KIFÜ

KÖZÉRTHETŐEN nem csak AZ IT BIZTONSÁGRÓL

Információ és IT biztonsági kultúra fejlesztése a közigazgatásban

ÚJ SZÉCHENYI TERV

KÖZÉRTHETŐEN (nem csak) AZ IT BIZTONSÁGRÓL

Jelen tájékoztató kiadvány célja, hogy elősegítse a biztonságtudatos szervezeti kultúra fejlesztését a közigazgatásban dolgozók számára. Ezt az alapvető elektronikus információbiztonsági kockázatok bemutatásával, megelőzésük és kezelésük ismertetésével teszi a felhasználók, az informatikusok és a vezetők nézőpontjából!

szerző: Horváth Gergely Krisztián, CISA CISM

Budapest, 2013

Tartalomjegyzék

Ajánlás

A KIFÜ ELNÖKÉNEK AJÁNLÁSA AZ OLVASÓKHOZ

A kiadványt kidolgozó projekt gazdájaként, a Kormányzati Informatikai Fejlesztési Ügynökség elnökeként köszöntöm Önöket!

A hazai közigazgatás fejlesztése a működést és a szervezetek együttműködését támogató eszközként, és az állampolgároknak nyújtott szolgáltatások csatornájaként is tekint az információs és kommunikációs technológiákra.

Ugyanakkor közszférán belül is egyre többször kell szembesülnünk azzal, hogy az adatok nincsenek biztonságban. Ezek az esetek sokszor informatikai hiányosságokra, illetve a biztonságtudatosság hiányára vezethetőek vissza. Az informatikai ismeretek hiányosságai kockázatot jelentenek a közigazgatás minden szintjén. A kockázatok a szervezeteken belül a felhasználók tudásszintjével, és jogosultságaik mértékével arányosak: a kockázatok a hamis lánclevelek továbbküldésétől kezdve a jelszavak átadásán keresztül akár az idegen államok információszerzésének lehetővé tételéig terjednek.

Az emberi tényező okozta kockázat rendkívüli információbiztonsági események csökkentésére az egyik leggazdaságosabb és igazoltan hatékony módszer a felhasználók munkaköri és felelősségi szintjének megfelelő továbbképzés, és biztonsági felkészítés. A felhasználók hiányos biztonságtudatosságából eredő veszélyeket tehát a közigazgatásban dolgozók felkészítésével, jó eséllyel, meg is előzhetjük. Az Államreform Operatív Program által finanszírozott ÁROP 1.1.17 projekt egyik lényeges eleme jelen útmutató, mely nem kevesebbre vállalkozik, mint hogy mindenki számára érthetővé teszi az információ és IT biztonsági alapismereteket, és gyakorlati javaslatot ad a legjellemzőbb esetek kezelésére.

Reményeink szerint minden közigazgatásban dolgozó kolléga számítógépére eljut ez a tájékoztató, és hasznos olvasmányként lapozzák fel, ha segítségre van szükségük a helyes döntések meghozásához az elektronikus információ biztonság területén.

Kiadványunk olvasásához kívánok hasznos időtöltést!

Szijártó Zoltán
Elnök

Bevezetés

A TÁJÉKOZTATÓ CÉLJÁNAK ÉS FELÉPÍTÉSÉNEK BEMUTATÁSA

Informatikai biztonság napjainkban

A felhasználók szempontjából jellemző, hogy az új készülékeket, webes szolgáltatásokat egyre többen veszik igénybe az életük egyre több területén. A népszerű készülékek (táblagépek, okostelefonok) könnyítik az életünket, ehhez azonban több különböző szolgáltatás – személyes információk – adatait szinkronizálják akár néhány perces gyakorisággal. Ennek a kényelemnek az a következménye, hogy a magán és a munkavégzéssel összefüggő adatok keverednek, és a biztonságuk is sérülhet.

A világhálón elérhető szolgáltatások fejlődésével, a közösségi funkciók rendkívül dinamikus térnyerésével összefüggésben a biztonsági kockázatok számossága és a hatásuk mértéke is nő. Ma már természetes sokunknak olyan személyes adatok megadása akár nyilvános weboldalakon is, amelyet korábban csak közeli ismerőseinkkel, munkatársainkkal osztottunk meg. Egyes szolgáltatások világszintű népszerűségével, milliós felhasználói számukkal egy szoftver hiba, vírus vagy kártevő program károkozásának mértéke nagyságrendekkel nőhet.

Hazai információbiztonsági felmérések (ISACA-HU, 2011) eredményéből látható, hogy a magyarországi helyzet sem jobb. Az információbiztonsági stratégia fontosságát részben felismerték a hazai társaságok, de kevés konkrét lépést tettek a megvalósítás érdekében ugyanakkor csökkent a területre fordítható forrás.

A közigazgatáson belüli tapasztalatok azt mutatják, hogy megkezdődött a szükséges szabályozások kiadása jogszabályi szinten, a szakmai irányítás és felügyelet intézményrendszerének kialakítása és felkészülnek a szakemberek továbbképzésére is. A közeljövő feladata lesz ezek megvalósítása, és a keretek tartalommal való feltöltése az egyes szervezetek szintjén. Nem egy év alatt fogja elérni a legtöbb szervezet a szükséges biztonsági szintet, mert a jogszabály lehetővé teszi annak fokozatos teljesítését, ugyanakkor a fokozottabban védendő rendszerekre szigorúbb követelményeket támaszt, így azok védelme prioritást élvez.

A tájékoztató célja

A kiadvány az Európai Unió támogatásával az Államreform Operatív Program finanszírozásával az ÁROP 1.1.17 pályázatnak megfelelően készült el. Jelen tájékoztató kiadvány célja, hogy elősegítse az elektronikus információ biztonsági kultúra fejlesztését a közigazgatásban.

A cél elérését a témakör alapvető információinak jól felépített szerkezetben, közérthető nyelvezettel való közzé adásával törekszik elérni a közigazgatás dolgozói számára munkavégzésük jellemzőbb élethelyzeteit figyelembe véve. Ezáltal az Olvasó magabiztosan lesz képes felismerni az informatikai biztonsági kockázatokat a legújabb műszaki eszközök esetén is (pl. okostelefonok), és megfelelő megoldásokat választhat az elkerülésükre, illetve ha már bekövetkezett, akkor a baj csökkentésére.

Ennek megfelelően az Olvasó megismerheti a biztonság alapelveit, az információbiztonsági kockázatok sajátosságait, a kerülendő felhasználói szokásokat, és a javasolt kockázatkezelési módszereket az átlagos felhasználók, az informatikusok és a vezetők szemszögéből.

Segítség az IT biztonság megismeréséhez

A kedves Olvasó első látásra meglepődhetett azon, hogy a tájékoztató anyag ilyen vastag, talán első gondolata az volt, hogy miért is lenne ilyen sok információra szüksége az IT biztonságról. Sajnos az elmúlt másfél évtizedben egyre nőtt az informatika és a világháló veszélyeinek száma, és összetettsége, és nőtt az általuk okozott kár mértéke. Kiemelkedően fontos tehát a károk megelőzése. A tapasztalat azt mutatja, hogy a leghatékonyabb fegyver az internetes bűnözés elleni harcban a tudás: tudni, hogy milyen veszélyek vannak, tudni, hogy mit tehetünk az ellen, hogy károsultak legyünk, és mit kell tenni, ha mégis bekövetkezik. A biztonság rajtunk múlik!

A kiadványunk azért készült, hogy segítse az Olvasót, hogy felvértezze magát. Bátorítjuk rá, hogy ismerkedjen a témakörrel, és az érdeklődésének és tudásszintjének megfelelő részeket ismerje meg először, majd ha szükségét érzi vegye elő újra, lapozza fel és használja a tudását a saját maga és munkahelye érdekében! Ideális esetben ez a kiadvány egy belső biztonságtudatosítási program kiegészítéseként, belső képzéssel egybekötve jut el az Olvasóhoz, ahol közvetlen lehetőség van az egyéni tapasztalatok megosztására és a felmerült kérdések megválaszolására. Javasoljuk, hogy ha kérdése merül fel a kiadványban olvasottakkal kapcsolatban keresse meg a munkahelye biztonsági vezetőjét, vagy információbiztonsági vezetőjét. Ők azok, akik hitelesen a munkahelyét veszélyeztető kockázatok ismeretében tudnak segíteni Önnek a megfelelő válaszok megadásában.

Egy lehetséges feldolgozása az anyagnak:

- az elektronikus információbiztonságban nem jártas kollegák számára az Alapvető biztonság fejezetek megismerése első olvasásra, majd a többi veszélyforrások áttekintését, hogy átfogó képet kapjanak. Fontos még az irodai informatikai eszközök és programok biztonságos használata.
- az elektronikus információbiztonságban jártas kollegák számára Bevezetés gyors áttekintését javasoljuk az a tartalomjegyzék alapján az esetleg nem ismert témák átolvasását, majd a számukra releváns veszélyek megelőzésük, és elhárításuk módszereinek megismerését és gyakorlati megvalósítását.
- az elektronikus információbiztonság kialakításáért és működtetéséért felelős informatikusok számára az általános információk mellett a Biztonságos üzemeltetés fejezet megismerése, majd a 2. mellékletben szereplő további információforrások egyéni vagy csoportos feldolgozása és akár belső ajánlások kialakítása.
- a munkahelyeken vezető beosztásban levő munkatársak számára a Biztonságtudatos vezetés fejezet megismerése és a napi gyakorlatba átültetése továbbá az 1. mellékletben felsorolt jogszabályok alkalmazása a saját szervezetére.
- az elektronikus információbiztonság irányításáért felelős vezetők számára a teljes kiadvány megismerése, a kiadvány és mellékleteiben hivatkozott információforrások felhasználásával munkahelyi biztonságtudatosító program indítása, illetve felülvizsgálata.

A tájékoztató felépítése

A dokumentum felépítése egységes szerkezetet követ. A fejezetek rövid szöveges összefoglalást tartalmaznak, majd témánként 1-2 oldal terjedelemben a bemutatott kérdések lényeges jellemzőit, kockázatait mutatja be közérthető egyszerűsítések segítségével. Ezen belül meghatározzák a problémát, példákkal szemléltetik, és megadják a lehetséges megelőzés, illetve védekezés módszereit.

A megértést jellemző képek, ábrák segítik. A dokumentumban való tájékozódást, illetve a kockázattal érintett területek egyértelmű azonosíthatóságát, és a kockázatok méretét vezérlő ábrák/piktogrammok (vizuális vezérlő elemekkel ellátott grafikai elemek) biztosítják.

Továbbá tartalmaz hivatkozásokat további szakmai anyagokra, melyek bővebben tárgyalják a kérdést. Ezért az informatikai biztonsági ismeretek alapismerete nélkül és középszintű ismeretével is jól forgatható olvasmány. Az a kedves Olvasó, aki nemzetközi informatikai biztonsági szakvizsgára készül, azért ne csak ezt a kiadványt használja, ott biztosan mélyebb ismeretekről kell számot adni.

A kiadvány kapcsán felmerült kérdésekre adott válaszokból egy tudásbázist (GYIK) építünk, és terveink szerint évente frissítjük a tájékoztatót is az aktuális kockázatok bemutatásával.

Az adott oldal címe (oldalminta)

Veszély bemutatása (Miről beszélünk?)

Jellemző hatása: Alacsony, Közepes, Magas

Mit veszélyeztet:

(a felhasználó, a rendszerműködés,
az információbiztonság,
és a nemzetbiztonság terén)

ILLUSZTRÁCIÓ / KÉP

Példák, érdekességek:

Veszély megelőzése:

Veszély elhárítása: (Mit tegyünk, ha bekövetkezik?)

További információ: hivatkozások

Alapvető biztonság

AZ INFORMÁCIÓBIZTONSÁG ALAPELVEINEK BEMUTATÁSA

IT biztonsági kérdés - felelek

Mi a biztonság?

Az információbiztonság kérdéseit taglaló média megjelenések és publikációk sok esetben nem szabatosan fogalmaznak, esetenként teljesen helytelenül használják, keverik a fogalmakat, ami akadályozza a téma pontos megértését. A következőkben törekszünk a fogalmak közérthető módon való tisztázására.

Kezdjük talán a leggyakoribb tévedéssel! Az adatvédelem és az adatbiztonság NEM szinonimái egymásnak! Adatvédelem alatt a személyes és érzékeny adatok jogszabályi (Avtv.) védelmét érti a jogalkotó, adatbiztonság alatt pedig a számítógépes rendszerekben tárolt, feldolgozott, vagy továbbított adatok biztonságának fenntartására kell gondolnunk.

A biztonság maga pedig egy a szervezet számára kedvező állapot, melynek megváltozása nem valószínű, de nem is kizárt. Azaz egy lakókörnyezet akkor biztonságos például, ha nyugodtan sétálhatunk haza az utcán nappal és éjjel egyaránt, nem kell folyton azt figyelnünk, hogy honnan ér minket támadás.

Az informatikai biztonság az informatikai rendszer olyan kedvező állapota, amelyben a kezelt adatok bizalmassága (confidentiality), sértetlensége (integrity) és rendelkezésre állása (availability) biztosított (CIA elv), valamint a rendszer elemeinek biztonsága szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos. Ahol

- bizalmasság: csak az arra jogosultak ismerhetik meg az információt;
- sértetlenség: az információ tartalma és formája az elvárttal megegyezik, beleértve az is, hogy az elvárt forrásból származik (hitelesség), igazolható, hogy megtörtént (letagadhatatlanság), egyértelműen azonosítható az információval kapcsolatos műveletek végzője (elszámoltathatóság), továbbá rendeltetésének megfelelően használható;
- rendelkezésre állás: az a tényleges állapot, amikor egy informatikai rendszer szolgáltatásai az arra jogosultak számára egy meghatározott időben rendelkezésre állnak és a rendszer működőképessége sem átmenetileg, sem pedig tartósan nincs akadályozva;
- zártság: az összes releváns veszélyt (fenyegetést) figyelembe veszi;
- teljes körűség: a rendszer minden elemére kiterjed a védelem;
- folytonosság: időben folyamatosan megvalósul a védelem;
- kockázatokkal arányosság: a rendszer várható működésének időtartamában a védelem költsége arányban van a lehetséges kárral.

Az információbiztonság tágabb fogalom, mint az IT biztonság. Beleértjük az információ minden – nem csak elektronikus – megjelenési formájának, az információs szolgáltatásoknak és az ezeket biztosító információs rendszereknek a védelmét.

Miért fontos az IT és az információbiztonság?

Az informatika korábban elképzelhetetlen módon könnyítheti meg a felhasználók életét, például kapcsolatot tarthatunk távol levő szeretteinkkel, és a közszférában is széles körben elérhetővé teszi a közigazgatás szolgáltatásait. Ugyanakkor, az informatika korábban elképzelhetetlen módon veszélyeztetheti az életünket (pl. számítógépes játékfüggőség, adatlopó kártevőprogramok), a szervezetek biztonságát (pl. adatszivárgás), és teheti sérülékennyé akár a létfontosságú infrastruktúra elemeket (pl. DoS támadás[1]).

Az információbiztonság helyzete sajátos, egyszerre van jelen egy szervezet minden területén, sőt, a feltételeinek megfelelő kialakítása és működtetése jóval túlmutat az információ biztonságos kezelésén. A szervezet minden erőforrásának, az embereknek, az eszközöknek, az információs rendszereknek, és más vagyontárgyaknak a szabályozását, viselkedését, használatát, ellenőrzését jelenti. Irányítása a felső vezetés felelőssége.

Az információval szemben elvárás, hogy a megfelelő időben, pontosan, és naprakészen álljon rendelkezésre, de csak azok számára, akik jogosultak megismerni azt. Ez az információ minden formájára igaz, azaz a szóban, a papíron, és az elektronikus formában tárolt, kezelt, feldolgozott és továbbított formáira egyaránt.

Általában az informatikától egyszerűen csak azt várja el mindenki, hogy működjön. Azt már nehezebb meghatározni, hogy pontosan ki mit ért ezen, de abban egyetérthetünk, hogy ne kelljen (túl sokat) várni a válaszra, ha valamit kérdezünk, és a rendszer válasza a feltett kérdésre reagáljon, pontos és hiteles legyen.

Ezeket az elvárásokat szakszerűen a COBIT[2] – az informatikai irányítás ISACA által kidolgozott de facto nemzetközi szabványa – így határozza meg:

- Eredményesség – az üzleti folyamat szempontjából jelentőséggel bír, időben helyes, ellentmondásmentes és használható.
- Hatékonyság – optimálisan (legtermelékenyebben és leggazdaságosabban) használható fel.
- Bizalmasság – engedély nélküli nem hozható nyilvánosságra.

[1] A szolgáltatásmegtagadásos (Denial of Service vagy DoS) támadás egy meghatározott alkalmazás, operációs rendszer ismert gyengeségeit, vagy valamilyen speciális protokoll tulajdonságait (gyengéit) támadja meg. Célja, hogy az alkalmazás, vagy rendszer elérésére feljogosított felhasználókat megakadályozza a számukra fontos információk, a számítógép-rendszer vagy akár a számítógép-hálózat elérésében.

[2] Az ISACA, mely az információrendszer ellenőrök, az információbiztonsági, informatikai irányítási és informatikai kockázatkezelési szakemberek nemzetközi szervezete az informatikai irányítás, kockázatkezelés, információbiztonság irányítás és informatikai ellenőrzés jó gyakorlatait magába foglaló keretrendszer. A módszertan elsősorban a szakmai vezetőknek ad segítséget ahhoz, hogy felmérhessék és elfogadható szintre csökkenthessék azokat a kockázatokat, amelyeket az informatika üzleti folyamatokba épülése jelent. Iránymutatásokat tartalmaz egy kontroll rendszer kialakításához és annak a folyamatos működtetéséhez.

- Sértetlenség – a vállalati értékek és elvárások szerinti pontosság, teljesség, és érvényesség.
- Rendelkezésre állás – az információ és szolgáltatásának képessége akkor áll rendelkezésre, amikor az üzleti folyamatnak szüksége van rá most, és a jövőben.
- Megfelelőség – törvényeket, jogszabályokat, szabályozásokat és szerződéses megállapodásokat (előírt üzleti követelményeket) betartva áll elő az információ.
- Megbízhatóság – a vállalkozás működtetése és a pénzügyi megbízhatósági, és irányítási kötelezettségek teljesítése érdekében szükséges információt kapja a szervezet vezetése.

Sajnálatos, hogy a biztonságos működés igénye gyakorta csak a biztonság látszatának a megteremtését jelenti, nem a valós biztonságot. A szakemberek törekszenek rá, hogy objektív módon határozzák meg a biztonság mértékét és állapotát. A laikusok számára a biztonság bizalmi kérdés. Gyakran megesik, hogy nem biztonságos rendszerben bíznak az emberek, a biztonságosban pedig nem. A biztonság egy szervezet vezetője számára is gyakran nehezen „eladható" terület, hiszen megléte nem pontosan érzékelhető, már csak a biztonság hiánya az, amelyet tapasztalhatunk.

Miért nehéz valóban biztonságos működést kialakítani? Ahhoz, hogy egy szervezet, vagy egy információs rendszer biztonságát meg tudjuk teremteni, pontosan ismernünk kell a rendszer célját és releváns kockázatok mértékét, és azzal arányos védelmi rendszert kell kialakítani.

Információbiztonság: fizikai, logikai és humán biztonság

Nemzetközi szabványok (ISO 27000 szabványcsoport) határozzák meg az integrált információbiztonsági rendszerekkel kapcsolatos követelményeket, amelynek jelentős eleme az IT biztonság, de az informatikai rendszerektől függetlenül például papíron tárolt információk védelmét lefedi.

Az MSZ ISO/IEC 27001 célja, hogy modellként szolgáljon információbiztonsági irányítási rendszerek (ISMS) kialakításához, megvalósításához, működtetéséhez, figyelemmel kíséréséhez, átvizsgálásához, fenntartásához és fejlesztéséhez. Továbbá tartalmazza a szervezet információbiztonsági irányítási rendszerének külső szakértő általi ellenőrzésének követelményeit, és lehetővé teszi a tanúsíthatóságot.

