jegyzett cég végzi. Az állami felhatalmazás esetében ugyanis arról van szó, hogy a céget és az általa használt eljárást állami szerv megvizsgálta, alkalmasnak találta, és az alkalmasságot folyamatosan felügyeli. Tanúsítani — értelemszerűen — csak létező adatkezelő rendszert vagy terméket lehet.

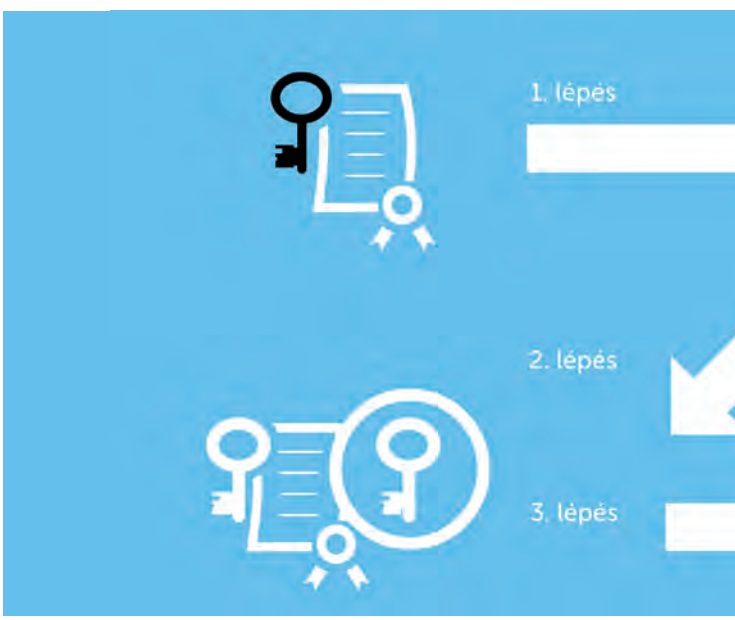
A biztonsági helyzet értékelése során elfogulatlan, független vizsgáló megismeri az adatkezelő rendszer vagy termék biztonsági helyzetét és valamilyen módszerrel kimutatja az elfogadhatatlan kockázatokat jelentő gyenge pontokat. Két szokásos munkamódszere az ún. követelményes és a kockázatelemzéses. Nemcsak meglévő, hanem tervezett helyzet biztonsága is értékelhető: a munka tehát mind létező, működő, mind tervezett rendszer vagy termék esetében elvégezhető.

Követelményes vizsgálat esetén az alap valamilyen előzetesen meghatározott követelményrendszer. A vizsgáló azt veszi számba, hogy mely előírt követelmények nem teljesülnek.

A kockázatelemzéses vizsgálat első lépése a későbbi szűken értelmezett kockázatelemzés alapjának rögzítése: az adatok és a működés, azaz a munkafolyamatok értékeinek számszerűsítése. A gyenge pontok és a fenyegetések meghatározását követően, a kockázatelemzés a fenyegetések által okozott lehetséges kár nagysága, és a bekövetkezés gyakorisága alapján kimutatja a biztonsági szempontból legkritikusabb területeket.

Itt hívjuk fel a figyelmet arra, hogy csak akkor szabad a kockázatelemzéses munkamódszert alkalmazni, ha annak számszerű alapjai megteremthetőek, valamint rendelkezésre állnak statisztikák a bekövetkezett káreseményekről. Ha a számszerű alapok ésszerű mennyiségű munkaráfordítással nem teremthetőek meg, vagy nincsenek statisztikák, a követelményes munkamódszert célszerű, illetve kell választani.

A biztonsági követelmények meghatározása a fent írtakhoz hasonlóan, két fő munkamódszerrel lehetséges. A biztonsági helyzet értékeléséhez hasonlóan, a mind meglévő, működő, mind tervezett rendszer vagy termék esetében elvégezhető. A biztonsági követelmények meghatározása itt azt jelenti, hogy a vizsgáló megismeri az adatkezelő rendszer vagy termék rendeltetését, a vele kezelt adatok körét, és ennek alapján előírja, hogy mely szabványos biztonsági osztály követelményeit kell a rendszernek vagy terméknek teljesítenie.