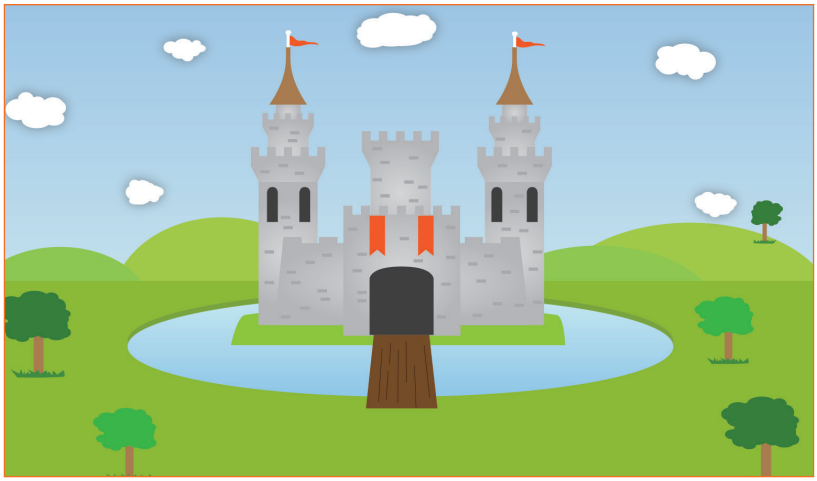
Az MSZ ISO/IEC 27002 az információbiztonság menedzsmentjének gyakorlati kódexe. A korábbi informatikai biztonsági ajánlásoktól eltérően, a biztonsági követelményeket és intézkedéseket a szervezet üzleti céljaiból és stratégiájából vezeti le szervezeti szintű, informatikai biztonságmenedzsment központú szemléletben. Az ISO 27002, a minőségbiztosításra vonatkozó ISO 9000-es szabványokhoz hasonlóan, a teljes körű informatikai biztonság megteremtéséhez szükséges szervezési, szabályozási szempontrendszert adja meg.

A szabvány a védelmi intézkedéseket az alábbi logikai csoportokba szervezi:

- kockázatelemzés;
- biztonságpolitika, szabályzati rendszer;
- biztonsági szervezet;
- vagyontárgyak kezelése;
- személyi biztonság;
- fizikai és környezeti biztonság;
- kommunikáció és üzemeltetés biztonsága;
- hozzáférés-ellenőrzés;
- információs rendszerek beszerzése, fejlesztése és karbantartása;
- incidenskezelés;
- üzletmenet-folytonosság;
- megfelelőség.

Védelmi rendszerek – több szintű védelem

Hagyományosan a biztonságot a határok erős védelmével valósították meg. Gondolhatunk itt egy várárokkal körülvett magas sziklafallal körbevett erődítményre, melybe egy felhúzható palló segítségével egyetlen kapun keresztül lehet bejutni, amelyet marcona őrség véd.



Napjainkban is fontos része a védelemnek a fizikai védelem, amelynek főbb részei a következők:

- mechanikai védelem;
- elektronikai jelzőrendszer;
- élőerős védelem;
- beléptető rendszer;
- biztonsági kamera rendszer;
- villám és túlfeszültség védelem;
- tűzvédelem.

Az informatikai biztonság alapvetően függ az információs rendszerek elemeiből integrált komplex rendszerek biztonsági megfelelőségétől, és az információs rendszereket működtető szervezet folyamatainak érettségétől, a szakemberek, és az irányítást végzők szakképzettségétől, és a belső kontroll rendszer minőségétől. Az információbiztonságot a tágabb és szűkebb környezetre szabva kell kialakítani, megvalósítani, működtetni és fejleszteni.

Adatvédelem: személyes és különleges adatok jogszabályi védelme

Magyarországon az állami és önkormányzati szervek adatok, és ezeket tartalmazó dokumentumok sokaságát kezelik. Ezek részben nem nyilvános, vagy fokozottan védett minősített adatok, részben pedig bárki által korlátlanul megismerhető közérdekű adatok, információk. Ezek lehetnek természetes személyre vonatkozó, az adott szervezet vagy más szervezet működésére vonatkozó. Az adatok kezelését, gyűjtését, továbbítását jogszabályok határozzák meg. A hazai adatvédelmi szabályozás egyike a legszigorúbbaknak nemzetközi szinten, alapjait az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény fekteti le.

Fokozottan fontos ez a jogi védelem az állam irányító, szabályozó, ellenőrző szerepének megnövekedése, valamint az informatika szolgáltatások széles körű bevezetése miatt, amely kiterjedt, de célhoz kötött adatgyűjtéssel és kezeléssel jár együtt. A személyes adatok védelmét nem csak az állami adatkezelés szempontjából kell biztosítani, hiszen a vállalatok, vállalkozások számára is komoly piaci értéke van például egy elektronikus levélcímnek, vagy pontos felhasználói és vásárlási szokásainknak.

A személyes adatoknak egy szűkebb köre az olyan érzékeny adatok, amelynek sérülése a magánszférát komolyan érinti, különleges adatnak minősül és szigorúbb védelem alatt áll. Ilyen például a nemzeti kisebbséghez tartozásra, a politikai pártállásra, szexuális életre -vonatkozó adat, a bűnügyi személyes adat és az egészségügyi állapotra vonatkozó adat.

Adatkezelésnek tekintendő az adatokon végzett bármely művelet, beleértve az adatok gyűjtése, rögzítése, rendszerezése, tárolása, módosítása, felhasználása, továbbítása, nyilvánosságra hozatala, szinkronizálása, összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása. A személyes adatok kezelése törvényi felhatalmazás, vagy az érintett – különleges adatok esetén írásos – hozzájárulása esetén lehetséges kizárólag egyértelműen meghatározott cél érdekében felhasználni.

Az adatvédelmi jogszabályok betartását hatóság, a Nemzeti Adatvédelmi és Információszabadság Hatóság felügyeli és a jogszabályok be nem tartása esetén komoly bírságot szabhat ki, illetve fel is függesztetheti az adatkezelést.

A minősített adatok védelmének intézményrendszerét, a nemzeti és külföldi minősített adatok védelmének egységes felügyeletét, és a minősített adatok kezelésének hatósági engedélyezését a Nemzeti Biztonsági Felügyelet (NBF) látja el a Közigazgatási és Igazságügyi Minisztérium szervezeti keretében. Az NBF egyik szervezeti egysége feladata a közszféra információs rendszereinek kiberbiztonsági vizsgálata is.

Információbiztonság: állami és önkormányzati elektronikus információ, és infrastruktúrák jogszabályi védelme

A létfontosságú infrastruktúra védelmére vonatkozó jogszabályok 2008-2013 között léptek hatályba. Ezek olyan létfontosságú fizikai és információs-technológiai berendezések és -hálózatok, szolgáltatások és eszközök védelmét érintik, amelyek összeomlása vagy megsemmisítése súlyos következményekkel járhat a polgárok egészsége, védelme, biztonsága és gazdasági jóléte, illetve a kormányok hatékony működése szempontjából.

Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. Korm. határozata meghatározza Magyarország kibertérre vonatkozó értékrendjét, jövőképét és céljait, és előre vetette a dinamikusan változó kibertér igényeihez és az ez által generált feladatokhoz alkalmazkodni képes kormányzati képességeket biztosító kormányzati struktúra kiépítését.

A stratégia gyakorlati megvalósulását hivatott biztosítani még a 2013 áprilisában elfogadott, az állami és önkormányzati rendszerek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv). A törvény felállítja a szükséges intézményrendszert a nemzeti vagyon részét képező nemzeti elektronikus adatvagyon, illetve a létfontosságú információs rendszerek és rendszerelemek biztonsága alapfeltételei megteremtéséhez.

Az intézményrendszer része a Nemzeti Biztonsági Felügyelet új szakhatósági feladata, amely keretében a biztonsági incidensek megelőzését, a sérülékenységek és hibás működési beállítások felkutatását végzi, továbbá javaslatot tesz azok elhárítására, valamint közreműködik a biztonsági incidensek műszaki vizsgálatában.

Az Ibtv. és végrehajtási rendeletei létrehozták a Nemzeti Elektronikus Információbiztonsági Hatóságot (továbbiakban: NEIH) és szakhatósági feladatokkal ellátásával ruházzák fel az elektronikus információbiztonság területén. A Hatóság fő feladata, hogy felügyelje a költségvetési szervek információtechnológiai, adatkezelő- és feldolgozó tevékenységét és az információtechnológiai fejlesztési projektekben az információbiztonsági követelmények teljesülését. Továbbá engedélyezi az érintett szervezetek által az Európai Unió tagállamaiban történő elektronikus információs rendszer üzemeltetését, és ellenőrzi az érintett szervezetek által az Európai Unió tagállamain kívül történő elektronikus információs rendszerüzemeltetést.

Információs rendszerek elemei

Az informatikai irányítás nemzetközi de facto sztenderdje – a Cobit – az információs rendszerek elemeit négy csoportba sorolja: információ, infrastruktúra, alkalmazói rendszer, és emberi erőforrás. Az infrastruktúra és az alkalmazói rendszerek ismertetése közérthetően:

- hardver:
  - szerver (több felhasználó munkáját segítő központi számítógép);
  - munkaállomás/PC (egy felhasználó munkáját segítő asztali számítógép);
  - hordozható számítógép/laptop/notebook (a PC hordozható változata, saját akkumulátorról órákig üzemel);
  - mobiltelefon (kezdetben telefonálásra, ma már fényképezésre és számítógépezésre is alkalmas készülék, kézi számítógép);
  - táblagép (a hordozható számítógépeket egyszerűbb, billentyűzet nélküli érintőképernyős változata, kézi számítógép);
  - adathordozó, adattároló egység (számítógépen feldolgozható állományok, dokumentumok, fényképek, adatbázisok tárolására, és visszaolvasására alkalmas eszköz);
  - adatbeviteli (input) eszközök: billentyűzet, digitalizáló tábla, stb.;
  - adatkimeneti (output) eszközök: nyomtató, képernyő, stb.;
- szoftver:
  - operációs rendszer (a számítógépek hardver eszközeit működtető programok);
  - virtualizáció (egy fizikai számítógépen több logikai számítógép egyidejű működtetését lehetővé tevő szoftverrendszer);
  - adatbázis kezelő (az alkalmazások által használt adatok tárolását, strukturált előhívását, és azokkal különböző műveleteket végző szoftver);
- hálózat:
  - aktív hálózati eszközök (hálózati adatforgalmat vezérlő és ellenőrző miniszámítógépek, melyek működése az üzemeltetők által módosítható);
  - passzív hálózati eszközök (hálózati eszközök, amelyek az előre beléjük rögzített feladatokat végzik);
  - hálózat biztonsági eszközök (pl. tűzfalak, hálózati betörés detektálók, tartalomszűrők, általában olyan egyedi célra felkészített számítógépek, amelyek egy elvárt biztonsági funkciót valósítanak meg);
- dokumentáció:
  - az informatikai rendszerre vonatkozó leírások, útmutatók, kézikönyvek, tervek;
- alkalmazói rendszerek:
  - az alkalmazói rendszerek egy adott ügyvitelt, vagy egyéb tevékenységet támogató funkciók, vagy funkciócsoportok végrehajtására fejlesztett számítógépes eljárások, olyan szoftverek, amelyek az operációs rendszer segítségével működnek, gyakran adatbázis-kezelőt is használnak.

Információ:

- olyan tény, amelynek megismerésekor olyan tudásra teszünk szert, amelynek addig nem voltunk birtokában. Az információ tehát értelmezett adat.

Fontosabb informatikai fogalmak:

- URL: egy weboldal címének megnevezése, amely alapján a címtár a technikai címet (IP cím) megtalálja, egy címen egyébként több honlap is működhet. Az a haszna, hogy könnyen megjegyezhetjük egy honlap elérhetőségét. Van olyan támadási módszer, ahol a címtár támadásán keresztül egy valós, és jogszerű URL-t egy kártevő IP címre irányít. Ha https-sel kezdődik, akkor titkosított kapcsolatot használ. Figyeljünk rá, hogy pontosan írjuk le a címet, mert kártevő honlapokra is kilyukadhatunk.
- QR-kód[3]: léteznek olyan URL rövidítő szolgáltatások, amelyekkel könnyen felírható lesz egy hosszabb cím is. Ezeket újabban a segítik a QR kódok is, amelyek kétdimenziós vonalkódok, és amelyeket többek között okostelefonokkal való használat során vehetünk igénybe.

[3] Nevét az angol Quick Response rövidítéséből kapta (gyors válasz), amely a gyors visszafejtési sebességre, és ebből adódóan a gyors válaszadó képességre utal. A QR kód a hagyományos vonalkódhoz képest több százszor annyi adatot képes kezelni.

Információbiztonság irányítása és menedzselése ugyanazt jelenti?

A megnövekedett és egyre komplexebbé váló információs rendszerek elleni támadásokra való reagálás már régóta nem csupán műszaki kérdés, hanem egy olyan probléma, amivel a felső vezetésnek komolyan szembe kell néznie! A vezetőnek kell meghatározni azokat a célokat, a célok megvalósításának irányelveit, és a feladatok végrehajtását végző szervezetet, amelyek eredményesen biztosíthatják az elvárt biztonsági szintet.

Önmagában nem vezet eredményre, ha az információbiztonságot különböző biztonsági intézkedések életbe léptetésével vagy valamely szabvány adaptálásával kívánjuk megteremteni. A szervezet célkitűzéseinek elérését szolgáló, gazdaságos információbiztonság sokkal inkább a bevált szervezetirányítási gyakorlatok alkalmazásával érhető el. Az információbiztonsági funkció tehát minden szervezet belső irányítási és kontroll rendszerének része kell, hogy legyen.

Az üzleti világ módszertanai (pl. COBIT, BMIS[4]) ehhez hozzáteszik még azt is, hogy az információbiztonság irányítását és menedzselését a szervezetek céljainak elérése érdekében, a kockázatokkal arányban levő módon, a rendkívüli biztonsági eseményeket megelőzve, feltárva, helyesbítve kell végezni.

Az ISACA háromévente felméri világszerte, hogy milyen tevékenységeket végeznek az információbiztonsági szakemberek, és ehhez milyen szaktudásra van szükség. A felmérés eredményeit közzéteszi, és ennek alapján frissíti az Információbiztonsági Vezető Tanúsítvány (CISM) vizsgakövetelményeit is.

A következő négy fő területet tartalmazza jelenleg a vizsga:

1. Információbiztonság irányítása – a szervezet céljaival, kötelező és vállalt feladataival, a szervezetet veszélyeztető tényezőkkel és a biztonságra fordítható erőforrásokkal összhangban levő irányítási rendszert kell az információbiztonsági területen is kialakítani.
2. Információs kockázatkezelés és megfelelés – a jogszabályokban előírt és a szervezet vezetője által elfogadott szinten kell tartani az információs rendszereket veszélyeztető kockázatokat.
3. Információbiztonsági program kidolgozása és megvalósítása – az információbiztonsági stratégiával összhangban kell kialakítani és megvalósítani az információbiztonsági programot.
4. Információbiztonsági rendkívüli eseménykezelés – a szervezetet érő károk csökkentése érdekében tervezett módon kell az információbiztonsági eseményeket és következményeik helyreállítását kezelni.

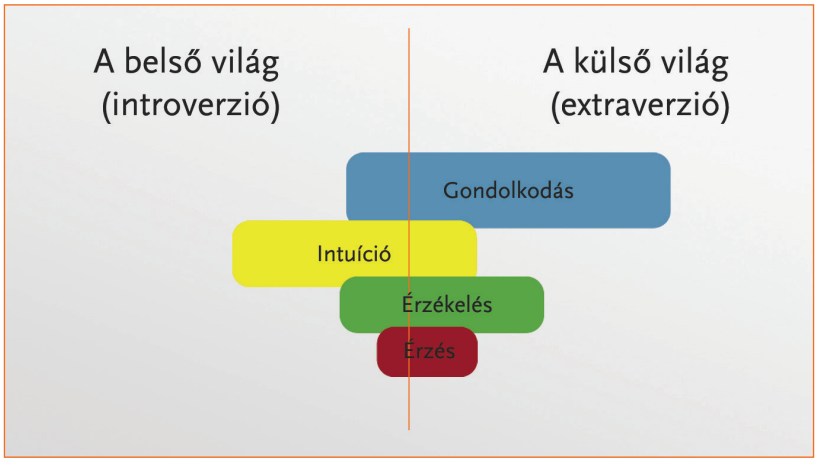
Az információbiztonság irányítási feladatokkal kapcsolatos ISACA ajánlások a Biztonságtudatos vezetés fejezetbe kerültek beépítésre.

[4] BMIS – Business model for information security, az ISACA holisztikus információbiztonság menedzsment módszertana, mely beépült a COBIT 5 keretrendszerbe.

Mindenki ugyanúgy látja a biztonság fontosságát?

A biztonság szubjektív fogalom, hiszen az emberek nem csak korukra, nemükre, szakmai hátterükre nézve különböznek egymástól, hanem alapvető személyiségjegyeik is eltérőek. Egy munkahelyi kultúra az egyik ember számára ideális, és a munkára serkentő lehet, de elképzelhető, hogy a másik ember számára ugyanez a munkakörnyezet nehéz, vagy akár elviselhetetlen.

A személyiség tulajdonságai a környezeti hatásokra adott, az agyunkból kiinduló tudatos, és tudatalatti válaszokat határozzák meg. A tulajdonságokból áll össze a személyiségtípus. Karl Jung személyiségtípus elmélete jól szemlélteti az egyének különbözőségét. Négy ellentétpárt határozott meg, amelyeket egy-egy betűvel jelöli, így alkotva négybetűs rövidítéseket. Ezek variációi összesen 16 típust adnak. Ezek közül leginkább az ENTJ képes a biztonsági kultúra követésére, azonban képzéssel fejleszthető más személyiség esetében is ez a képesség.



Az ENTJ személyiségek kifejezetten igénylik, hogy egy szabályozott, minden választási lehetőségre választ adó szabályrendszer kötöttségei között, rendszeresen ismétlődő, kiszámítható tevékenységeket végezzen (pl. termelés, adatfeldolgozás), ahol a csoportvezetője rendszeresen ellenőrzi a munkáját és visszajelzést ad. Ez a helyzet bénító, frusztráló és elviselhetetlen lesz ISPF személyiségek számára, akik inkább olyan problémák megoldásával szeretnek foglalkozni (pl. marketing, termékfejlesztés), amelyekkel nem találkoztak korábban. Számukra az ideális munkakörnyezet a tágan meghatározott szabályok között, rugalmas munkaidőben történő foglalkoztatás jelenti, hogy akkor dolgozhassanak, amikor ihletük van, mert akkor lesznek eredményesebbek. Nyilvánvaló, hogy mindkét kollega munkájára szüksége lehet a szervezetnek.

A megfelelő biztonsági kontroll rendszer kialakításához és fenntartásához fontos a munkavállalók különböző személyiségének felismerése, és az ehhez illeszkedő intézkedések meghatározása. Sérül ugyanis a szervezet biztonsága, ha az egyének nem előírásszerűen végzik feladatukat, egy adott biztonsági eseményre nem megfelelően reagálnak.

Vasvári György[5] szerint az alábbi kérdések segítik eldönteni, hogy hol tart a biztonsági kultúra kialakítása, és ezeken a területeken mit szükséges fejleszteni:

1. Tudják-e, indokoltnak tartják-e jogaikat, kötelezettségeiket?
2. Tevékenységük során azok szerint járnak-e el?
3. Felismerik-e a védelmi intézkedések szükségességét, van-e veszélyérzetük?
4. Felismerik-e, és elítélik-e azokat, akik a biztonsági szabályokat megsértik, a védelmi intézkedéseket nem rendeltetésszerűen hajtják végre?
5. Vállalják, hogy hatást gyakorolnak a biztonsági követelményeket tudatosan vagy véletlenül, emberi gyengeségük miatt, részben illetve egészében megsértő kollégákra?
6. Felismerik-e, akarják-e felismerni a nem erkölcsös, etikus magatartást tanúsítókat?
7. Biztonsági tudatosságuk révén konstruktív részesévé válnak-e a szervezeti egység, csoport szubkultúrájának?

Milyen a biztonságtudatos szervezet?

A szervezet biztonságáért vállalt felelősség, a szervezet vezetése által meghatározott biztonsági szintnek, mint követelménynek elfogadása és a hiánya következményeinek elismerése, valamint a biztonsági szempontból erkölcsös, etikus magatartási kultúra együttesen jellemzi a biztonság tudatos szervezetet.

Egy szervezetnél akkor jó a biztonsági kultúra, ha a munkatársak ismerik jogaikat és kötelezettségeiket, és érvényesítik is azokat. Azoknak a munkatársaknak, akik tudatlanságból, hanyagságból, vagy szándékosan nem biztonságtudatosan viselkednek, ismételt biztonságtudatossági oktatáson kell részt venniük, illetve el is marasztalhatják őket. A biztonsági kultúrát tehát az egyének biztonságtudatos magatartása alakítja ki, ahol kialakult, ott a munkatársak tudják, mi veszélyeztet(het)i a biztonságot, és ennek megfelelően cselekszenek is.

Az egészséges veszélyérzetnél annyiban különbözik a biztonságtudatosság, hogy nem csak felismerjük, hogy a biztonsági elvárásoktól eltérő viselkedés veszélybe sorolhat minket, vagy a szervezetet, hanem azt is, hogy ilyen helyzetben mit tegyünk, és mit ne tegyünk.

A biztonságtudatosságra külső (pl. jogszabályok, szabványok, politikai hatások, piaci hatások, természeti hatások, egyének környezetének) és belső tényezők (pl.: szabályzatok, a közvetlen vezetés utasításai, humánpolitika, az ellenőrzés) egyaránt hatással vannak.

Azért fontos a vállalati kultúra részévé tenni a biztonságot, mert a szervezeti kultúra befolyásolja az egyének hovatartozás tudatát, helyzetét, szerepét a szervezetben. Tehát a biztonsági kultúra, és a

[5] Vasvári György: Vállalati biztonságirányítás – Informatikai biztonságmenedzsment, Info-Szakkönyv Bt., 2007.

szintjének fenntartása, vagy emelése önmagában is védelmi intézkedés. Célszerű a biztonsági kultúra szintjét évente értékelni.

A biztonságtudatosság megjelenhet vállalati szokásokban (pl. minden értekezlet után a fali táblát letöröljük), a belső kommunikációban használt nyelvezetben, és szimbólumok alkalmazásában.

A biztonságtudatosság hiányában a szervezet nem ismeri fel megfelelően a rendkívüli biztonsági eseményeket, és nem képes felmérni azok következményeit. Ez azt eredményezheti, hogy a szervezet nem lesz képes a kötelező és vállalt feladatai ellátására.

Megelőzés módszerei: ismeretszerzés, tudatosítás

Alapvető és más lehetőségekhez képest olcsóbb módszer az, ha felkészítjük a felhasználókat, szervezetünk munkatársait arra, hogy felelősen, a biztonságot veszélyeztető tényezők ismeretében végezzék munkájukat. Továbbá legyenek felkészítve azoknak az eszközöknek és információs rendszereknek a használatára, amelyek szükségesek a munkájukhoz, így is csökkentve az emberi hibákból fakadó biztonsági eseményeket. Ennek eredményességét tudja fokozni, ha ezeket az ismereteket jól érthető formában, szakemberek által összeállított megbízható információkra építve, és a felnőttképzés és szervezetfejlesztés korszerű eszközeit felhasználva adjuk át munkatársainknak.

Jelen tájékoztató anyag is része annak a folyamatnak, amelynek eredményeképpen a közszférában dolgozó munkatársak alapvető ismereteket szerezhetnek, megismerve ez által az informatika használatának veszélyeit, így felkészülhetnek a kockázatok elkerülésére, vagy a bekövetkezett kockázatok felismerésére, és a károk csökkentésére.

Az informatikai biztonsági tudatosítás eredményes megvalósítása komplex, személyre szabott szervezeti kultúrafejlesztési program, melynek része az adott szervezetet érintő kockázatok felmérése, a kockázatkezelési stratégia meghatározása, az informatikai biztonsági szabályozás kiadása, és a felhasználóktól elvárt viselkedési szabályok meghatározása. A szükséges információk birtokában végezhető el a biztonságtudatosítási program személyre szabása, majd a dolgozók felelősségi és felkészültségi szintjének legmegfelelőbb képzési, tudásátadási formák meghatározása, a tudás átadása, visszaellenőrzése.

Megelőzés módszerei: adatmentés

A legkézenfekvőbb megoldás, amely biztosítja az elektronikus információk megsemmisülés elleni védelmét az, ha többszörözzük őket. Le kell másolni rendszeresen, és az eredeti helyétől eltérő biztonságos helyen kell tárolni az információs rendszerekben és adathordozókon (külső merevlemez, DVD stb.) tárolt adatokat.

A másolatok megléte véd a rendszerek és adathordozók meghibásodása, a véletlen adattörlés vagy módosítás, és a szándékos károkozás ellen is. A másolásra alkalmazott műszaki megoldásoktól, az adatok visszaállítására használt eljárásoktól függ, hogy milyen gyorsan lehet visszaállítani az adatokat. A mentések gyakorisága pedig azt határozza meg, hogy két mentés között elvileg mennyi adat veszhet el.

Fontos felhívni a figyelmet, hogy adott szervezeten belül az informatikai részleg végzi az adatok mentését, ezért általában szükségtelen, sőt biztonsági szempontból kifejezetten veszélyes, gyakran tiltott is a munkavégzés során készített dokumentumok, iratok, levelezés saját adathordozón való tárolása, szervezeten kívülre hordozása. Miért van ez? Általában egy olcsó kisméretű adathordozót (pl. memóriakártyát, USB-memóriát) használnak erre a munkatársak, amelyen titkosítás nélkül tárolják az adatokat. Belátható, hogy ez könnyen nyomtalanul eltűnhet. Veszett már el például hordozható adathordozón több millió adózó adata, és kórházban kezelt betegek adatai, és nem nyilvános előterjesztések munkaanyaga. Gondoljuk végig, hogy a magunkkal hordott adatok milyen kárt okozhatnak illetéktelen kezekben!

A szervezetünk adatait tehát csak akkor tegyük saját adathordozónkra, ha meggyőződtünk arról, hogy a szabályok megengedik, és feltétlen szükséges. Ebben az esetben mindig titkosítsuk az adatokat (például az ingyenes Truecrypt programmal).

Megelőzés módszerei: felhasználók számítógépeinek védelme

A közszférában dolgozó munkatársak a személyes tulajdonukban levő számítógépek tekintetében felelősek azok védelméért. Ez fokozottan fontos abban az esetben, ha ezeket a számítógépeket a hivatali kommunikációra, illetve munkavégzésre is igénybe veszik. Minden felhasználótól elvárható, hogy az alapvető védelmi intézkedések beállítását és működtetését képes legyen elvégezni. Ide soroljuk a rendszerszoftverek frissítését (Windows esetén például automatikusan elvégzi a rendszer, ha bekapcsoljuk), vírus és kártevő védelmi szoftverek működtetését (ingyenesen letölthetőek széles körű dokumentáció és telepítési utasítás áll rendelkezésre), és szoftveres tűzfal működtetését (Windows rendszer része, de ingyenes egyéb tűzfalak is elérhetőek).

Abban az esetben, ha fokozni szeretnénk a számítógépeink védelmét használhatunk külön virtuális gépet például a hivatali munkára, illetve telepíthetünk úgynevezett homokozót (sandbox), amely megakadályozza, hogy programok, különösen böngészők, a rendszer beállításait megváltoztathassák. Ezek megfelelő beállítása már középszintű felhasználói ismereteket feltételez.

A közszféra szervezetei által használt számítógépeiknek védelmét a szervezet informatikai részlege, vagy egy külső szolgáltató működteti. Ebben az esetben a felhasználók felelőssége annyi, hogy ezeket a védelmi rendszereket ne kapcsolják ki, illetve jelezzék, ha nem, vagy hibásan működnek. Speciális eset, ha személyes tulajdonú számítógépet a hivatal belső hálózatán kíván egy munkatárs használni. Ilyenkor általában szükséges, hogy a hivatal által meghatározott informatikai beállításokat alkalmazzák a gépen a megfelelő biztonság érdekében. Ha ehhez a munkatárs nem járul hozzá, akkor általában maximum internet kapcsolatot fog kapni a belső hálózaton, semmi máshoz nem férhet hozzá.

Fontos eszköz a számítógépek fizikai védelme is. Általában a szervezetek belső szabályzatban tiltják, hogy felügyelet, vagy megfelelő védelem nélkül hagyjuk a hordozható számítógépeket. Például egy gépjármű utasterében ne hagyjunk számítógépet. A csomagtartó sem biztosít megfelelő védelmet, mert a tolvajoknak megvannak az eszközeik, amellyekkel kifigyelik, hogy van-e számítógép a gépkocsiban. A számítógépes eszközök használatát a szervezetek általában a Felhasználói szabályzatban, illetve az Informatikai biztonsági szabályzatban szabályozzák.

Biztonsági események bejelentése, kivizsgálása, elhárítása

Mit is értünk rendkívüli IT biztonsági esemény (IT biztonsági incidens) alatt? Az informatikai rendszer védelmi állapotában beállt illetéktelen változás, amelynek hatására az informatikai rendszerben kezelt információ bizalmassága, sértetlensége, hitelessége, funkcionalitása, rendelkezésre állása megsérül, vagy a sérülésük kockázata megnő. Ilyen esemény lehet például adathalászok támadása, vagy akár az áramellátás megszűnése.

Szervezeti szinten belső szabályzatban kell definiálni (pl. IT Biztonsági Szabályzat, Katasztrófa Terv) az informatikai üzemeltetési és informatikai biztonsági feladatokat és azok felelősét, valamint a vonatkozó folyamatokat, eljárásokat. Jó gyakorlat, hogy egy központi helyen kezelik az igényeket, és a rendkívüli eseményeket, mert így központilag nyilvántartott, és nyomon követhető a kezelésük. Az informatikai rendszerek felhasználóinak a feladata általában ezzel kapcsolatban az, hogy időben bejelentsék a szokatlan működést, illetve működés megszakadását.

A rendkívüli IT biztonsági esemény kivizsgálása általában helyben kezdődik. Megnézik, hogy volt-e már hasonló eset, van-e elkerülő megoldás, illetve megoldás az IT biztonsági eseményre. Ahol informatikai szolgáltatók vesznek igénybe részben, vagy teljes mértékben ott a kiszervezett szolgáltatásokra ezt vagy a szolgáltató végzi, vagy együttműködnek vele.

Amennyiben csalás, vagy külső támadás gyanúja merül fel, akkor a biztonsági terület is bekapcsolódik az esemény vizsgálatába. Szükség esetén a hatóságok segítségét is lehet kérni, ha olyan jellegű a biztonsági rendkívüli esemény.

Az ismert sérülékenységek azonosításában kormányzati szinten a kormányzati és ágazati CERT[6]-ekhez kell fordulni.

Mi a felhasználók felelőssége?

A szervezetben a munkatársak és szerződéses dolgozók számára kötelező a jogszabályok és a szervezet belső szabályzatainak és a vezetői utasításoknak a betartása.

Általában az információs rendszerek felhasználóitól elvárt viselkedési normákat felhasználói szabályzatban, vagy más szabályzatok részeként határozzák meg. Alapvetően azt tartalmazza, hogy a

[6] CERT – hálózatbiztonsági központok, amelyek fő feladata a hálózatbiztonsági incidensek kezelése, az állami szféra vagy egyes ágazatok informatikai rendszereinek hálózatbiztonsági támogatása. A CERT-ek megfelelő technikai háttérrel rendelkeznek ahhoz, hogy időben reagáljanak és kezeljenek minden hálózatbiztonságra és létfontosságú információs infrastruktúrára veszélyes eseményt. A bejelentett eseményeket a központok bizalmasan vezetik.

rendszereket kizárólag munkavégzés céljára, a munkavégzéshez szükséges mértékben lehet használni. Gyakran kitér a szabályozás arra is, hogy a rendszerek és a szervezet biztonsága érdekében az informatikai rendszer működését, és a felhasználók tevékenységét a szervezet figyelemmel kíséri.

A Közigazgatási és Igazságügyi Minisztérium által kiadott etikai kódex tervezet (ZÖLD KÖNYV az állami szerveknél érvényesítendő etikai követelményekről) és a Magyar Kormánytisztviselői Kar által a közszolgálati tisztviselőkről szóló 2011. évi CXCIX. törvény felhatalmazása alapján kiadott Hivatásetikai Kódex[7] további útmutatást nyújt a különböző szabályzatokban egyértelműen nem meghatározott elvárások tekintetében.

[7] http://mkk.org.hu/node/102

Biztonsági kultúra megvalósításának alapelvei

Az OECD[8] az információs rendszerek és hálózatok biztonságára vonatkozó útmutatóban[9] kilenc alapelvet határozott meg a biztonsági kultúra sikeres megvalósítása érdekében. Ezek az elvek a felhasználókra, a vezetőkre, és a szakpolitika szintjére egyaránt eredményesen alkalmazhatóak. Természetesen minden szinten az egyéni szerepeknek megfelelően változik a felelősség. Az alapelvek követése segít az információk megszerzésében, tudatosításában, a szükséges képességek elsajátításában. Az alapelvek egymást erősítik, ezért mindegyiket indokolt figyelembe venni a biztonsági kultúra alakítása során! Az OECD felhívja még a figyelmet arra, hogy egyensúlyt kell teremteni a demokratikus társadalom értékei és a biztonság között.

1) Tudatosítás elve

Meg kell értenünk és tudatosítanunk, hogy az információs rendszerek és hálózatok hasznát csak úgy élvezhetjük, veszélyeiket csak úgy kerülhetjük el, ha a biztonsági kockázatok tudatában használjuk őket.

Az első védelmi vonal tehát az informatikai kockázatok és a rendelkezésre álló védelmi lehetőségek tudatosítása. A kockázatok belső és külső irányból is felmerülhetnek. Ez azt jelenti, hogy egy felhasználói, vagy üzemeltetési hiba veszélyeztetheti a saját, illetve a vele kapcsolatban levő rendszerek és hálózatok biztonságát. Az integrált rendszerek megfelelő biztonsága érdekében az érintetteknek ismerniük kell a rendszerük felépítését, a hálózatokban elfoglalt helyét, és a biztonság érdekében alkalmazható intézkedéseket.

2) Felelősség elve

A felhasználók, az üzemeltetők, a fejlesztők és a tulajdonosok is felelősek az információs rendszerek és hálózatok biztonságáért. A rendszerek biztonsága függ a velük összeköttetésben levő helyi és globális rendszerek biztonságától. Ahhoz, hogy a biztonságot fenn tudjuk tartani, minden érintettnek tudatában kell lennie saját felelősségével, és ezt számon kell tudni rajta kérni.

Minden szervezetnek rendszeresen felül kell vizsgálnia saját szabályzatait, gyakorlatait, intézkedéseit és eljárásait, és értékelnie kell, hogy ezek megfelelőek-e. Minden érintettnek, aki részt vesz informatikai termékek és szolgáltatások fejlesztésében, tervezésében és szállításában, foglalkoznia kell a rendszerek és hálózatok biztonságával és a szükséges tájékoztatást időben meg kell tennie. Ennek eredményeként a felhasználók jobban megértik a termékek és szolgáltatások biztonsági vonatkozásait és a saját felelősségüket a biztonsággal kapcsolatban.

---

[8] OECD: Organisation for Economic Co-operation and Development - Gazdasági Együttműködési és Fejlesztési Szervezet

[9] Guidelines for the Security of Information Systems and Networks, OECD, 2002.

3) Válaszintézkedések elve

Az érintetteknek kellő időben, egymással együttműködve kell a váratlan biztonsági eseményeket megelőzni, észlelni, illetve az ezekre vonatkozó megfelelő válaszintézkedések megtenni.

Felismerve az információs rendszerek és hálózatok összekapcsolódását, és a gyors és széleskörű károkozás lehetőségét, az érintetteknek időben és együttműködve kell a váratlan biztonsági eseményeket kezelni. Szükség szerint meg kell osztaniuk egymással a fenyegetésekkel és sebezhetőségekkel kapcsolatos információkat, és gyors és hatékony eljárásokat kell alkalmazniuk, hogy együttműködve megelőzzék, észleljék, illetve reagáljanak a váratlan biztonsági eseményekre. Ahol lehetséges, ez akár határokon keresztüli információcserével és együttműködéssel is járhat.

4) Etika elve

Az érintetteknek tiszteletben kell tartaniuk mások jogos érdekeit.

Tekintettel arra, hogy az információs rendszerek és hálózatok alkalmazása átszövi a társadalmunkat, az egyéneknek fel kell ismerniük, hogy cselekedeteik vagy azok hiánya adott esetben káros hatással is lehetnek a többi felhasználóra. Az etikus viselkedés ezért létfontosságú, az érintetteknek törekedniük kell arra, hogy a jó gyakorlatokat kialakítsák és alkalmazzák, a biztonság igényét elfogadják, és mások jogos érdekeit tiszteljék.

5) Demokrácia elve

Az információs rendszerek és hálózatok biztonságát megvalósító megoldásoknak a demokratikus társadalmak alapvető értékeivel összeférhetőnek kell lenniük.

A gondolatok és eszmék cseréjének szabadságát, az információ szabad áramlását, a személyes adatok megfelelő védelmét, a nyitottságot és az átláthatóságot indokolatlan mértékben nem szabad korlátozni.

6) Kockázatfelmérés elve

A biztonság tervezése és megvalósítása során a releváns lényeges kockázatokat fel kell mérni.

A kockázatfelmérés azonosítja a fenyegetéseket és a sebezhetőségeket, kitérve a legfőbb belső és külső tényezőkre, úgymint a technológia, a fizikai és emberi tényezők, politikai irányelvek és harmadik személy által nyújtott biztonsági szolgáltatások. A kockázatfelmérés lehetővé teszi az elfogadható szervezeti kockázati szint meghatározását, és segítséget nyújt az információs rendszerek és hálózatok biztonságát fenntartó megfelelő szabályozások kialakításában a megvédendő információ jellegével és

fontosságával arányban. Tekintettel az információs rendszerek összekapcsolására, a kockázatfelmérésnek ki kell térni a másoktól származó, vagy a mások részére okozható hatásokra.

7) Biztonságtervezés és végrehajtás elve

Az érintetteknek a biztonságot az információs rendszerek és hálózatok kialakítása során lényeges szempontként kell kezelni, és megvalósítani.

A rendszereket, hálózatokat és irányelveket az optimális biztonság megvalósítására kell megtervezni, alkalmazni és koordinálni. Megfelelő óvintézkedéseket kell tervezni és elfogadni annak érdekében, hogy az azonosított fenyegetésekből és sebezhetőségekből származó potenciális károkat elkerüljék, vagy csökkentsék. A szervezet rendszereiben és hálózataiban található információ értékével arányos műszaki, és nem műszaki óvintézkedésekre van szükség. A biztonságot az összes termék, szolgáltatás, rendszer és hálózat alapvető elemévé, valamint a rendszertervezés és az architektúra szerves részévé kell tenni. Az átlagos felhasználók számára ez leginkább saját igényeik meghatározására, a termékek és szolgáltatások kiválasztására terjed ki.

8) Biztonságmenedzsment elve

Az érintetteknek minden szempontra kiterjedő módon kell a biztonságmenedzsment feladatokat végezniük.

A biztonságmenedzsmentnek kockázatfelmérésen kell alapulnia, felölelve az érintettek tevékenységének és működésének minden vonatkozását. A rendkívüli események megelőzésére, feltárására, és velük kapcsolatos válaszintézkedésekre, rendszer helyreállításra, karbantartásra, felülvizsgálatra és ellenőrzésre vonatkozó előremutató válaszokat kell adnia a kialakuló fenyegetésekre vonatkozóan. Az információs rendszerek és hálózatok biztonságával kapcsolatos irányelveket, gyakorlatokat, intézkedéseket és eljárásokat össze kell hangolni az összefüggő biztonsági rendszer kialakítása érdekében. A biztonságmenedzsmentre vonatkozó követelmények függenek az érintettség szintjétől, az érintett szerepétől, a szóban forgó kockázatoktól és rendszerkövetelményektől.

9) Újraértékelés elve

Az érintetteknek az információs rendszerek és hálózatok biztonságát felül kell vizsgálniuk és újra kell értékelniük. A biztonsági irányelvekben, gyakorlatokban, intézkedésekben és eljárásokban szükséges módosításokat el kell végezniük.

Folyamatosan jelennek meg új és változó fenyegetések, és sebezhetőségek. Az érintetteknek a biztonság minden aspektusát folyamatosan felül kell vizsgálniuk, át kell értékelniük és változtatniuk kell, hogy a felmerülő kockázatokat kezelhessék.

A biztonsági kultúra fejlesztése

A biztonságtudatosságot, és a közösségek biztonsági kultúrájának fejlesztését az egyének, családok, kisközösségek, szervezetek szintjén és országos szinten is lehet, és célszerű is fejleszteni. Az ismereteket végül az egyéneknek kell megtanulniuk, de kevés ember képes arra, hogy magától megtalálja, megértse és meg is jegyezze ezeket az ismereteket. Szükségesek olyan köztes csatornák, segítő szervezetek és segédeszközök, amelyek minden embernek a számára szükséges tudást a számára „megemészthető" formában juttatja el. A hazánkban is elterjedt példákat röviden ismertetjük.