A kockázatelemzéses munkamódszer esetében a vizsgáló — kockázatelemzéses munkamódszerrel — kimutatja az adatkezelő rendszer vagy termék biztonsági szempontból legkritikusabb területeit; a biztonsági követelményeket a feltárt biztonsági hiányosságok képezik. A biztonsági vizsgálatok nyomán értelemszerűen a biztonságot növelő intézkedési javaslatok is készülhetnek. A biztonsági követelmények meghatározására, helyzetének értékelésére, valamint fokának tanúsítására napjainkban számos munkamódszer, szabvány, ajánlás áll rendelkezésre. Amint kifejtettük, a jó szakember számára napjainkban elengedhetetlen ehhez jól megalkotott relációs adatbázis-kezelő használata (MMM, 2004. január, p. 58 - 59).

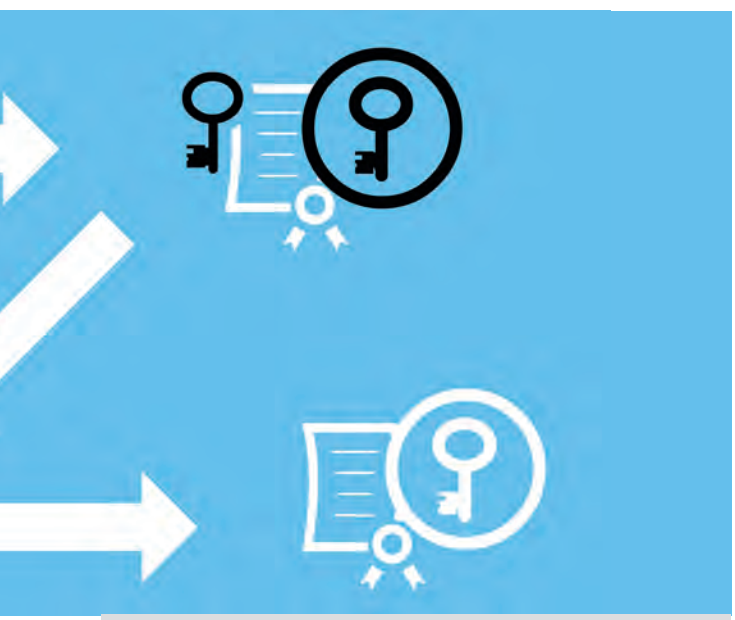
A rossz protokoll

A mobil eszközök azért jelentenek új biztonsági kihívást, mivel pontosan hordozhatóságuk korlátozza a feldolgozási sebességet, a tárolókapacitást és magát a

drótnélküli rádiókommunikációs csatornát. A rossz protokoll pedig feltörhetővé teszi a mégoly megfejthetetlennek tűnő rejtjelezést is — nézzük hogyan!

A rejtjelezés hatékonysága az alkalmazott algoritmustól, a rejtjelezés helyétől és idejétől, valamint a kulcskiválasztás kritériumaitól, generálásától, szétosztásától és tárolásától függ. Egy rejtjeles szöveg (kriptogram) akkor lehet feltétlenül biztos, ha az egyetlen helyes megoldáshoz sem ad elégséges információt.

Shannon már a '40-es években kimutatta, hogy az egyetlen, matematikailag feltétlenül biztos rejtjelező eljárás a Vernam-féle "egyszeri szalag". Nevét onnan kapta, hogy az ötvenes években két lyukszalagot kombináltak össze: az



4. ábra. Kommunikáció teljesen titkos magánkulcsokkal

eredeti szöveget, és egy véletlenszám által generáltat. Ennek máig is ható, nagy jelentőségét bizonyítja, hogy a Moszkva-Washington "forró drót" ma is ezt az elvet — technikailag kissé modernizálva — alkalmazza. Eszerint egy rejtjeles szöveg (kriptogram) akkor lehet feltétlenül biztos, ha az egyetlen helyes megoldáshoz sem ad elégséges információt. Ehhez Shannon egy "unicitási távolságot" definiált, ami azt jelenti, hogy a rejtjelezendő szöveg redundanciájának meg kell haladnia a kulcs információját. Tekintve, hogy az egyszeri szalag unicitási távolsága végtelen, ezért ez az egyetlen matematikailag feltétlenül biztos rendszer.

Emberi tényező

Persze lehet mégoly matematikailag biztos ez is, a kulcsként szolgáló „szalagot" futárral, lepecsételt diplomatatáskában kell a másik félnek átadni, hisz akár a „drótos", akár a műholdas átvitel lehallgatható, meghamisítható, elirányítható. És itt jön megint az „emberi tényező"...