Biztonságtudatosítást segítő szervezetek a társadalom különböző szintjein fejtik ki tevékenységeiket:

- **A kormányzati szervezetek** össztársadalmi és közigazgatási szinten is végeznek ilyen tevékenységet: szakpolitikai és hatósági szinten a Nemzeti Fejlesztési Minisztérium és a minisztérium szervezetébe tartozó Nemzeti Elektronikus Információbiztonsági Hatóság (a továbbiakban: NEIH), hatósági szinten a Nemzeti Biztonsági Felügyelet (a továbbiakban: NBF), rendvédelemi szinten az Országos Rendőr Főkapitányság és az Országos Katasztrófavédelmi Főigazgatóság.
- **A társadalmi szervezetek** inkább társadalmi szinten és oktatási intézményekben aktívak: Infótér Egyesület az informatika társadalmi hasznosságát kívánja segíteni, a Safer Internet hangsúlyozza a gyerekek felkészítését az internet biztonságos, és felelős használatára.
- **A szakmai szervezetek** részt vesznek a társadalmi biztonságtudatosításban, de inkább a közigazgatási szervezetek és gazdasági társaságok biztonsági kultúrájának fejlesztéséhez biztosítják a tudatosítást végző szakemberek felkészítését, a tudatosítás módszereit és segédeszközöket: informatikai ellenőrök, biztonsági szakemberek és vezetők (ISACA Magyarország Egyesület), hálózatbiztonsági és infrastruktúra védelmi szakemberek (KIBEV – Önkéntes Kibervédelmi Összefogás), számítástechnikai szakemberek (Neumann János Számítógép-tudományi Társaság), elektronikus aláírás szakértők (Magyar Elektronikus Aláírás Szövetség), informatikai igazságügyi szakértők.
- **A gazdasági társaságok** egy része a saját szervezetén belüli biztonságtudatosításon túl társadalmi szinten is végez tudatosítást. Ilyenek például a távközlési szolgáltatók, akik a szolgáltatásbiztonság növelése, és a társadalmi felelősségvállalás céljából segítik az információbiztonság tudatosítását (pl. UPC reklámok).

Biztonságtudatosítást segítő csatornák:

- **hírleveleket** biztonságtudatosítási céllal közigazgatási és szakmai szervezetek is közzétesznek, illetve belső felhasználásra nagyobb szervezetek is készítenek;
- **tájékoztató honlapokat** minden típusú szervezet alkalmaz, ezek segítik a strukturált információ átadását és egyszerűen frissíthető a tartalmuk;
- **közösségi hálózaton levő információs csatornák**at széles körben használnak ismeretátadásra, így a szakmai közösségek biztonságtudatosítást is segítik (pl. Linkedin csoport, Youtube lista);

- **közösségi tájékoztató programok**at általában állami támogatás mellett a társadalmi és szakmai szervezetek tartják (eMagyarország pontok, közösségi házak, iskolák);
- **szervezeteken belüli képzések**et a szervezet vezetése utasítására és támogatásával szerveznek, a szervezet méretétől és a rendelkezésre álló források mértékétől függően központilag, illetve helyileg készített segédeszközöket alkalmazva.

Biztonságtudatosítást segítő segédeszközök:

- **tájékoztató brosúrák:** általában egy témát 1-10 oldalban közérthetően, színes grafikai elemekkel illusztráló tájékoztató anyagok;
- **kérdőívek, és egyszerű játékok:** ösztönösen segítik a figyelem felkeltését, az ismeretek játékos megszerzését. Növeli a játékok által elért célközönség méretét, ha nem csak a játék örömeért lehet játszani, hanem egyedi díjakat is lehet nyerni;
- **figyelemfelhívó videó klipek:** általában 1-5 perc hosszú dramatizált filmanyagok, amelyek egy biztonsági kockázatot, vagy azok helyes kezelését mutatják be;
- **távoktatás (eLearning):** általában egy adott szervezeten belül, a szervezetre szabott módon végzik, amely segítségével az egyes felhasználó saját tempójában végezhető az ismeretszerzés, és mérhetővé válik az ismeretek átadásának eredményessége;
- **iskolai oktatás:** általában általános és középiskolai szinten iskolai különórákat szerveznek, az intézmény saját felkérésére, vagy biztonságtudatosítást végző társadalmi és szakmai szervezetek kezdeményezése alapján;
- **kötelező képzések szervezése:** definiált célcsoport számára, az elérendő képzési szint szerint változó időtartalmú oktatás, amely végén a résztvevők számot adnak tudásukról, a képző intézmény pedig a képzés elvégzéséről igazolást állít ki;
- **konferenciák:** eltérő célközönségű, az általánostól a mély szakmai ismeretek átadásának, információk kicserélésének és megvitatásának fóruma;
- **az ellenőrzések:** biztosítják, hogy a szabályok által előírt, és a vezetés által elvárt gyakorlatok hiánya kiderüljön a vezetés számára, akik a megfelelő szankciókat alkalmazzák a szabályszegőkkel szemben. A szankcionálás eszközei fontosak a biztonság megvalósítása során, mert ez az eszköz azok számára, akiket az oktatás és a pozitív motivációs eszközök sem voltak képesek rávenni a kívánt gyakorlatok szerinti munkavégzésre;
- **rendkívüli események kiértékelése és a következtésekről tájékoztatás készítése:** segíti a biztonság iránti figyelem fenntartását, és megelőzheti a rendkívüli események ismételt előfordulását.

A közigazgatási tevékenységet végző szervezeteknél a biztonságtudatosítást célszerű egy felépített szervezeten belüli képzési és tájékoztató program formájában megvalósítani, azonban fontos építeni a más csatornákon elérhető további képzési és tájékoztató anyagokra, mivel ezek fokozhatják a program eredményességét, és gazdaságosságát is. Jelen tájékoztató is számos hivatkozást tartalmaz további ismeretszerzési lehetőségekre.

Egy vagy több **külső szervezettel való közvetlen együttműködés** szintén segítheti a szervezeten belüli szakemberek munkáját:

- Az adott ágazat más szervezeteivel közösen szervezhetnek biztonságtudatosító programot, tarthatnak biztonságtudatosítást segítő szakmai napot, rendezvényeket.
- Az Alkotmányvédelmi Hivatal biztonságtudatosító programjában való részvétel kiegészíthető a szervezet belső tudatosító programját.
- Az általános információbiztonsági tájékoztató honlapok anyagát felhasználhatjuk a belső tájékoztató anyagok kialakítása során (ha szükséges a felhasználási engedélyt megkérve).
- Informatikai szolgáltatókkal együttműködve a közigazgatási szervezetek leszámolhatnak zombi hálózatokkal.
- Egyetemi és kutató cégekkel együttműködve gyorsabban tárhatnak fel eddig nem ismert támadási formákat, és a kiber fegyvereket.
- A középiskolai tanárok és a felsőoktatás oktatóinak felkészítése, a képzők képzése, középtávon hozzájárul ahhoz, hogy a közigazgatásba bekerülő fiatalok biztonsági tudásszintjére már csak a szervezet sajátosságait kelljen ráépíteni.
- Nagyon fontos a széles közösségekre hatással levő szervezetek, például a média cégek, vagy hírformáló bloggerek bevonása társadalmi szinten az információbiztonság tudatosság növelésében. Tájékoztató televíziós műsorok, a hírekben a rendkívüli biztonsági események magyarázata és a tanulságok levonása eredményes eszköz lehet. Tapasztalatok azt mutatják, hogy a média bevonásának hiánya inkább akadályozza a biztonságtudatosítást, minthogy semleges lenne: az információ éhséget kielégíteni kívánó bulvár hírek gyakran szakmailag nem megalapozott, vagy hibás információkat tartalmaznak, amely inkább növeli az emberek fejében a témától való félelmet, és rossz gyakorlatokat terjeszt.

A szervezeten belüli program sikere azon múlik, hogy ne csak egy kívülről jött kötelező gyakorlatként tekintsen rá a szervezet vezetése, hanem értse meg az adott szervezetre ennek a hatását, és álljon a program élére személyes példamutatással, és a szükséges források biztosításával. Fontos még, hogy a szervezeten belüli program ne csak kívülről kapott „konzerv" tájékoztató anyagra épüljön, hanem jól alkalmazható, az adott szervezeten belül is értelmezhető gyakorlati módszereket is adjon, és lehetőleg készüljenek olyan segédletek, amelyek a napi munkavégzésben is használhatóak (pl. Outlook biztonsági beállítása).

Fel kell hívni a figyelmet még arra, hogy a szervezeten belül betöltött szerephez illeszkedve kell az ismereteket átadni:

- Általános információ és IT biztonsági ismeretek ismertetése **minden munkatárs** részére, kötelezően.
- Az **információs rendszerek felhasználói** számára az információ és IT biztonsággal kapcsolatban kötelező képzés biztosítása, a jártasság megszerzésére a biztonságos munkavégzés érdekében.

- A szervezet **döntéshozó illetve vezető munkatársai** részére a felelősségi szintjüknek és szerepüknek megfelelő, kötelező képzés, és képességfejlesztés biztosítása.
- A **biztonsági szakemberek és vezetők** továbbképzési rendszerének kidolgozása, a szervezetet érintő új veszélyek és kezelésük módjára vonatkozó képzés, és a gyakorlati eljárások átadása.

A biztonsági kultúra fejlesztését a következő lépésenként célszerű megtenni:

1. A szervezeti biztonsági kultúra érettségének meghatározása.
2. A vezetés a szervezetre vonatkozó elvárások figyelembe vételével meghatározza a biztonsági kultúra kívánatos érettségi szintjét.
3. Biztonsági kultúra fejlesztési programot alakítanak ki és indítanak el.
4. A szükséges szabályozásokat, intézkedéseket, oktatásokat megvalósítják lépésről lépére.
5. A program eredményességének rendszeres mérése.

A gyakorlati életben az itt ismertet jó gyakorlatokat csak azt követően kezdik el alkalmazni, hogy egy jelentős hatással járó biztonsági rendkívüli esemény bekövetkezett. Megtakaríthatunk azonban jelentős erőforrást, és megelőzhetünk komoly presztízs veszteséget, ha elé megyünk a rendkívüli eseményeknek és felkészítjük a szervezetünket, ezzel megelőzve a bekövetkezésüket, illetve ha ez nem lehetséges csökkentve a kárt, amit okozhatnak.

Számítógépes visszaélések

A SZÁMÍTÓGÉP FELHASZNÁLÓKAT KÖZVETLENÜL FENYEGETŐ VESZÉLYEK ÉS KEZELÉSÜK

A következő fejezet nem kevesebbre vállalkozik, mint hogy a napjaink leginkább elterjedt informatikai biztonsági veszélyeit ismertesse, és segítse az Olvasót azok megértésében, és a velük kapcsolatos teendők megismerésében.

Mikor gyanakodjunk arra, hogy a számítógépünk (szervezetünk információs rendszere) nem biztonságos?

Az informatikai biztonsági problémák esetében is fontos elv „a jobb félni, mint megijedni". Ha a megszokottól eltérő működést tapasztalunk a számítógépes eszközeink használata során, célszerű utánajárni annak, hogy mi lehet az oka. Ilyen lehet a rendszer elindulásának, a rendszer működésének vagy az internetezés sebességének jelentős lassulása, a rendszerek összeomlása, a böngészés során felugró ablakokban reklámok megjelenése.

Tájékoztatni kell az informatikai részleget, vagy a szolgáltató ügyfélszolgálatát, vagy ennek hiányában a helyi informatikust a tapasztalt helyzetről.

Milyen hatással lehetnek a számítógépes veszélyek adatainkra és tulajdonunkra?

Szerteágazó módon lehetnek az információs rendszerekre ható veszélyek hatással ránk és a szervezetünkre. A hatásuk a jelentéktelentől akár a katasztrofálisig terjedhet és jóval túlmutathat az egyénen, illetve a szervezet határain.

Lehetséges hatások például:

- személyes és különleges adataink illetéktelen kezekbe kerülnek;
- visszaélnek a jogosultságainkkal, amely segítségével például munkahelyi rendszerekből adatokat töltenek le, vagy akár internetbankból pénz utalnak át a nevünkben;
- információs rendszerek működését lassítják, vagy akadályozzák meg;
- az információs rendszerünk erőforrásait felhasználva további visszaéléseket követnek el (pl. kéretlen levélküldés, más honlapok támadása);

- üzleti titkok, vagy minősített információk sérülhetnek;
- fizikailag eltulajdoníthatják eszközeinket, értékeinket.

A számítógépes veszélyek bemutatásánál arra törekedtünk, hogy a közszférában dolgozók számára értelmezhető, legvalószínűbb módszereket mutassuk be, ezáltal is segítve a lényeges ismeretek átadását.

Veszélyek: jogosulatlan adathozzáférés, módosítás

Miről beszélünk?

Jellemző hatása: Alacsony, Közepes, Magas

Az információs rendszerekben kezelt adatok illetéktelen személyek általi módosítása. A jogosulatlan adathozzáférés, vagy módosítás gyakran személyhez kötött felhasználói azonosítók és jelszavak megszerzésével, az informatikai rendszerek hiányos védelme miatt, vagy védelmének szándékos kijátszásával történik.

Mit veszélyeztet?

- Felhasználó: amennyiben nem tudja bizonyítani a felhasználó, akkor lehetséges, hogy a jogosulatlan adathozzáférések következményeit neki kell viselnie.
- Rendszerműködés: az információs rendszerekben az adatok jogosulatlan módosítása veszélyeztetheti a rendszer működését, sérülhet a rendszer zártsága.
- Információbiztonság: a szervezetek által kezelt bizalmas és titkos információk sérülhetnek, kerülhetnek jogosulatlanul nyilvánosságra, amelynek hírnevet veszélyeztető, és anyagi következményei is lehetnek.
- Nemzetbiztonság: a közigazgatáson belül fokozott hatása lehet a jogosulatlan adathozzáférésnek, az ország érdekeit, nemzetközi pozícióját veszélyeztetheti, ha egy védendő információ jogosulatlanul nyilvánosságra kerül.

Példa:

A mentési rendszer beállításainak módosításával például hibás mentések készülhetnek, és az adatok egy rendszerösszeomlást követően nem állíthatóak helyre.

A szolgáltató csődjét okozta például egy biztonsági szolgáltatásokat nyújtó cég, a DIGINOTAR 2011-es feltörése. Ebben az esetben hitelesnek látszó digitális tanúsítványokat bocsátottak ki feltehetően iráni hekkerek hat héten keresztül, és amikor feltárták a visszaélést, a hírnév csorbulása és az anyagi következmények miatt három hét alatt csődöt jelentett a holland cég. Az eset közvetve hatással volt a holland elektronikus közigazgatási szolgáltatások működésére is.

Hogyan előzzük meg?

A jogosulatlan adathozzáférés megelőzésére több módszert kell párhuzamosan alkalmaznunk:

- Fel kell készítenünk a munkatársakat arra, hogy körültekintőek legyenek. A munkahelyen használt jelszavaikat csak olyan számítógépen használják, amelyek biztonságosnak tekinthetőek. A jelszavakat csak akkor gépeljék be, ha meggyőződtek arról, hogy a környezetükben senki nem tudja leolvasni, és nem rögzítheti biztonsági kamera.
- Kockázatoknak megfelelő védelmi rendszert kell kialakítani, amelyben a felhasználók a minimálisan szükséges jogosultságokkal rendelkeznek. A védelmi rendszernek olyan nyomon követési funkciókkal (monitoring) kell rendelkeznie, hogy a rendkívüli biztonsági események jó eséllyel megelőzhetőek, azonosíthatóak vagy helyesbíthetőek legyenek.
- Az információs rendszerek tervezése során olyan kontrollokat kell előírni és megvalósíttatni, mely megakadályozza, hogy érvényesen lehessen adatokat módosítani az információs rendszer felhasználói felületét megkerülve.
- Magukat az adatokat lehet például egy „borítékba" zárni digitális aláírás technológia felhasználásával.

Mit tegyünk, ha bekövetkezik?

Haladéktalanul értesíteni kell a szervezet biztonsági vezetőjét! Az adatokhoz való jogosulatlan hozzáférés, és azok jogosulatlan módosítása komoly biztonsági probléma magában, de a védelmi rendszer nagyobb hiányosságait jelezheti a jéghegy csúcsaként egy jogosulatlan hozzáférés.

Ha még olvasna erről:

http://pcworld.hu/kozosseg/igy-lopjak-el-a-facebookos-jelszavadat.html
http://threatpost.com/final-report-diginotar-hack-shows-total-compromise-ca-servers-103112/
http://en.wikipedia.org/wiki/DigiNotar

Veszélyek: jelszavak feltörése

Miről beszélünk?

Jellemző hatása: Alacsony, Közepes, Magas

A jelszavak kitalálását, vagy számítástechnikai kódfejtő eszközökkel való megszerzését nevezzük jelszó feltörésnek. Tipikus módszer a gyakran használt jelszavak és személyes adatok próbálgatása, illetve a szavak és azok kombinációjának próbálgatása elektronikus szótárak és jelszótörő programok segítésével. Ha ezek nem működnek, akkor marad az úgynevezett nyers erő (brute force) módszer, amely az összes lehetséges karakter kombinációját kipróbálva találja meg a jelszót.

Jelszó hosszúsága	Többféle karaktertípusnál	Csak kisbetűs karaktereknél
3 karakter	0, 86 másodperc	0,02 másodperc
4 karakter	1,36 perc	0,046 másodperc
5 karakter	2,15 óra	11,9 másodperc
6 karakter	8,51 nap	5,15 perc
7 karakter	2,21 év	2,23 óra
8 karakter	2,10 évszázad	2,42 nap
9 karakter	20 évezred	2,07 hónap
10 karakter	1899 évezred	4,48 év
11 karakter	180 365 évezred	1,16 évszázad
12 karakter	17 184 705 évezred	3,03 évezred

Mit veszélyeztet?

- Felhasználó: a felhasználók személyes és különleges adatainak biztonságát veszélyezteti, ha jogosulatlanul hozzáférhetnek az adataikhoz (például elektronikus postafiókjába betörnek).
- Rendszerműködés: a kiemelt felhasználók és rendszergazdák jelszavainak megszerzésével veszélyeztetni lehet a rendszerek üzemszerű működését, vagy meg is lehet állítani. Nagyobb károkozást jelentő visszaélések kezdeti lépése lehet a jelszavak feltörése.
- Információbiztonság: a kiemelt felhasználók és rendszergazdák jelszavaival nagy mennyiségű adatot lehet jogosulatlanul megszerezni, és akár az esemény megtörténtének nyomát is el lehet tűntetni.
- Nemzetbiztonság: a közigazgatásban használt információs rendszerek jelszavainak megszerzésével adott esetben hatványozottan nagyobb kárt lehet okozni: országos rendszerek adatait megszerezni, infrastruktúra elemek működését veszélyeztetni.

Példa:

A felhő szolgáltatók üzleti modelljének terjedésével egyszerűen megvásárolható árucikké vált 1 óra szerver kapacitása, illetve akár párhuzamosan 100 vagy több szerver kapacitása megvásárolható egy – adott esetben akár lopott – hitelkártya segítségével. Innentől kezdve relatívvá vált, hogy egy jelszó feltörése elvileg egy átlagos asztali gép kéthavi kapacitását igényli, ezért elég havonta változtatni.

Nos ez 60 átlagos asztali gép számára már csak 1 nap, de négyprocesszoros szervergépből már elég 15, ha ezekben több magos processzor van akkor még kevesebb...

Leggyakoribb jelszavak: 123456, password, „telefonszámok", „születési dátumok", „szerettek neve", „kisállatok neve", „kedvenc csapat".

Hogyan előzzük meg?

Használjunk összetett és kellően hosszú jelszavakat, sőt sokkal inkább jelmondatokat, amelyek könnyen megjegyezhetők, és lehetőleg valamilyen módosítást követően – például számok használata magánhangzók helyett – szótárakban nem szereplő jelsorozatot kapjunk. Fokozottan védendő rendszerek esetén a felhasználónév-jelszó-azonosítás már nem elég, itt további kiegészítő kontrollokat indokolt alkalmazni, például kódgeneráló eszközöket (token). Ha ez nem lehetséges használjunk 8 karakternél nagyobb összetett jelszavakat, amelyeket jelszótároló és generáló alkalmazások segítségével tudunk „megjegyezni".

Az alkalmazások bejelentkezési felülete kiegészíthető olyan funkcióval, amely az elrontott jelszavak ismételt rögzítése előtt – Touring teszt (CAPTCHA), vagyis képek felismertetése segítségével – kizárja az automatizált jelszó feltörést.

Ne adjuk ki senkinek a jelszavunkat, és ne is meséljük el, hogy milyen logika szerint választunk jelszavakat!

Mit tegyünk, ha bekövetkezik?

Haladéktalanul jelentsük a biztonsági szakterületnek! Ha van lehetőségünk rá, azonnal cseréljük le a jelszót, illetve gondoljuk végig, hogy a megszerzett jelszó segítségével esetleg milyen más szolgáltatást kompromittálhatott a támadó. Például ha a postafiókunkat törte fel más szolgáltatásokhoz igényelhetett új jelszót, vagy ha máshol is ugyanazt a jelszót használtuk, akkor hozzáférhetett azokhoz a szolgáltatásokhoz is.