Most egy — elsőre talán viccesnek ható — ógörög módszerre térünk ki. Saját technikai eszközeikkel ők alkalmazták először a háborúkat is eldöntő „matematikailag biztos egyszeri szalagot" (legalábbis az elvet — és van-e valami, amit a görögök nem?).

Nos, lekopaszították egy emberszámba alig vett rabszolga fejét, és szép görög kalligráfiával rátetoválták az üzenetet. Ezután mintegy két hetet kellett csupán várni hajának kellő hosszúságú növekedésére. Útra kelt, és áthaladt az ellenséges területeken is — a módszer igazán egyszeri lehetett!

Beszéljünk most két — a második világháborúban alkalmazott — az ellenfelek által megfejthetetlennek bizonyult módszerről is!

Az Egyesült Államok hadserege navahó indián nyelven küldte a hadászatilag sorsdöntő információkat, sőt még azon belül is „transzformáltak" — például a sas jelentette a repülőgépet, medve a tankokat, stb.

A németek a teljesen mechanikus Enigma rejtjelezője előtt pedig megállt a szövetségesek tudománya. Erről a szerzőnek két, egymásnak ellentmondó információja van. Jó pár évvel ezelőtt napilap írt arról, hogy a szövetségesek egyszerű lopással jutottak a megfejtéshez. A németek elkövették azt a fatális tévedést — mondhatjuk banánhéj-hatásnak is — hogy postai úton továbbították a készüléket. Lengyelországban egy szombati postazárást követően vasárnap hajnalig elég volt az idő a megfejtésre, aztán mintha mi sem történt volna, ment minden tovább a németeknek a biztosnak vélt úton. És emberezrek élete múlott ezen...

Most viszont [5]-ben arról olvashatunk, hogy Alan Turing és Goldon Welchmann „Bomba" nevű gépükkel a Bletchley Parki angol lehallgató központban 1940 közepétől rendszeresen tudták olvasni a német légierő üzeneteit, majd a szövetségesek egy U-110 tengeralattjáró elfogásával jutottak a géphez, és ez tovább könnyítette Turing munkáját.

Visszatérve a mai műszaki kérdésekre: jelenlegi ismereteink szerinti egyszeri szalagon kívül az összes többi, matematikailag nem feltétlenül biztos rejtjelezés hatékonysága is nagyban függ az alkalmazott algoritmustól, a rejtjelezés helyétől és idejétől, valamint a kulcskiválasztás kritériumaitól, generálásától, szétosztásától és (főleg hierarchikus) tárolásától. Sőt azt kell mondani, hogy aktív támadások ellen a titkosító transzformáción túl megfelelő, további szabályokkal kell gondoskodni a manipuláció megnehezítéséről — ezek a kripto-protokollok.

A „sikeres" elrontás

Még a legerősebb rejtjelező transzformáció sem nyújt kellő védettséget hibásan tervezett protokollkörnyezetben, ezért ebbe a körbe tartozik a partner hitelességének megállapítása, a megszemélyesítés felfedése, sőt megakadályozása is. Álljon itt egy példa, hogy a napjainkban "legerősebbnek" ítélt kettős kulcsú (például RSA) rejtjelezést rossz protokollal hogyan "sikerülhet" elrontani. Például egy "sima" kód-kulccsal az adó, míg egy másik kóddal a vevő titkosít. Csakhogy a kulcsok eltéríthetők — nem biztos, hogy az kapja, akinek az adó szánta.

Ezzel szemben az MIT-n évtizedekkel ezelőtt kifejlesztett Kerberos a maximális bizalmatlansággal él, ugyanakkor minimális terheket rak a felhasználókra (**4. ábra**).

A Kerberos használója egyszerű, — titkosítást nem igénylő — rejtjelezés nélküli szöveget küld a jogosultsági szerverhez, amely válaszul erre hitelesítő adatokat küld vissza. Ezelőtt azonban ezeket a hitelesítő adatokat rejtjelezi egy olyan kulccsal, amelyet csak a használó és a Kerberos ismer. Ezt a titkos jelszót rejtjelezett formában a kulcsosztó állomás (KDC) adatbázisában tárolják. Amint ez megérkezik a használóhoz, ő a kulccsal visszafejti. Amennyiben valamilyen oknál fogva nem tudná visszafejteni, máris képtelen lesz a további lépésekre. Így a jogosultság elnyerése a kliens munkaállomásán és nem a Kerberos biztonsági szerver szintjén történik.