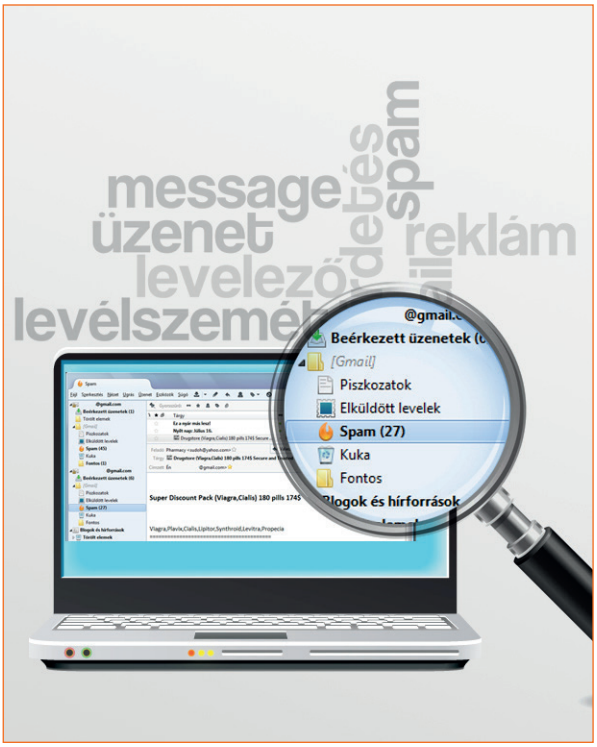
Ha még olvasna erről:

http://iesb.hu/logikai-biztonsag/biztonsagos-jelszavak-es-a-gyenge-jelszavak-feltorese/
http://www.roboform.com/hu/

Veszélyek: kéretlen levelek (spam)

Miről beszélünk?

Jellemző hatása: Alacsony, Közepes, Magas



A kéretlen levelek, ahogy az elnevezése is mutatja, olyan elektronikus levelek vagy üzenetek, amelyet semmilyen módon nem kért a címzett, és nem is várta, hogy részére küldjék. Gyakran reklámokat, felhívásokat tartalmaz, esetenként illegális termékek (például hamisított gyógyszerek) vásárlására buzdít, de része lehet más csalási módoknak (például egy részvény vásárlására szólít fel). A feladó valódi személyét szinte mindig elrejtik, vagy meghamisítják. Fontos tisztában lennünk azzal, hogy magánszemélyek címeire kéretlen leveleket küldeni törvénysértés.

Mit veszélyeztet?

- Felhasználó: az időnket rabolja leginkább a kéretlen levelek törlése, de ha bedőlünk nekik, akkor például akár az életünket (nem megfelelő minőségű illegális gyógyszer), vagy vagyonunkat (csökkenő árú részvény) is veszélyeztetheti.
- Rendszerműködés: jelentős rendszer erőforrásokat köt le a kéretlen levek továbbítása, szűrése. Akár túl is terhelheti a rendszert, ebben az esetben szolgáltatás kiesést és karbantartási költséget is jelent.
- Információbiztonság: kéretlen levelek segítségével kideríthető, hogy egy tartományon belül milyen aktív postafiókok vannak, ha figyelik a levelek olvasását, majd ezek jelszavainak feltörésével hozzáférhetnek a rendszerhez. Veszélyeztethetik a rendszerek rendelkezésre állását a szolgáltatások leterhelésével.
- Nemzetbiztonság: az Egyesült Államokban jelentős gazdasági kárt okoz az illegális szolgáltatások értékesítése, a gyógyszerhamisítás elleni harcban építenek például a kéretlen levelek forrásának azonosítására.

Példa:

Jellemző kéretlen levél típusok az illegális gyógyszereket reklámozó levelek, melyek gyakran vágyfokozó kék tabletták utánzatait hirdetik. Egyik ilyen hálózat feltárása során az FBI arra jutott, hogy

egy összetett csalási hálózat áll a kéretlen levelek mögött: több feltört szerveren keresztül küldték a kéretlen leveleket, amelyek vágyfokozó gyógyszerek megvásárlására csábítottak. Megrendelés alapján egy indiai gyógyszergyár készítette a tablettákat, egy volt szovjet tagköztársaságbeli bank állt a weboldal fizetési szolgáltatása mögött, és a megbízók Oroszországból irányították az illegális gazdasági tevékenységet.

Hogyan előzzük meg?

A kéretlen levelek egyik legjellemzőbb forrása az, hogy weboldalakra kitesszük a keresőrobotok által is olvasható formátumban az e-mail címünket, vagy kétes hírű weboldalakon regisztrálunk adott esetben ingyenes erotikus tartalom, vagy nem jogtiszta szoftver reményében. Ezeket ne tegyük! A rendszergazdák a levelező szerverek megfelelő biztonsági beállításaival, jó eséllyel képesek kiszűrni ezeket az üzeneteket.

Mit tegyünk, ha bekövetkezik?

Legjobb tanács a kéretlen levelekkel kapcsolatban, hogy olvasás nélkül töröljük, ha véletlenül a postafiókunkban landol! Véletlenül se kattintsunk rá a levelekben levő hivatkozásokra, vagy a csatolt állományokra, még a leiratkozás linkre sem! Ha a szervezetünk elektronikus postafiókjába kapunk ilyen üzenetet, akkor azt jelezzünk a belső szabályzat szerint. Azért fontos jelezni egy kéretlen levelet is, mert egy összetett támadás részei is lehetnek. Jogi lépéseket is lehet tenni, ha azonosítható a forrása, és bejelenthetik az NMHH részére.

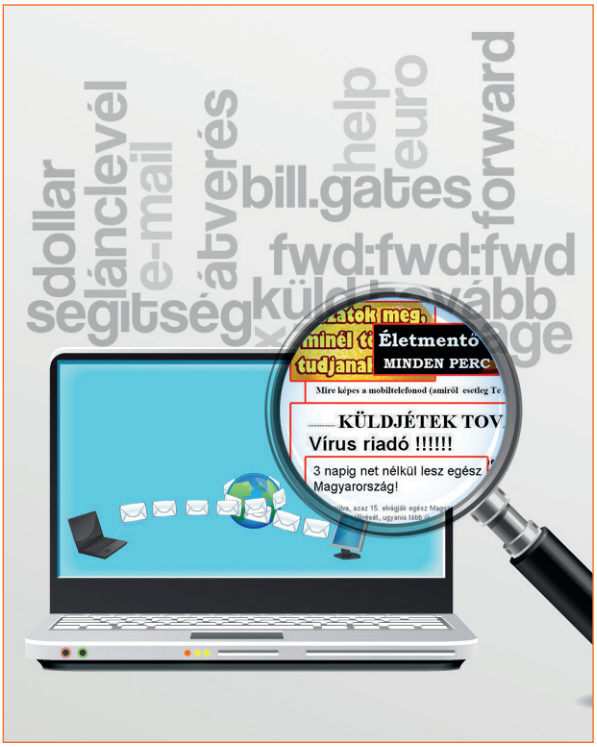
Ha még olvasna erről:

http://hu.wikipedia.org/wiki/Spam
http://www.virushirado.hu/oldal.php?hid=44
http://infoter.eu/cikk/magyarorszagon_az_e-mailek_70_szazaleka_spam

Veszélyek: hamis lánclevelek (hoax)

Miről beszélünk?

Jellemző hatása: Alacsony, Közepes, Magas



Olyan elektronikus levél, vagy üzenet, amely valamilyen új információt oszt meg, és arra ösztönzi a címzettet, hogy a levelet minden ismerősével önkéntes módon ossza meg. Első formái például egy új – fiktív – vírusra hívták fel a figyelmet, amelyek fertőzését néhány fájl törlésével megakadályozhatjuk, ugyanakkor ezek a fájlok a Windows szükséges részei voltak, így törlésük a rendszer működését akadályozta meg.

Mit veszélyeztet?

- Felhasználó: az időnket rabolják leginkább a hamis lánclevelek, és gyakran hamis reményt keltenek. Továbbküldésük rossz fényben tűntet fel minket azon ismerőseink előtt, akik ismerik az információbiztonsági kockázatokat.
- Rendszerműködés: jelentős rendszer erőforrásokat köt le a továbbításuk, szűrésük.
- Információbiztonság: egyik „legjobb” módszer az aktív elektronikus levélcímek összegyűjtésére, amelyet a kéretlen levelek küldői előszeretettel alkalmaznak. Így a biztonság elleni támadás előkészítésére is használhatják.
- Nemzetbiztonság: személyek kapcsolatrendszerének feltérképezésére alkalmasak a lánclevelek, amelyek segítségével további információ szerezhető meg.

Példa:

Időről időre felbukkannak hasonló lánclevelek, amely minden x. címzettnek valamilyen ajándék telefont, vagy pénzt ígérnek. Ajándék telefont, de pénzt sem kapott egyetlen továbbküldőjük sem, viszont aki indította az a hozzá visszajutó, működő elektronikus levélcímeket például el tudja adni, vagy kéretlen reklámokkal tudja megtölteni.

Hogyan előzzük meg?

Hívjuk fel családtagjaink és ismerőseink figyelmét az információbiztonság fontosságára, különösen, ha kéretlen levelet, vagy hamis lánclevelet küldenek, akkor küldjük vissza nekik azt az oldalt, ami igazolja, hogy átverés az üzenet. Néha sértődéshez vezet a módszer, de hosszú távon beválik.

Mit tegyünk, ha bekövetkezik?

Honnan ismerhetjük fel a lánccleveleket? Legkönnyebb dolgunk akkor van, ha már az elején szerepel egy utasítás: „Küldd el ezt a levelet minél több embernek!", emellett gyanús, ha szélsőséges módon a pozitív érzelmeinkre hat (pl. halálos beteg utolsó kívánsága), vagy komoly veszéllyel fenyeget (pl. vírus tönkreteszi a géped). Szoktak még híres emberekre, vagy nagyvállalatokra hivatkozni, hogy hihetőbbnek tűnjenek.

Legjobb tanács a hamis láncelevelekkel kapcsolatban, hogy olvasás nélkül töröljük, ha véletlenül a postafiókunkban landol! Véletlenül se higgyük el, ami le van benne írva, ne küldjük tovább szeretteinknek vagy rosszakaróinknak. Ha gyanús egy levél szövege, akkor a levél jellemző fogalmait (kulcsszavait) írjuk be egy kereső programba, és jó eséllyel egy láncelevelekről szóló oldalt fogunk kapni.

Ha még olvasna erről:

http://hu.wikipedia.org/wiki/Hoax
http://wwwold.kfki.hu/cnc/email/hoax.html
http://www.infoter.eu/cikk/gitaros_a_libiai_csataban_avagy_a_photoshop_arnyeka
http://www.origo.hu/techbazis/internet/20100924-hoax-uzenetek-amiket-semmikepp-sem-szabad-tovabbkuldeni.html

Veszélyek: vírusok

Miről beszélünk?

Jellemző hatása: Alacsony, Közepes, Magas

Olyan programrészlet, amely a megfertőzött program működtetése során másolja önmagát. Valamilyen meghatározott feltétel (pl. egy adott napon az évben) bekövetkezése esetén figyelmeztető, vagy romboló tevékenységet végez. Gyakran komoly károkat okoz, szolgáltatások megszakadását, vagy adatvesztést.

Több típusuk van, terjedésük szerint lehetnek a fájlokat fertőző vírusok (pl. makro vírus) és a rendszerek indításához szükséges bootszektort fertőző vírusok. Abban különböznek, hogy hogyan kerülnek a számítógépre. A fájlokat fertőző vírusok indítható állományok, vagy dokumentumok segítségével terjednek, magukat beleírva az állományba. Ha egy ilyen programot elindítunk, akkor a vírus aktivizálódik.

A makrovírusok többnyire olyan, szövegszerkesztőkkel létrehozott dokumentumokkal terjednek, amelyek rendelkeznek programozási lehetőséggel, makronyelvvel, pl. a doc fájlok. Táblázatkezelő programok esetében az előfordulás ritkább, de nem kizárt.

A bootszektor vírusok a számítógépek operációs rendszert betöltő területét fertőzik meg. A rendszerek indításával aktivizálódnak tehát.

Mit veszélyeztet?

- Felhasználó: különféle kellemetlen következménnyel járhatnak: adatvesztés, számítógépünk használhatatlanná válása, adatszivárgás, stb.
- Rendszerműködés: fejlettebb vírusok a védelmi rendszerek megkerülésével képesek szaporodni, akár teljes szervezet hálózatát megfertőzni, ezzel erőforrásokat kötnek le és a normál munkavégzést akadályozzák.
- Információbiztonság: vírusok segítségével szerezhető jogosulatlan hozzáférés rendszerekhez.
- Nemzetbiztonság: az információs rendszerek elleni összetett támadás egy elemeként kártevő kódok rendszerekbe juttatását végezhetik.

Példa:

Az első vírus állítólag egyidős az első számítógéppel, és az első személyi számítógép (PC) vírus (BRAIN)is elég korán elszabadult. Az egyik vírusirtó cég utánajárt a vírus megjelenésének 25. évfordulóján, és meg is találták a szerzőket Pakisztánban. Ez még csak információt terjesztett.

Ezt követően jelentek meg a vicces vírusok (pl. potyogós vírus), a figyelemfelhívó vírusok a 90-es évek elején, majd az irodai alkalmazások terjedésével párhuzamosan a dokumentumokon keresztül terjedő makrovírusok, amelyek az elmúlt évtizedben már sokkal inkább a feketegazdaság termelési eszközeivé váltak, lehetővé téve adatlopásokat, és lebénítva a szolgáltatásokat.

Hogyan előzzük meg?

A vírusfertőzéseket naprakész – automatikusan frissülő – víruskereső szoftver, és tűzfal alkalmazásával jó eséllyel megelőzhetjük. Fontos megelőző intézkedés még a külső adathordozók vírusellenőrzése a rajtuk levő állományok használata előtt. Ne állítsuk le a rendszeresen ütemezett víruskeresést a munkahelyi gépünkön, azok feladata a vírusok felderítése.

Mit tegyünk, ha bekövetkezik?

Ha vírust feltételezünk a gépen, jelezzük a szervezet szabályzatának megfelelően, általában a központi hibabejelentőn. Ne próbáljuk magunk leirtani.

Ha az otthoni gépünk vírusos, akkor szükségünk lesz egy naprakész vírus írtóra, és egy vírusmentes indítólemezre / USB memóriára. A gép vírusmentes indítólemezről való újraindításával meggyőződhetünk a vírusfertőzésről a víruskereső teljes keresés funkciójának futtatásával. A fertőzött állományokat, ha szerencsénk van, tudja javítani a vírusirtó, ha nem, akkor ezeket törölnünk kell. Az érintett fájlok alapján azonosítható, hogy honnan származik a fertőzés. A törölt állományokat mentésből vissza kell állítani. Előfordulhat, hogy a teljes rendszer újratelepítésével tudunk csak megszabadulni a vírustól, ebben az esetben a lényeges rendszerbeállítások (pl. elektronikus postafiók cím, felhasználónév) és az adataink mentését el kell végezni, hogy ne szenvedjünk adatvesztést.

Ha még olvasna erről:

http://www.cert.hu/content/amit-v%C3%ADrusirt%C3%A1sr%C3%B3l-tudni-kell
http://www.virushirado.hu/oldal.php?hid=43
http://campaigns.f-secure.com/brain/
http://computerworld.hu/computerworld/40-eves-az-elso-komputer-virus.html

Veszélyek: féreg (worm)

Miről beszélünk?

Jellemző hatása: Alacsony, Közepes, Magas

A számítógépes férgek olyan kártevő programok, amelyek a hálózatok hibáit, vagy hiányos biztonsági beállításait használják fel arra, hogy terjesszék magukat. Az önsokszorosításon kívül a féreg sokféle dologra beprogramozható, pl. fájlok törlésére. Egyik jellemző következményük, hogy hátsó ajtót nyitnak a rendszerekre, amin keresztül adatokat szereznek meg, illetve zombi hálózat részévé teszik a támadott számítógépet.

Mit veszélyeztet?

- Felhasználó: felemészthetik a számítógép memóriáját.
- Rendszerműködés: ha más kárt nem is okoznak, akkor is terhelik a rendszerek kapacitását, és csökkentik a rendelkezésre álló adathálózati sávszélességet.
- Információbiztonság: a férgek által nyitott hátsó ajtók segítségével adatok lophatóak el a rendszerekből, ezért komolyan veszélyeztetik az információbiztonságot.
- Nemzetbiztonság: a férgek nem kímélik a közszféra rendszereit sem, ezért az adatok ellopása ebben az esetben érintheti a nemzeti érdekeket is.

Példa:

A férgek nagy részét csak arra tervezték, hogy terjedjenek. Ezáltal felhívják a figyelmet valamilyen biztonsági hibára. Azonban még ezek (pl. a MyDoom) is jelentős kárt képesek okozni. 2009-ben például a francia légierő gépeit több támaszponton is földre kényszerítette egy féreg (Conficker) fertőzése, mert a repülési terveket nem tudták eljuttatni a pilótákhoz az informatikai rendszer biztonsági zárlata miatt. Angliában kórházi rendszereket és hadihajókon használt számítógépeket is megfertőztek. Egyes feltételezések szerint kormányzati forrást is használtak egyes férgek fejlesztéséhez, amely segítségével célzott kibertámadásokat képesek megvalósítani.

Hogyan előzzük meg?

A számítógépek és hálózatbiztonsági eszközök és szoftverek rendszerek frissítésével, az ismert férgek által alkalmazott kommunikációs csatornák tűzfalakban való blokkolásával előzhetjük meg a terjedésüket.

Mit tegyünk, ha bekövetkezik?

A féregfertőzés bekövetkezését követően a fertőzött gépek hálózatból való kizárásával csökkenthető a kár. A helyreállítás ezt követően a hálózat biztonságossá tételével folytatódhat, majd a kártevők egyenként történő leirtásával, vagy a fertőzött gépek újratelepítésével oldható meg teljesen.

Ha még olvasna erről:

https://en.wikipedia.org/wiki/Computer_worm
http://en.wikipedia.org/wiki/Conficker
http://www.infoter.eu/cikk/a_nagy_conficker-konspiracio_a_titkosszolgalat_is_erintett_lehet
http://www.digitalthreat.net/2009/05/worm-evolution/#

Veszélyek: Trójaik

Miről beszélünk?

Jellemző hatása: Alacsony, Közepes, Magas

A görög mitológiában szereplő trójai falovakhoz hasonlóan, az embereket megtévesztésével éri el, hogy a számítógépre telepítsék. A trójai programok olyan hamis szoftverek, amelyek a látszólagos funkciójuk mellett más nem jogszerű tevékenységet végeznek. Az egyszerűbb változatai csak a hasznosság látszatát mutatják, míg fejlettebb változataik valóban képesek az ígért funkciók elvégzésére. A leggyakoribb fertőzési módszert a letöltések és a veszélyes honlapok jelentik. A számítógépünk trójaival fertőződhet egy üzenet csatolmányának megnyitásával, azonnali üzenetküldő programon keresztül, de megkaphatjuk valamilyen adathordozón keresztül is.

Mit veszélyeztet?

- Felhasználó: a felhasználók személyes és érzékeny adatait veszélyezteti a trójai programok jelenléte.
- Rendszerműködés: a rendszerünk biztonsága sérül, ha arról adatokat szivárogtatnak kifelé, vagy távolról képesek hozzáférni a csalók.
- Információbiztonság: a szervezeteknél levő fertőzött gépek fokozott veszélyt jelentenek a szervezet által kezelt információ biztonságára.
- Nemzetbiztonság: az adatlopások érinthetnek olyan információt, hálózatok működésére, munkahelyi információkra vonatkozóan, amelyek veszélyeztethetik a nemzetbiztonságot is.

Példa:

Egyik legismertebb trójai a Zeus nevű kártevő: banki információkat, és felhasználói azonosítókat és jelszavakat gyűjtött össze és lopott el főleg 2007 és 2011 között. Becslések szerint 70 millió dollárt tulajdonítottak el a segítségével és felszámolására irányuló FBI akcióban 100 embert tartóztattak le az Egyesült Államokban, az Egyesült Királyságban és Ukrajnában.

Főbb típusai:

- a hálózat felderítő programok;
- trójaiba beépített vírus terjesztők (adott feltétel teljesülése esetén szabadon engedi a vírust);
- időzített bombát tartalmazó programok (adott idő eltelte után megszűnik működni, vagy egy adott időpontban aktivizálódik).

Hogyan előzzük meg?

A számítógépek és hálózatbiztonsági eszközök és szoftverek rendszerek frissítésével, az ismert trójaik által alkalmazott kommunikációs csatornák tűzfalakban való blokkolásával előzhetjük meg a terjedésüket.

Mit tegyünk, ha bekövetkezik?

A trójai fertőzés bekövetkezését követően a fertőzött gépet hálózatból le kell választani, és vírusirtó programmal vagy manuálisan le kell telepíteni, vagy törölni a szoftvert. A helyreállítás esetenként csak a fertőzött gépek újratelepítésével történhet meg.

Ha még olvasna erről:

http://hu.wikipedia.org/wiki/Tr%C3%B3jai_program
http://www.sg.hu/cikkek/77211/irani_uzemeket_tamadott_a_stuxnet
http://en.wikipedia.org/wiki/Zeus_(Trojan_horse)
http://www.infoter.eu/cikk/nemet_hackerek_trojai_haboruja

Veszélyek: rootkit-ek (rendszermagot fertőző kártevő)

Miről beszélünk?

Jellemző hatása: Alacsony, Közepes, Magas

A rootkit olyan szoftvercsomag, amelyek segítségével egy hekker egyszerűen bejuthat a korábban feltört rendszerbe. A számítógépes rendszerek központi részét, a rendszermagot nevezik angolul rootnak (gyökér) és a telepítő programot kit-nek. Ennek segítségével bizalmas adatokat gyűjthet, vagy irányíthatja a fertőzött számítógépet.

A legtöbbször úgy telepítik magukat, hogy a rendszerfájlokat megfertőzik ugyan, de azok továbbra is ellátják feladatukat. A rootkit végső célja a kártékony kiber-tevékenység támogatása, például a billentyű-leütések naplózása vagy a hálózati kapacitás illetéktelen felhasználása adatok kiszivárogtatására, kéretlen levelek küldésére. Gyakran Windows rendszerekre készülnek, annak népszerűsége miatt.

Mit veszélyeztet?

- Felhasználó: az átlagos felhasználók gyakran észre sem képesek venni egy rootkit jelenlétét a számítógépén. Lényegében láthatatlan módon képes a számítógép működésének befolyásolására, és adatok megszerzésére.
- Rendszerműködés: gyakran látszólag nem befolyásolják a rendszerek működését, azonban alapvetően veszélyeztetik a rendszerek biztonságát.
- Információbiztonság: segítségükkel sérül a fertőzött rendszerekben kezelt információk biztonsága, jogosulatlanul megismerhetik és letölthetik azokat.
- Nemzetbiztonság: idegen államok gyakran használják hírszerzési célra, vagy gazdasági társaságok esetében ipari kémkedésre is.

Példa:

Windowson először 1999-ben találtak rootkit-et (NTRootkit), Mac operációs rendszeren 2009-ben, a közelmúltban pedig ipari rendszereket fertőző rootkit-et is találtak (Stuxnet). 2005-ben hívta fel a

figyelmet a rootkit-ek re a Sony BMG által kiadott CD lemez, amely szerzői joga védelme érdekében egy Extended Copy Protection nevű programot telepített a háttérben, amely korlátozta a CD-hez való hozzáférést. Nagy botrány és bírósági ügy is lett belőle, mivel a Sony BMG az általa forgalmazott lemezekkel a felhasználókra veszélyes, és akár anyagi kárt okozó szoftvert telepített anélkül, hogy megfelelő tájékoztatást nyújtott volna. A rosszindulatú kártevőkre, férgekre és trójai programokra jellemző módon rejtőzködő, Windowst futtató gépekre észrevétlenül települő és szabályosan, a Windows segítségével el nem távolítható DRM-programok[10] ismert biztonsági rést kínálnak a bűnözők számára a rendszer eredményesebb megfertőzésére, valamint a licencszerződéssel ellentétben adatokat gyűjtenek és továbbítanak a Sony BMG szerverei felé.

Hogyan előzzük meg?

A számítógépek rootkit-tel való megfertőződését úgy előzhetjük meg, ha átfogó végpont védelmi szoftvercsomagot használunk, azaz vírusvédelmi szoftvert (anti-virus), szoftveres tűzfalat (firewall), továbbá odafigyelünk arra, hogy rendszeresen frissítsük a számítógépre telepített szoftvereket. Ezeket megfelelő beállításokkal automatikussá lehet tenni.

Mit tegyünk, ha bekövetkezik?

Ha arra gyanakszunk, hogy nem csak mi irányítjuk a gépünket, frissítsük a védelmi szoftvereinket, majd kapcsoljuk ki a hálózatot és teljes keresést indítsunk el rajtuk.

Munkahelyünkön a vonatkozó szabályzatoknak megfelelő eljárásrendet kövessük! Általában ez központi hibabejelentőn való bejelentés megtételét jelenti. A rootkit-eket esetenként csak célzott keresésssel, speciális biztonsági szoftverekkel lehetséges azonosítani, és eltávolítani.

Ha még olvasna erről:

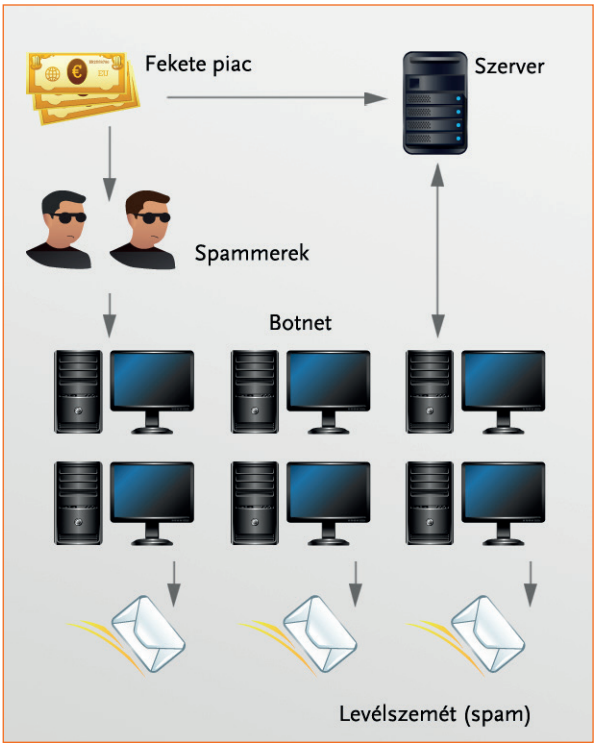
http://hu.wikipedia.org/wiki/Rootkit
http://www.infoter.eu/cikk/iden_is_szamithatunk_a_rejtozkodo_kartevokre
http://www.virushirado.hu/hirek_tart.php?id=1980

[10] DRM: Digital Rights Management, digitális jogkezelő eljárás.

Veszélyek: zombihálózat (botnet)

Miről beszélünk?

Jellemző hatása: Alacsony, Közepes, Magas



Az illegális zombi gépek hálózatát olyan hétköznapi gépek alkotják, amelyeket otthon, az iskolában, vagy rosszul védett vállalati hálózatok részeként használunk. Azért nevezzük zombi hálózatnak, mert tudtunk és engedélyünk nélkül olyan rejtett program fut rajtuk, amely egy központi vezérlő számítógéptől időközönként utasításokat fogad, és az utasítások szerint számolási feladatot végez, kéretlen levelek millióit továbbítja, személyes adatokat lop el, elrejti a hackerek eredeti IP címét vagy akár szolgáltatás megtagadásra irányuló támadást (DoS) indítatnak róla. Egy-egy nagyobb zombi hálózat több tízezer gépet képes irányítani.

Mit veszélyeztet?

- Felhasználó: a nem jól védett otthoni gépeket támadhatja, a gépek erőforrásainak használatával a felhasználó számára lassítja a gépet. Ha illegális tevékenységre használják a gépet, akkor a felhasználónak számolnia kell jogi eljárással, ahol akár bizonyítania is kell tudnia, hogy nem szándékosan intézett támadást a gépéről.
- Rendszerműködés: vállalati hálózatok gépein megtelepedve jelentős számítási kapacitást köthet le, illegális tevékenységek kiindulópontja lehet.
- Információbiztonság: a zombihálózat adatok ellopásához is eszközül szolgálhat, de a rajta keresztül végzett DoS támadás a szolgáltatások rendelkezésre állását akadályozza.
- Nemzetbiztonság: léteznek olyan fejlett zombi hálózatok, amelyeket kormányok, illetve bűnszervezetek építtettek ki hírszerzés, vagy akár ipari kémkedés céljából.

Példa:

Az elmúlt években több, euróban is milliós nagyságrendű kárt okozó összehangolt visszaélés sorozatot tártak fel a rendvédelmi szervek és biztonsági szolgálatok. A BlueFrog DDoS támadást valósított meg egy izraeli internet biztonsági cég ellen, 2006-ban heteken keresztül akadályozták a cég oldalainak működését. Használnak zombi hálózatokat internetes reklámozási csalásra, ahol a botnet végzi

a felhasználók helyett a reklámokra kattintást, átverve a reklámok hatékonyságát mérő rendszereket, így gyakran dollár milliókat is juttatva a reklámokat megjelenítő oldalaknak. Szintén gyakori a zombi hálózatok kéretlen levélküldésre való felhasználása.

A teljes kormányzat működését akadályozta napokig az Észtország elleni botnet támadás, továbbá a banki rendszerekben is komoly gondokat okozott.

Hogyan előzzük meg?

A számítógépek kártevő programokkal való megfertőződését úgy előzhetjük meg, ha átfogó végpont védelmi szoftvercsomagot használunk, azaz vírusvédelmi szoftvert (anti-virus), szoftveres tűzfalat (firewall), kártevő program felderítő szoftvert (anti-malware), továbbá odafigyelünk arra, hogy rendszeresen frissítsük a számítógépre telepített szoftvereket. Ezeket megfelelő beállításokkal automatikussá lehet tenni.

Mit tegyünk, ha bekövetkezik:

Ha arra gyanakszunk, hogy nem csak mi irányítjuk a gépünket, – például ha nem ülünk a gép előtt, akkor is energiatakarékos módba lépés helyett folyamatosan működik – frissítsük a védelmi szoftvereinket, majd kapcsoljuk ki a hálózatot és teljes keresést indítsunk el rajtuk. Munkahelyünkön a vonatkozó szabályzatoknak megfelelő eljárásrendet kövessük! Általában ez központi hibabejelentőn való bejelentés megtételét jelenti. A zombi hálózatoktól csak következetes védelmi intézkedésekkel lehet megszabadulni, mert egyre fejlettebb módszereket alkalmaznak, és újabban önvédelmi eljárásokat is beléjük programoztak (észleli, ha fel akarják tárni a működését, és megváltoztatja azt).

Ha még olvasna erről:

https://en.wikipedia.org/wiki/Botnet
http://www.infoter.eu/cikk/tavaly_ev_vegen_is_jelentos_karokat_okoztak_a_tomeges_halozati_elarasztasos_tamadasok
http://www.itbusiness.hu/Fooldal/itpeople/technologia/Zombihalozat_zombiszoftver.html
http://www.biztonsagosinternet.hu/tippek/a-botnetekrol

Veszélyek: reklámprogramok (adware)

Miről beszélünk?

Jellemző hatása: Alacsony, Közepes, Magas

A reklámprogram célja, hogy egy terméket, számítógépes programot, annak készítőjét vagy egy céget reklámozzon, általában trójaiként, vagy kereskedelmi programok ingyenes változatainak részeként települ a számítógépre. Alapvetően nem jelentenének nagy veszélyt, ha ennek a modellnek a leple alatt olyan változatok nem jelentek volna meg, amelyek a személyes adatainkat, böngészési tevékenységünket gyűjtik és továbbítják.

Mit veszélyeztet?

- Felhasználó: a tevékenység végrehajtását megelőzően, vagy azzal párhuzamosan a képernyő egy részét reklámok takarják el, elterelik a felhasználók figyelmét. A reklámprogramok egy része személyes adatok gyűjtését végzi, ami a magánszféránk sérülésével jár.
- Rendszerműködés: a rendszer és hálózat erőforrásait a reklámok megjelenítésével terhelik.
- Információbiztonság: a tevékenységeink, szokásaink megfigyelése adatvédelmi kockázat.
- Nemzetbiztonság: a jogosulatlanul használt szoftverek adatszivárgást tehetnek lehetővé.

Példa:

Általában kereskedelmi szoftverek ingyenes változatainak részeként, vagy trójai kártevő programként települnek az adware programok. Újabban különösen megnőtt a számuk a mobiltelefonra készült alkalmazások között (pl. Android alkalmazásbolt).

Hogyan előzzük meg?

Számítógépünkre csak a felhasználói feltételek átolvasását követően telepítsünk szoftvereket, és csak megbízható forrásból: szaküzletből, ismert web áruházból, ismert szoftvergyűjteményből. Szervezetek esetében praktikus a felhasználói gépekre történő egyes szoftverek telepítését megtiltani, ez a reklámszoftverek telepítésére is vonatkozik.

Mit tegyünk, ha bekövetkezik?

Általában hasznos gyakorlat, ha olyan szoftvereket, amelyekre már nincsen szükségünk, eltávolítunk a számítógépünkről. Ezzel rendszer erőforrások szabadulnak fel, és csökkentjük a biztonsági kockázatokat. Amennyiben a reklámszoftver illegális tevékenységet is végez, akkor a kártevő programokhoz hasonlóan kell eljárni velük.

Ha még olvasna erről:

http://en.wikipedia.org/wiki/Adware
http://pcforum.hu/szotar/?term=adware
http://www.technet.hu/hir/20120625/veletlenul_orult_nyomtatasba_kezdhet_egy_trojai/

Veszélyek: kémprogramok (spyware), kártevő programok (malware)

Miről beszélünk?

Jellemző hatása: Alacsony, Közepes, Magas

Az interneten terjedő olyan programok összessége, amelyek célja, hogy a felhasználó tudomása nélkül megszerezzék a megfertőzött számítógép felhasználójának személyazonosító, banki vagy más személyes adatait. Ezeket általában böngészési szokásaink megfigyelésére, vagy visszaélések elkövetésére használják fel. Feltelepülésükre általában a felhasználó figyelmetlensége és/vagy a rendszerek biztonsági hiányosságai adnak lehetőséget.

A kémprogramok újabban már több funkció elvégzését lehetővé tevő modulokból állnak, amely a „kémkedés” mellett a rendszerek működésébe több módon képes beavatkozni. A közelmúltban megjelentek olyan kártevők (ransomware), amelyek váltságdíjat próbálnak meg kicsikarni a felhasználókból, az adatok/számítógép használhatatlanná tételével.

Mit veszélyeztet?

- Felhasználó: az interneten keresztül vezérelhető kémprogramok veszélyeztetik személyes és érzékeny adatainkat, jelszavainkat, bankkártya adatainkat, internetbank adatainkat.
- Rendszerműködés: a rendszerek működését általában kevéssé befolyásolják, ezzel is elősegítve azt, hogy rejtve maradjanak.
- Információbiztonság: a kémprogramok újabban az információ bizalmasságának sérülése mellett, a védelmi rendszerek egyéb módon való kijátszását is lehetővé teszik.
- Nemzetbiztonság: a közelmúlt tapasztalatai azt mutatják, hogy idegen államok agresszív módon használják a kémprogramokat információszerzése, ipari kémkedésre, és esetenként rendszerek elleni szándékos károkozásra.

Példa:

A kémprogramok hozzásegítik a támadókat mások nevében kötött szerződések és más kötelezettségek elvállalására (megszerzett személyazonosító adatokkal), de banki folyószámlákról is emeltek le pénzt ilyen módon.

A Duqu olyan kártékony program (felfedezője egyébként a BMGE CrySyS Adat- és Rendszerbiztonság Laboratóriuma), amely különböző programrészekből áll: pl. információ gyűjtő, kernel driver, kód beinjektáló modul. A kártevő moduláris felépítésű, több egyedi változata létezik, ezért a megtalálása is nehezebb.

Hogyan előzzük meg?

A hagyományos információs rendszer és hálózat védelmi funkciók (víruskereső, tűzfal) alkalmazása és naprakész frissítése fontos, de nem feltétlenül elég a kémprogramok megelőzésére.

Mit tegyünk, ha bekövetkezik?

A szervezet eljárásrendje szerint tájékoztassuk a biztonsági szakterületet. Fontos, hogy a kémprogramok, és működtetőik elleni sikeres küzdelemhez szükség van az program működési mintáira, a rendszer naplóeseményeire, ezért ezeket a feltárást megelőzően ne töröljük.

Ha vírusvédelmi rendszerünk működése ellenére kémprogram kerül a gépünkre, akkor az adott kémprogram célzott eltávolítását lehetővé tevő kémprogram eltávolító szoftvert hívhatunk segítségül. Az erősen fertőzött rendszerek esetén gyakran csak a rendszer teljes újratelepítése ad megoldást.

Ha még olvasna erről:

http://hu.wikipedia.org/wiki/K%C3%A9mprogram
http://hu.wikipedia.org/wiki/K%C3%A1rt%C3%A9kony_programok
http://hu.wikipedia.org/wiki/Duqu
http://www.virushirado.hu/hirek_tart.php?id=708

Veszélyek: hamis szoftverek (rogue software, scareware)

Miről beszélünk?

Jellemző hatása: Alacsony, Közepes, Magas

Illegális, illetve legálisnak látszó, de a látszólagos funkciók mellett illegális tevékenységet is végző szoftverek. Ilyenek például az úgynevezett trójai falovak, amelyek például látszólag játékprogramok, de emellett megfigyelik a felhasználók tevékenységét.

Mit veszélyeztet?

- Felhasználó: a felhasználók tudta nélkül olyan funkciókat élesít a számítógépen, amelyeket a felhasználó nem kívánt élesíteni, ennek következtében a program adatokat gyűjthet a gépéről. A licenc feltételektől eltérően értékesített, például másolt DVD lemezen értékesített szoftverek, még ha meg is egyeznek az eredetileg kiadott szoftverrel, jogszabályi megfelelési kockázatot jelentenek.
- Rendszerműködés: a hamis, illetve illegális szoftverek hibás működése esetén nincs lehetőségünk a gyártói támogatás igénybevételére.
- Információbiztonság: a hamis, illetve illegális szoftverek használata arra utal, hogy az információbiztonsági kontroll rendszer nem megfelelően működik a szervezetnél.
- Nemzetbiztonság: amennyiben kormányzati rendszerekbe jutnak be, veszélyeztethetik az információs rendszerek biztonságát.

Példa:

Az egyik jellemző álcája a kártevő programoknak, hogy víruskeresőnek álcázzák magukat. A gyanútlan felhasználó figyelmét arra hívják fel, hogy vírus van a gépén, amit ez a program ingyenesen eltávolít, ha telepítjük. A háttérben pedig reklámokat jelenítenek meg, felhasználói szokásokat gyűjtenek, vagy adatgyűjtési tevékenységet végeznek.

Hogyan előzzük meg?

A hamis szoftverek telepítését megelőzhetjük, ha megbízható forrásból származó szoftvereket töltünk le, vagy vásárolunk. Megbízható forrás lehet egy ismert gyártó saját weboldala, vagy ingyenes és shareware alkalmazások gyűjtőoldala. Ha kételkedünk egy szoftver megbízhatóságáról, akkor egy internetes keresés általában megfelelő információt biztosít az adott szoftverről, vagy weboldalról. Ha valakinek korábban problémája volt vele, akkor jó eséllyel felhívta rá mások figyelmét.

Mit tegyünk, ha bekövetkezik?

Ha hamis szoftvert telepítettünk, és rájöttünk, akkor nincs más hátra, mint a program eltávolítása, ezt az operációs rendszernek a programok eltávolítása funkciójával tehetjük meg. Ha csak letöröljük a programot, akkor a beállításai még gondot okozhatnak. A beállítások kézzel való törlése pedig haladó számítógépes ismereteket feltételez. Ha a munkahelyi gépünkön találtunk hamis szoftvert, akkor a belső szabályzatban leírtak szerint jelentsük be!

Ha még olvasna erről:

https://en.wikipedia.org/wiki/Rogue_security_software
https://en.wikipedia.org/wiki/List_of_rogue_security_software
http://www.sg.hu/cikkek/71552/minden_napra_jut_egy_uj_hamis_biztonsagi_szoftver
http://www.infoter.eu/cikk/karterites_a_hamis_biztonsagi_szoftvert_terjeszto_bunbanda_aldozatainak

Veszélyek: adathalászat (phising)

Miről beszélünk?

Jellemző hatása: Alacsony, Közepes, Magas

Egy csaló weboldal egy ismert szervezet vagy vállalat hivatalos oldalának láttatja magát, és megpróbál személyes adatokat, például felhasználói azonosítókat, jelszavakat, bankkártya adatokat megszerezni.

A csalók gyakran elektronikus levelet vagy azonnali üzenetet küldenek a címzettnek, amiben elérik, hogy az üzenetben szereplő hivatkozásra rákattintson, amely egy átalakított weboldalra vezeti. Ha követi az ott szereplő utasításokat, akkor áldozattá válhat.

Mit veszélyeztet?

- Felhasználó: leginkább a felhasználók érzékeny és bizalmas adatait, pénzügyi információt veszélyeztetik.
- Rendszerműködés: a rendszereink működését általában nem akadályozzák, kéretlen levelekként jelennek meg. Ha a támadás a szervezet információs rendszerei ellen irányul, akkor a szervezet rendszereiben használt felhasználó nevek és jelszavak megszerzésével a rendszer működését is befolyásolhatják.
- Információbiztonság: sérülhetnek a személyes adataink, pénzügyi adataink a támadás következtében.
- Nemzetbiztonság: ha a támadás a közszféra valamely információs rendszere ellen irányul, akkor nemzetbiztonsági kockázatot jelent.