Dollármilliós incidensek

Ma a nagyobb cégek mindössze harmada képes mérni és értékelni saját informatikai biztonsági mutatóit, noha a biztonsági incidensek évente dollármilliós kárt okoznak nekik. Ezt állapította meg 2002-ben a KPMG első nemzetközi információbiztonsági felmérése. A KPMG munkatársai világszerte olyan cégeket vizsgáltak, amelyeknek éves forgalma meghaladta az 50 millió dollárt. A felmérés szerint a cégek a vírusokat és az információs rendszert illegálisan feltörő behatolókat (hackereket) jelölték meg a legfőbb veszélyforrásnak. A vizsgálatok azonban azt mutatták, hogy a vírusok (a cégek 61 százaléka számolt be vírustámadásról) után a technikai berendezések lopása okozza a legtöbb kárt (38 százalék). Hackertámadást a cégek 12 százaléka jelentett — ez csak a hatodik leggyakoribb veszélyforrás.

Noha a vizsgált cégek informatikai költségvetésük 10 százalékát fordítják a biztonságra, azt már nem ellenőrzik, megtérül-e ez a ráfordítás. Egy-egy informatikai biztonsági probléma kezelése átlagosan 108 ezer dollár kiadást jelent a társaságoknak. Ennek ellenére a legtöbb vállalat túl magabiztos saját biztonsági színvonalát tekintve: 58 százalékuk tartja úgy, hogy minden ésszerű lépést megtett a védekezésért, ugyanakkor közülük is minden tizedik elismerte, hogy semmilyen formában nem méri a biztonsági lépések hatékonyságát, sőt 52 százalékuk nem rendelkezik olyan rendszerrel, amely észleli az illetéktelen behatolást. A valódi teljesítményt mindössze a cégek mintegy harmada (35 százalék) képes mérni és értékelni, míg a vállalatok több mint fele azt sem tudta megmondani, mennyit költ az informatikai biztonság megteremtésére.

VÖRÖS GÁBOR

IRODALOM

[1] Ne dőljünk be a hókuszpókusz szoftvereknek — Chip Magazin 2014/7 p.110
[2] Személyes közlés Győri Ferenc főszerkesztő úrtól — Chip Magazin, MediaCity Kft. 2019. május
[2] A számítógépes információbiztonság alapjai — LSI Oktatóközpont 2001
[3] Nem kell feltalálni — Információbiztonsági szabványok — Műszaki Magazin 2005/10
[4] Kiváló leírás a kriptográfiáról: *https://bit.ly/2kmFOwD*
[5] A második világháború története — Ringler Axel Springer Magyarország Kft 2019 p. 44
[6] Davies — Price: Security for Computer Networks — John Wiley & Sons, Second Edition, 1989
[7] Shannon: Communication Theory of Secrecy Systems — Bell System Technical Journal vol 28. p. 656, 1948. október
[8] Hunt,C: TCP/IP Network Administration — John Willey's London, 1998
[9] A megfigyelések és lehallgatások kora — Chip Magazin, MediaCity Kft. 2010. június
[10] Biztonsági tippek profiktól — Chip Magazin, MediaCity Kft. 2010. június

E SZÁMUNK SZERZŐI

BABINSZKI EDIT: PhD, geológus, Magyar Bányászati és Földtani Szolgálat, Budapest; CSABA GYÖRGY: professor emeritus, az MTA doktora, Budapest; ILLÉS ERZSÉBET: PhD, űrkutató csillagász, összehasonlító planetológus, CSFK, Konkoly Thege Miklós Csillagászati Intézet emerita kutatója; KAPUSI FELÍCIA: biológus, MTA Ökológiai Kutatóközpont, Duna Kutató Intézet; MIKA JÁNOS: egyetemi tanár, az MTA doktora, Eszterházy Károly Egyetem, Eger; MITRE ZOLTÁN: MSc hallgató, Eszterházy Károly Egyetem, Földrajz és Környezettudományi Intézet, Eger; PATKÓ LÁSZLÓ: vadbiológus, WWF Magyarország; RABB MÁRTON MIHÁLY: kutató biológus, Eötvös Loránd Tudományegyetem, Budapest; VÖRÖS GÁBOR: villamosmérnök, a digitális technika doktora; ZOMBORI PÉTER: MSc hallgató, Eszterházy Károly Egyetem, Földrajz és Környezettudományi Intézet, Eger.

KÖVETKEZŐ SZÁMUNKBÓL

Novemberi számunkban Eötvös Lorándra emlékezünk halálának 100. évfordulója alklamából.