Példa:

Gyakran valós bankok internetbank oldalát imitálva, kéretlen hamis elektronikus levelekkel kívánják rávenni a felhasználókat arra, hogy megadják felhasználó nevüket, jelszavukat, PIN kódjukat, és egyéb azonosítóikat, majd ezek ismeretében megszerzik a pénzüket. A hazai nagybankok többségét érte már ilyen jellegű támadás, de a bankok közötti összefogással ezek által okozott károkat csökkenteni tudták.

Hogyan előzzük meg?

Az adathalászatot a felhasználók és az ügyfelek képzésével, biztonságtudatosításával előzhetjük meg. Emellett több böngészőhöz telepíthető olyan kiegészítő, amely jelez adathalász oldalra lépéskor.

Mit tegyünk, ha bekövetkezik?

Ha adathalászat gyanúját tapasztaljuk jelentsük a szervezet szabályzatának megfelelően, és például a bankunknál. Ha anyagi kár ér minket, érdemes feljelentést tenni a rendőrségen.

A szervezetek úgy csökkenthetik a hatását, hogy monitoring rendszerek segítségével már a próbálkozásokat is kiszűrik, és gyorsan reagálnak a csaló weboldalak betiltása érdekében.

Ha még olvasna erről:

http://hu.wikipedia.org/wiki/Adathal%C3%A1szat
http://www.antiphishing.org/
http://computerworld.hu/computerworld/valogatas-nelkul-tamadnak-a-vilag-legveszelyesebb-adathalaszai-20091030.html
http://www.infoter.eu/cikk/hitelkartya_adatok_megszerzesere_iranyulo_adathalasz_tamadasok_a_facebook-on

Veszélyek: fertőző honlapok

Miről beszélünk?

Jellemző hatása: Alacsony, Közepes, Magas

A veszélyes honlapok alatt olyan internetes oldalakat értünk, amelyeknek már akár a meglátogatása is veszélyezteti a számítógépünk biztonságát. A weboldalba ágyazott kártevő kód általában ismert rendszer sérülékenységeket kihasználva, kártevő programokat telepít a felhasználó gépére.

Mit veszélyeztet?

- Felhasználó: a fertőző honlapokon keresztül települő kártevő programok veszélyeztetik a személyes és érzékeny adatainkat, jelszavainkat, bankkártya adatainkat, internetbank adatainkat.
- Rendszerműködés: a rendszerek működését általában kevéssé befolyásolják, ezzel is elősegítve azt, hogy rejtve maradjanak.
- Információbiztonság: a fertőző honlapokon keresztül települő kémprogramok az információ bizalmasságának sérülése mellett a védelmi rendszerek egyéb módon való kijátszását is lehetővé teheti.
- Nemzetbiztonság: a kormányzati informatikai rendszerek többségében elérhető a munkatársak számára az Internet, még a biztonsági szoftverekkel védett rendszerekben is egy új kártevő eljuthat a felhasználó gépére a böngészőn keresztül és adatszivárgást segíthet elő.

Példa:

Az interneten több millió fertőző honlap található, a többségüket nem a készítőjük akarta fertőzővé tenni, hanem hekkerek törték fel, és telepítettek rá kártevő programokat. A kifejezetten kártevők terjesztésére létrehozott oldalak pedig úgy készülnek, hogy minél több ember figyelmét keltség fel, ilyenek lehetnek például a feltört programokat terjesztő oldalak, vagy a felnőtt tartalmat terjesztő oldalak.

Hogyan előzzük meg?

Első lépés az alapvető tudás megszerzése a számítógép és az internet működéséről, és kockázatairól.

Segíti a számítógépünk védelmét végpont védelem telepítése, és hasznos kiegészítő biztonsági funkció a böngészőkbe beépülő kiegészítő segédprogram (WoT[11]), amely a nem megbízható oldalak meglátogatása előtt figyelmeztetést jelenít meg. Lehetőségünk van még a weboldal tanúsítvány érvényességének ellenőrzése.

Az aktív tartalmak, mint például az Active-X, a Flash, vagy a Java nagy kockázatot hordoz a számos biztonsági sérülékenység miatt. Ezek gyakori frissítése, vagy letiltása növeli a biztonságot.

A szervezeteknél frissített hálózati tartalomszűrő rendszerek képesek biztosítani a meglátogatható weboldalak korlátozását. Ha a fertőző honlapot már észlelték korábban, és beépítették a tartalomszűrő szabályrendszerébe, akkor ez is képes megelőzni a fertőzést.

A weboldalakat működtető rendszereink frissítése és figyelemmel kísérése szintén szüksége.

Mit tegyünk, ha bekövetkezik?

Ha arra gyanakszunk, hogy weboldalon keresztül fertőzés érte a gépünket, frissítsük a védelmi szoftvereinket, majd kapcsoljuk ki a hálózatot és teljes keresést indítsunk el rajtuk.

Munkahelyünkön a vonatkozó szabályzatoknak megfelelő eljárásrendet kövessük! Általában ez központi hibabejelentőn való bejelentés megtételét jelenti.

Ha még olvasna erről:

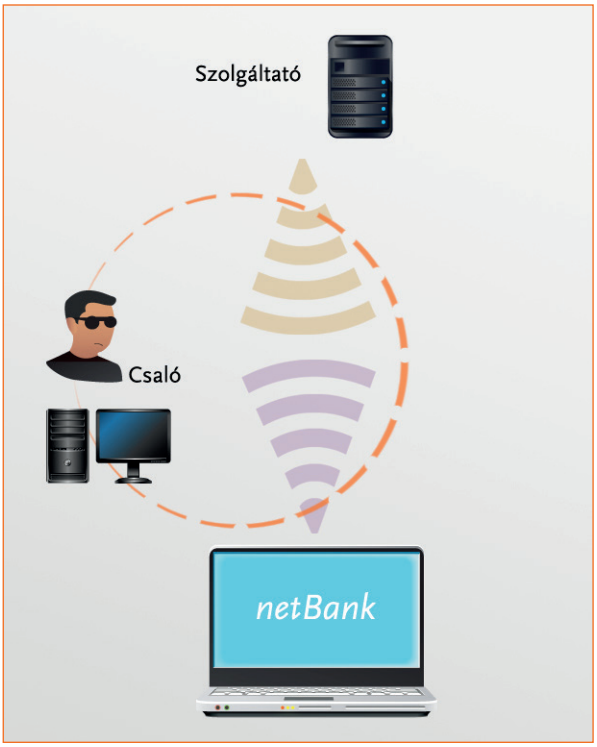
http://www.virusoshonlap.hu/
https://support.google.com/webmasters/answer/163635
http://www.technet.hu/hir/20111015/700_000_weboldalt_fertozott_meg_egy_uj_virus/
http://biztonsag.computerworld.hu/index.php/uj-vizekre-eveznek-a-virusterjesztok.html

[11] WoT: Web of trust – megbízhatósági hálózat. Olyan oldalak gyűjteménye, amelyet a felhasználók kártékonynak találtak.

Veszélyek: adatforgalom eltérítése (Man-in-the-middle)

Miről beszélünk?

Jellemző hatása: Alacsony, Közepes, Magas



Az adatforgalom eltérítésére irányuló, vagy közbeékelődéses támadások általában a felhasználó és a szolgáltató közötti kommunikációba beékelődő programokkal végzik, amely segítségével a belépett felhasználók adatforgalmát szerzik meg, és módosítják, így nem szükséges a jelszó ismerete a csaló által küldött parancsok futtatására.

A sikeres támadáshoz a támadónak hozzá kell férnie a kommunikációs csatornához, képesnek kell lennie elkapnia a rajta küldött információt és meg kell akadályoznia, hogy eljussanak a valódi címzetthez.

Mit veszélyeztet?

- Felhasználó: általában értékes célpontokra fejlesztenek ki ilyen támadást, ezért a felhasználókat leginkább nemzetközi internet bank szolgáltatások használata során veszélyeztetheti.
- Rendszerműködés: a felhasználók számítógépén a támadott szolgáltatás működését módosítja az adatforgalom eltérítéssel járó támadás.
- Információbiztonság: a támadott szolgáltatáson keresztül küldött üzentek bizalmassága és sértetlensége sérül.
- Nemzetbiztonság: közszférában használt rendszerek célzott támadása esetén kockázatot jelent.

Példa:

A csalók egy internetbanki közbeékelődéses támadásnál egy kártevő program segítségével a felhasználó számára internetbanknak látszanak, a bank számára pedig felhasználónak. Volt példa olyan visszaélésre, ahol a felhasználó által elutalt 10 EUR helyett a kártevő 1000 EUR-t utalt el saját magának, és az internetbank bankszámlakivonatán 10 EUR-t jelenített meg az eredeti címzetthez való utalásként, amikor a felhasználó lekérdezte az internetbank felületén a kérdéses tranzakciót. A csalásra akkor derül fény, ha a felhasználó a hagyományos bankkivonatot a kezébe veszi, vagy fedezethiány miatt a bankkártyája használhatatlanná válik.

Hogyan előzzük meg?

Végpont védelem telepítése segíti a számítógépünk védelmét. Lehetőségünk van a weboldal tanúsítványok érvényességének ellenőrzésére is. Fontos, hogy fokozott biztonságot igénylő tevékenységeket megbízható számítógépen és helyszínen végezzünk, így az internetkávézó nem ajánlott banki tranzakciók végzésére, de például egy bevásárlóközpontban talált „ingyen" WiFi kapcsolat még a saját számítógépünkről sem tekinthető biztonságosnak.

Mit tegyünk, ha bekövetkezik?

Ha arra gyanakszunk, hogy eltérítik az adatforgalmunkat, akkor egy másik számítógépen, amely más hálózaton csatlakozik a szolgáltatáshoz, próbáljuk ki a feltételezhetően támadott szolgáltatást (például munkahelyi számítógép, táblagép mobil internettel). Ha eltérő eredményt kapunk ugyanarra a kérésre, akkor akár ilyen támadás áldozata is lehetünk.

Munkahelyünkön a vonatkozó szabályzatnak megfelelő eljárásrendet kövessük! Általában ez központi hibabejelentőn való bejelentés megtételét jelenti.

Ha még olvasna erről:

https://en.wikipedia.org/wiki/Man-in-the-middle_attack
http://hu.wikipedia.org/wiki/K%C3%B6zbe%C3%A9kel%C5%91d%C3%A9ses_t%C3%A1mad%C3%A1s
http://computerworld.hu/computerworld/felelotlenul-kattintunk-mindenre-20090804.html

Fizikai visszaélések

AZ INFORMÁCIÓBIZTONSÁGOT FENYEGETŐ FIZIKAI HOZZÁFÉRÉST IGÉNYLŐ VISSZAÉLÉSEK

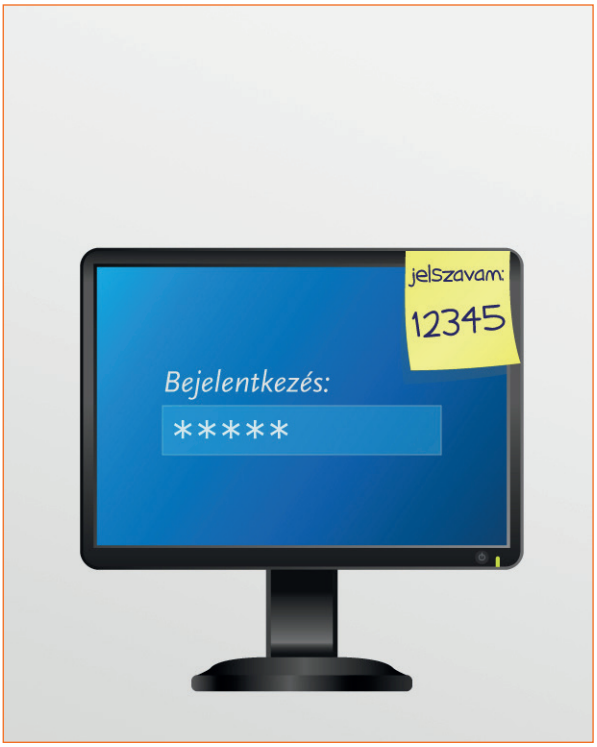
Számos olyan módszer ismert, amely segítségével a támadó adatokat szerezhet meg az információs rendszerekből anélkül, hogy magát az információs rendszert számítástechnikai eszközökkel támadná. Általában gyorsabb, olcsóbb az embereket megtéveszteni, vagy megvesztegetni, mint az informatikai rendszerekbe betörni!

A következőkben néhány jellemző, emberi hibára és megtévesztésre irányuló veszélyt ismertetünk.

Veszélyek: jelszavak ellesése (observing passwords attack)

Miről beszélünk?

Jellemző hatása: Alacsony, Közepes, Magas



Jelszavak ellesése alatt információs rendszerekhez való felhasználói hozzáférések olyan jogosulatlan megszerzését értjük, amikor nem a jelszavak feltörésével szerzik meg azt, hanem például egy másik személy a jelszó beírását közvetlenül, vagy kamera rendszeren keresztül látja. Hasonló eredmény érhető el, ha egy felhasználó számítógépére olyan szoftver telepít valaki, ami a felhasználó minden billentyűzet leütését rögzíti és továbbítja a telepítő személy felé.

Mit veszélyeztet?

- Felhasználó: személyes és érzékeny adatok nyilvánosságra kerülése, jó hírnév sérülése, és anyagi kár is lehet a következmény attól függően, mely rendszer jelszavát szerzi meg a támadó.
- Rendszerműködés: amennyiben kiemelt felhasználók jelszavát szerzi meg a támadó, jelentős kárt okozhat a rendszer adatainak törlésével, ellopásával, a működés akadályozásával, vagy felfüggesztésével.
- Információbiztonság: sérül az információ bizalmassága, ha az jogosulatlanul más tulajdonába vagy nyilvánosságra kerül.
- Nemzetbiztonság: kormányzati és egyéb minősített adatokhoz való hozzáférést is megkönnyítheti a jelszavak megszerzése.

Példa:

Egy okmányirodában az egyik munkatárs jelszavát ellesve követett el egy megtévedt kollega okirat hamisítást, ezáltal leplezve a tevékenysége nyomait. Az elkövetőt rögzítette az épületben levő biztonsági kamera, ennek köszönhetően a vizsgálat eredményeképpen felmentették az visszaéléshez használt felhasználónév tulajdonosát.

Hogyan előzzük meg?

Közigazgatási informatikai szolgáltatást csak olyan számítógépen engedélyezett használni , amelynek alapvető biztonságáról (frissített szoftverek, vírusvédelem, tűzfal) meggyőződtünk. Lehetőség szerint a jelszavunkat akkor írjuk be, amikor nincs körülöttünk olyan személy, aki rálát a billentyűzetünkre közvetlenül, vagy akár ablakon, tükrön keresztül, és nem is rögzíti kamera a helyiségben zajló tevékenységeket.

A rendszereket is biztonságosabbá tehetjük, adott esetben jelszó helyett biztonsági kódgeneráló eszköz által adott időszakos kód segítségével, így az ellesett jelszóval nem lesz képes a támadó a rendszerbe belépni.

A jelszavainkat – ha szükséges – biztonságos helyre jegyezzük fel, ne a tárcánkban hordjuk! Elérhetők olyan ingyenes, titkosított, jelszó széfprogramok, amelyeket USB memórián magunkkal vihetünk. A legtöbb intézményben a felhasználók nem jogosultak ilyen programok használatára és telepítésére, de célszerű a biztonsági terület által is megfelelőnek ítélt széfprogramok engedélyeztetése.

A böngészőkkel való jelszó megjegyeztetés biztonsági szempontból szintén nem ajánlott, mert ha a számítógép belépési jelszavát illetéktelen személy megszerzi, a böngésző segítségével hozzáférhet több, általunk használt szolgáltatáshoz is.

Mit tegyünk, ha bekövetkezik?

Azonnal változtassuk meg a jelszavunkat, és jelentsük a szervezet biztonsági vezetőjének, hogy gyanúnk szerint hozzáfért valaki a felhasználói fiókunkhoz.

További teendőkről a szervezet belső szabályzatai rendelkeznek, minden esetben az ebben foglaltak szerint kell eljárni!

Ha még olvasna erről:

http://en.wikipedia.org/wiki/Shoulder_surfing_(computer_security)
http://en.wikipedia.org/wiki/One-time_password
http://buhera.blog.hu/2009/06/28/mutasd_a_jelszavad
http://tesztelesagyakorlatban.testing.hu/keres_cikk.php?mit=7

Veszélyek: megtévesztésen alapuló csalások (Social engineering)

Miről beszélünk?

Jellemző hatása: Alacsony, Közepes, Magas

A bűnözők olyan pszichológiai manipulációs módszereket használnak, amellyel ráveszik a felhasználókat védett adataik, felhasználóneveik, akár jelszavaik elmondására. Általában ráijesztés módszerét használják, vagy azt használják ki, hogy ösztönösen segíteni akarunk másoknak.

Klasszikus esete, hogy az illetéktelen személy valamilyen legitim indokkal bejut a létesítményekbe , és ott információkat gyűjt. Gyakori módszer erre az információs rendszerekbe való belépést lehetővé tevő azonosítók, jelszavak telefonon keresztül történő megszerzése változatos, kitalált történetekkel.

Másik technikája az adathalászat (phising) hamisított elektronikus levelek küldésével tévesztik meg a célpontot. A komolyabb támadásoknál akár egyénre szabott megtévesztő levelek is előfordulnak.

Mit veszélyeztet?

- Felhasználó: az azonosítók és jelszavak kiadása különféle következménnyel járhat, a személyes adataink megszerzésétől kezdve, a hivatali rendszerekből való adatlopáson keresztül a szándékos károkozásig.
- Rendszerműködés: illetéktelen személyek egy megfelelő jogosultsággal rendelkező felhasználó nevének és jelszavának segítségével hozzáférhetnek rendszerek üzemeltetési funkcióihoz, megváltoztathatnak paramétereket, a rendszereket lassíthatják, leállíthatják.
- Információbiztonság: a támadók a megszerzett felhasználói azonosítókat és jelszavakat szinte mindig adatok megszerzése, illetve egyéb előnyszerzés céljából használják fel.
- Nemzetbiztonság: a közszféra által használt rendszerek azonosítóinak és jelszavainak megszerzésével védett információk szerezhetőek meg.

Példa:

Azok a telefonos megkeresések – lehetnek akár banálisan egyszerűek, vagy vad kitalációk –, amelyek arra irányulnak, hogy valamilyen személyes adatot, vagy számítógépes rendszerbe való belépéshez

szükséges adatot próbáljanak tőlünk megszerezni, szinte mindig ártó szándékkal történnek.

Volt példa olyan célzott adathalász támadásra, amikor a külügyminisztériumi dolgozó kifejezetten egy, a szakterületéhez tartozó, legitimnek tűnő helyről származó elektronikus levelet kapott, csatolt rendezvény meghívóval. Maga a dokumentum olyan fertőző kódrészletet tartalmazott, amely a hivatal rendszerének távoli jogosulatlan elérését tette volna lehetővé.

Hogyan előzzük meg?

Több módszere van annak, hogy csalás áldozatává váljunk. A megelőzés a biztonságtudatosság javítására épül:

- Egy nem várt, gyanús üzenetben levő hivatkozásra ne kattintson rá. Például ha azt írja a levél, hogy visszaküldik javításra a kulcsos gépkocsi igénylőlapját, és nem is igényelt kulcsos gépkocsit, akkor ne nyissa meg a csatolmányt, vagy a beszúrt hivatkozást. Törölje az üzenetet.
- Legyen gyanús, ha úgy nyert internetes lottón, hogy nem is játszott rajta, ez is csalásra utal.
- Ha gyanúsnak tűnik egy weboldal, akkor valamelyik keresőprogramban keressünk rá az oldal címét tartalmazó találatokra, hogy megtudjuk, mit gondolnak róla mások, tényleg legitim weboldal-e.
- Mielőtt egy levélben, vagy dokumentumban feltűntetett hivatkozásra rákattintana, húzza fölé az egeret, és ellenőrizze, hogy a felugró ablakban megjelenő cím egyezik-e a hivatkozás címével.
- Ha indokolatlanul személyes vagy érzékeny adatokat kérnek öntől elektronikus levélben, akkor ne adja meg azokat.
- Gyakran a csaló weboldalak felugró ablakainak álcázott kártevők kérnek be információkat rólunk. A rendes oldalak nem használják ezt a módszert. Ne adjunk meg felugró ablakban érzékeny adatokat.

Mit tegyünk, ha bekövetkezik?

Minél hamarabb csökkentsük a lehetséges károkat. Jelentsük az illetékes vezetőnek, ha a szervezeti munkával összefüggésben történt a megtévesztés.

Ha ismeretlen emberrel találkozunk a munkahelyünkön, kíséret nélkül, kérdezzük meg, hogy segíthetünk-e neki, és ha gyanús, akkor a biztonsági területet haladéktalanul értesítsük.

Ha még olvasna erről:

http://hu.wikipedia.org/wiki/Pszichol%C3%B3giai_manipul%C3%A1ci%C3%B3_(informatika)
http://en.wikipedia.org/wiki/Red_October_(malware)
http://www.biztonsagosinternet.hu/tippek/a-social-engineering-rol

Veszélyek: IT személyiséglopás (megszemélyesítés eltulajdonítása információs rendszerekben)

Miről beszélünk?

Jellemző hatása: Alacsony, Közepes, Magas

Általunk létrehozott felhasználók és felhasználói profilok megszerzése, vagy a nevünkben más által létrehozott felhasználói profil kialakítása információs rendszerekben.

Mit veszélyeztet?

- Felhasználó: személyes adatainkat, jó hírnevünket, és vagyonunkat is veszélyeztetheti, ha ellopják a felhasználói azonosítónkat. Rejtett titkainkat megismerhetik, a nevünkben tevékenykedhetnek.
- Rendszerműködés: a rendszerműködésre akkor lehet hatással, ha a személyiséglopást követően a megszerzett felhasználói jogosultságokkal befolyásolják a rendszer működését, például kéretlen leveleket küldenek, vagy kártevő programot telepítenek a nevünkben.
- Információbiztonság: személyes, üzleti és kormányzati adatok kiszivárgásához vezethet.
- Nemzetbiztonság: felhasználói profilok megszerzésével hozzájuthatnak szolgáltatások jelszavaihoz, ami a kormányzati informatikai rendszerekben használt jelszavak feltöréséhez vezethet.

Példa:

Városi legenda, hogy régebben tiltották a nemzetbiztonsági szolgálatok munkatársai számára, hogy közösségi hálózatokon regisztráljanak saját nevükben. A szolgáltatások rohamos terjedése (pl. iwiw) viszont azt eredményezte, hogy nagyobb kockázat volt egy idő után, ha a kollégák nem regisztráltak, mert már szinte csak ők nem voltak a közösségi oldalakon jelen, így bizonyos feltételekkel engedélyezték számukra.

Távol-keleti hírszerzők a NATO több tisztje nevében létrehozott Facebook profilok segítségével szereztek néhány évvel ezelőtt információkat más NATO alkalmazottakról. De hazai politikusok is estek áldozatul annak, hogy a nevükben hoztak létre profilt a közösségi oldalakon.

A személyes adatok segítségével például Angliában gyakran hitelt, vagy hitelkártyát igényelnek más nevében, majd nem törlesztik azokat. Ezzel anyagi kárt okozhatnak, és az illető hitelképességét is ronthatják.

Hogyan előzzük meg?

A profilunk jelszavának megszerzését úgy előzhetjük meg, hogy hosszú és összetett jelszavakat használunk, rendszeresen változtatjuk azokat, és olyan számítógépen,ami feltehetően nem biztonságos,nem gépeljük be a jelszót. Azt hogy más nyisson a nevünkben felhasználói fiókot, nehéz megelőzni, de segíthet, ha az ismertebb szolgáltatásokon létrehozzuk saját profilunkat, még ha nem is használjuk rendszeresen, hiszen ez esetben még egy profil a nevünkben nem nyitható. Tipikusan ismertebb személyiségek, vezetők számára javasolt, hogy hozzanak létre profilt a közösségi hálózatokon, nehogy a nevükben más tegye meg.

Mit tegyünk, ha bekövetkezik?

Keressük meg a szolgáltatót, és ha nem ad választ a megkeresésünkre, forduljunk szakértő jogászhoz, illetve komolyabb esetekben javasolt feljelentést tenni a rendőrségen.

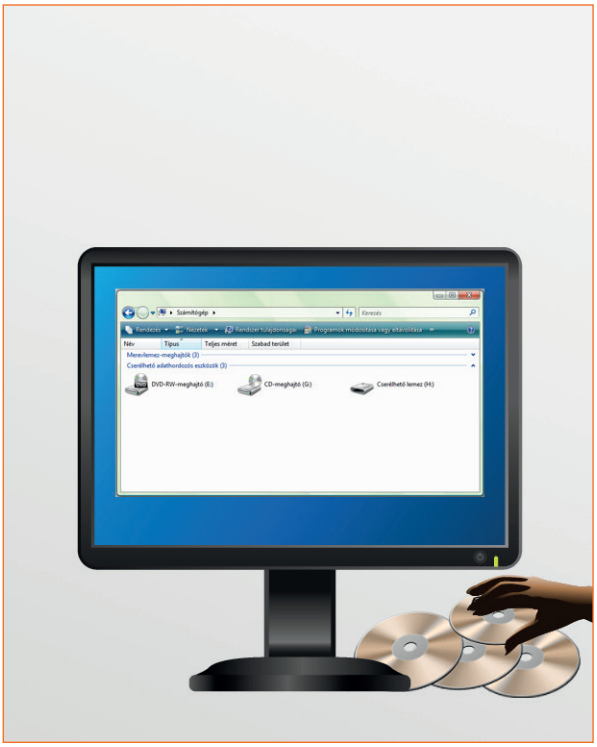
Ha még olvasna erről:

http://en.wikipedia.org/wiki/Identity_theft
http://www.technet.hu/hir/20091104/szemelyiseglopas_-_mi_az/
http://www.biztonsagosinternet.hu/tippek/a-szemelyazonossag-lopasrol

Veszélyek: eszközök és adathordozók eltulajdonítása

Miről beszélünk?

Jellemző hatása: Alacsony, Közepes, Magas



Abban az esetben, ha egy szervezetnél a fizikai biztonság nem megfelelő, vagy a felhasználók nem vigyáznak értéktárgyaikra, előfordulhat a számítógépes eszközök és adathordozók – gyakran hordozható eszközök – eltulajdonítása.

Mit veszélyeztet?

- Felhasználó: a számítógépes eszközünk, és az adathordozónk értéktárgy, ellopásuk vagyoni kárt okoz, de a rajta levő adatok elvesztése gyakran nagyobb veszteséget okoz.
- Rendszerműködés: a szervetek által használt számítógépek, vagy egyéb eszközök eltulajdonítása akadályozhatja a rendszerek működését.
- Információbiztonság: az eltulajdonított eszközökön, és adathordozókon általában az értékük többszörösét érő adatok találhatóak, amelyek, ha nem titkosítva tárolják őket, visszaélésekre buzdítják a tolvajt.
- Nemzetbiztonság: a közszféra által használt adatokat tartalmazó eszköz, vagy adathordozó eltulajdonítása nemzetbiztonsági következménnyel is járhat.

Példa:

2008-ban titkosítás nélküli lemezek tűntek el a HSBC Banktól, amelyeken 370.000 ügyfél életbiztosításának adatai szerepeltek.

Évente néhányszor a közszférában is elő fordul, hogy egy munkatárs elhagyja a telefonját, vagy ellopnak egy laptopot. Nem jellemző, hogy nyilvánosságra kerülnek a tárolt adatok, vagy, hogy azok megfelelően voltak-e védve, de a nemzetközi tapasztalatok alapján megvan az esélye az adatvesztésnek.

Hogyan előzzük meg?

Az ellopott adathordozókon keresztüli adatvesztést az adatok, illetve az adathordozók titkosításával előzhetjük meg. Ne tároljunk szükségtelenül adatokat hordozható eszközökön.

Mit tegyünk, ha bekövetkezik?

Az adatvesztést haladéktalanul jelentsük a belső szabályozásnak megfelelően, hogy a biztonsági terület időben megtehesse a szükséges lépéseket. Gyakran nagyobb probléma keletkezik abból, ha egy adathordozót elvesztettünk, és nem jelentjük be, mert a biztonsági elhárító lépések nem tehetők meg időben, és a bejelentés elmulasztása miatt is számon kérnek minket.

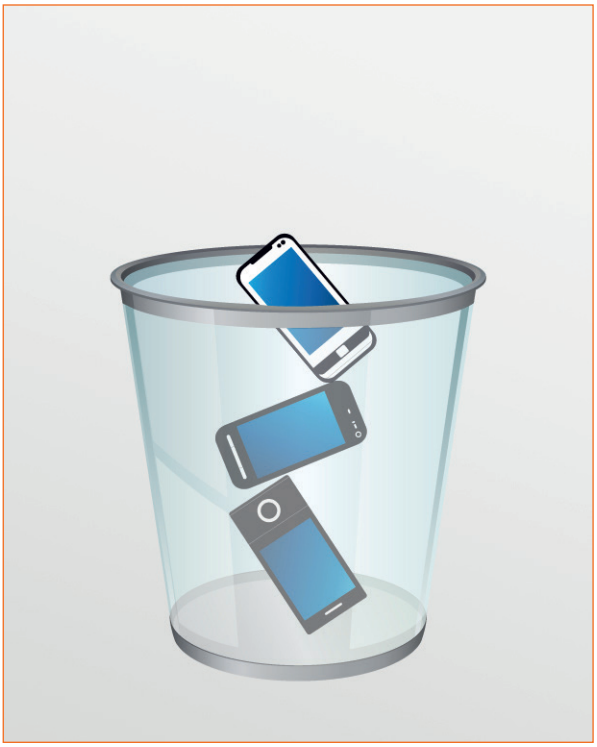
Ha még olvasna erről:

http://en.wikipedia.org/wiki/Data_theft
http://biztonsag.computerworld.hu/index.php/adatlopasok-nem-eleg-aggodni-vedekezni-is-kell-20120621.html
http://mysec.hu/magazin/uezleti-vilag/283-rengeteg-laptopnak-vesz-nyoma

Veszélyek: eszközök selejtezése, kidobása

Miről beszélünk?

Jellemző hatása: Alacsony, Közepes, Magas



Az otthoni felhasználók, a szervezetek által használt számítógépek és kiegészítő eszközök (pl. külső adathordozók), illetve más számítógépes adatokat tartalmazó eszközök (pl. multifunkciós nyomtatók, telefonok) néhány év alatt használaton kívül kerülnek. Ezeket általában raktározzák még egy ideig , de selejtezést követően legtöbbször szemétként végzik. Az eszközöktől való megszabadulás előtt végre kell hajtani az adatok végleges törlését. Ennek hiányában az eszközről megszerzett adatok felhasználása vagy nyilvánosságra hozatala jelentős károkat okozhat a szervezet számára.

Mit veszélyeztet?

- Felhasználó: különösen a gyorsan elavuló mobiltelefonok selejtezésekor célszerű körültekintően eljárni a készüléken tárolt telefonszámok, képek, és üzenetek védelme érdekében.
- Rendszerműködés: egy rendszer felújítása, vagy bővítése miatt feleslegessé váló eszköz, vagy adathordozó olyan információkat tartalmazhat a rendszer felépítéséről és biztonságáról, amely megkönnyítheti a még működő rendszerelemek támadását.
- Információbiztonság: a selejtezett adathordozókon tárolt, vagy egyszerű törléssel is letörölt adatok visszaállíthatóak, az értékes információk pedig megtalálják azokat, akik fizetnének értük.
- Nemzetbiztonság: minősített adatokat tároló hordozók selejtezése során nem engedhető meg, hogy visszaállítható legyen róluk az adat. Ezért minden selejtezés magas kockázatot jelent.

Példa:

A felhasználók 1-2 évente cserélik telefonjaikat, a használt készülékeket sokszor értékesítik. Ritka, hogy a felhasználó képes személyes adatainak visszaállíthatatlan módon valótörlésére. Ugyanez egy szervezet esetén nagyobb kárt is okozhat az eszközön tárolt telefonszámok, elektronikus levelek, és bizalmas üzenetek nyilvánosságra kerülésének kockázata miatt.

IT biztonsággal foglalkozó cégek a kiselejtezett számítógépeken többször végeztek teszteket a visszaállítható adatokról. Gyakran bizalmas vállalati adatokat találtak.

Több százezer gépet importálnak a fejlett országokból csak Nigériába, a számítógépek gyártási anyagainak újrahasznosítása érdekében. A bűnözők számára azonban a gépek műanyag burkolatánál, vagy a benne levő nemesfémeknél értékesebb lehet a merevlemezekről visszaállítható adat.

Hogyan előzzük meg?

Az eszközök selejtezése előtt visszaállíthatatlanul töröljünk minden adatot, vagy ha ez nem lehetséges, fizikailag semmisítsük meg az adathordozókat.

Mit tegyünk, ha bekövetkezik?

A selejtezett adathordozókon kikerülő adatok arra hívják fel a figyelmet, hogy a szervezet belső kontroll rendszere nem megfelelő. Ha ilyen bekövetkezik, akkor vizsgáljuk felül a vonatkozó szabályzatokat, legyen következménye a szabályok be nem tartásának, és biztosítsuk a technológiát az adatok megfelelő törléséhez.

Ha még olvasna erről:

http://biztonsagportal.hu/elajandekozott-adatok-nem-torodunk-az-adattorlessel.html
http://mysec.hu/magazin/kiemelt-hirek/327-elhanyagolta-az-adattoerlest-a-nasa
http://www.uzletihirszerzes.hu/%C3%BCzleti-biztons%C3%A1g/inform%C3%A1ci%C3%B3--%C3%A9s-adatv%C3%A9delem/2705-bizalmas-informcik-a-lecserlt-mobil-minden-titkot-kiad.html

Veszélyek: szemétbe dobott információ (kukabúvárkodás)

Miről beszélünk?

Jellemző hatása: Alacsony, Közepes, Magas

A jogosulatlan információszerzés egyik legrégebbi módszere a szemét átvizsgálása; a fellelt iratok, számítógépes adathordozók temérdek információval szolgálhatnak a kukabúvárnak.

Mit veszélyeztet?

- Felhasználó: az egyének felelősek a rájuk bízott információk kezeléséért. Egy tévesen kinyomtatott irat kidobása az első kukába ugyan csökkentheti a frusztrációnkat, ám így a kollegáktól kezdve a szervezetbe látogató vendégeken és a takarítókon keresztül, a szemétben kotorászók, a szemetesek, és a szándékos hírszerzők is hozzáférhetnek.
- Rendszerműködés: a rendszerek működését akkor képes veszélyeztetni, ha a kidobott információ segítségével a rendszerhez való hozzáférés lehetővé válik, vagy a jelszavak feltörhetővé válnak. ilyenkor a jogosulatlan hozzáféréshez hasonló veszélyek történhetnek meg.
- Információbiztonság: maga a kidobott adathordozón levő információ, és a fellelt információk összessége olyan eszközt biztosít, amely az adott információn túlmenő következtetések levonására alkalmas, illetve jogosulatlan információszerzést tesz lehetővé.
- Nemzetbiztonság: a szemétbe dobott információ jellegétől és mennyiségétől függően idegen országok hírszerzői számára is értékes lehet egy állami szervezet szemete.

Példa:

Feleslegesség vált munkaverziók és szükségtelenül nyomtatott másolati példányok darálás nélküli kidobása értékes információ lehet, adott esetben egy munkaanyagban szereplő megjegyzések többlet információt is tartalmazhatnak. A papír fecnire, pizzás dobozra írt üzenetek, jegyzetek, telefonszámok szintén értékes információt jelenthetnek.

Az informatikai rendszerekre vonatkozóan árulhat el információt az eszközök dobozainak kidobása, amely dobozok általában pontosan tartalmazzák az eszköz konfigurációját is.

Hogyan előzzük meg?

A szervezet méretének megfelelő számú és kapacitású iratmegsemmisítő gépet vásároljunk, vagy biztonságos módon gyűjtsük külön az irodai selejtet, és központi darálón, vagy külső szolgáltató segítségével biztonságos módon semmisítsük meg.

Fontos, hogy a biztonságtudatosítási képzés kitérjen az iratok és egyéb adathordozók szakszerű selejtezésére, megsemmisítésére. Legelterjedtebb módszer a papírok feldarabolása, a mágneses és optikai adathordozók fizikai megsemmisítése például iratmegsemmisítőben.

Az adathordozók, fénymásoló gépek, számítógépek és egyéb eszközök selejtezése során szintén az adatok visszaállíthatatlan törlését szükséges elvégezni.

Jó gyakorlat életszerű példák felhasználása a belső képzések során. Kis munkabefektetéssel a szervezet egynapi irodai szemetének összegyűjtésével és kiértékelésével olyan életszerű példához juthatunk, amely hosszú ideig szóbeszéd tárgya lehet, és segítheti a biztonságtudatos magatartás szokássá erősödését a munkatársakban.

Mit tegyünk, ha bekövetkezik?

Biztonsági események észlelése, vagy annak gyanúja esetén értesítsük a biztonsági szakterületet!

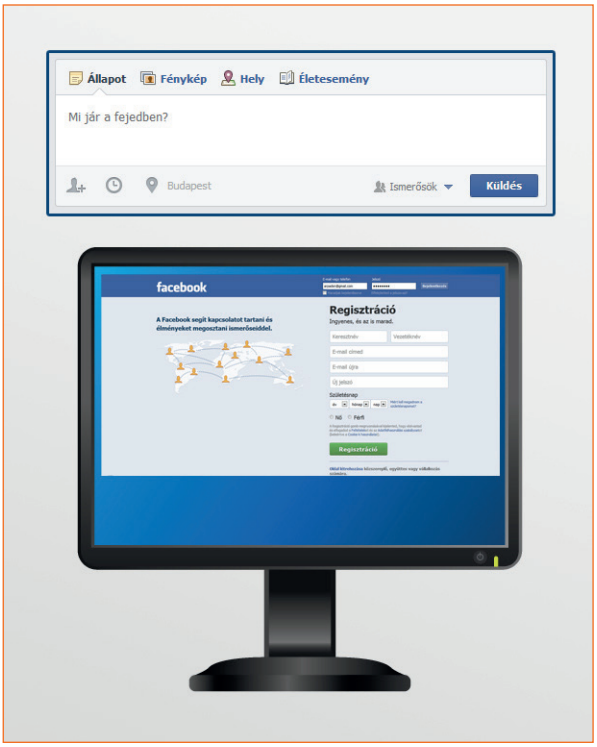
Ha még olvasna erről:

http://en.wikipedia.org/wiki/Dumpster_diving
http://www.nethirlap.hu/printme.php?cikk=13267
http://www.uzletihirszerzes.hu/uzleti-hirszerzes/5262-hogyan-dolgoznak-az-ipari-kmek.html

Veszélyek: személyes / hivatali adatok megosztása közösségi hálózatokon

Miről beszélünk?

Jellemző hatása: Alacsony, Közepes, Magas



Szándékosan, vagy véletlenül olyan adatokat oszthatunk meg az interneten magunkról, amelyek magukban, vagy összességében veszélyt jelenthetnek ránk, vagy a munkáltatónkra. Adott esetben az is ilyen információ lehet, hogy ha jelöljük, hogy éppen hol tartózkodunk (pl. 4square), vagy feltérképezhető a kapcsolati rendszerünk. Vigyázni kell az olyan közösségi oldalakkal, amelyen üzenőfalunkon üzenet közvetíthető.

Mit veszélyeztet?

- Felhasználó: személyes adatok megosztása vagyoni kárt okozhat, vagy egyéb módon sodorhat veszélybe minket.
- Rendszerműködés: a rendszerek biztonságát veszélyeztethetik a bűnözők a közösségi hálózatokon összegyűjtött információk segítségével.
- Információbiztonság: a közösségi hálón való közzététel sérti az információ bizalmasságát.
- Nemzetbiztonság: hivatali, vagy katonai információk közzététele veszélyeztetheti a nemzetbiztonságot.

Példa:

Ha közzétesszük magunkról, hogy milyen értékes ajándékokat kaptunk karácsonyra, a személyes adatainkból kiderül a lakcímünk, ezt követően megosztjuk, hogy hová megyünk 10 napra síelni, és még be is jelentkezünk a sípályáról, akkor a betörők biztosak lehetnek abban, hogy szinte védtelenül várja őket a lakásunk. Megtörtént eset volt itthon is a közlékeny felhasználó lakásának „elköltöztetése". A szomszédok furcsállták, hogy a lakó nem szólt előre, de itthon általában nincsenek ilyen jó viszonyban egymással a szomszédok.

A brit hadügyminisztérium online kampányban hívja fel a katonák figyelmét arra, hogy ne osszanak meg harctéri információkat a közösségi hálózatokon, ne tegyenek közzé videókat, és nyilvános helyen ne beszéljenek harctéri tevékenységről, mert a terroristák brit földön is támadhatják őket, illetve a kifecsegett információ a harctéren szolgálatot teljesítő bajtársaikat sodorhatja veszélybe.

Hogyan előzzük meg?

Az információ megosztása során legyünk tudatosak , ami veszélyt jelenthet ránk, vagy környezetünkben bárkire, ne tegyük közzé. Lehetőség szerint olyanokkal tartsunk kapcsolatot közösségi hálózatokon, akiket jól ismerünk, a programok biztonsági beállításait pedig tudatosan végezzük. Az információ hasznos lehet, ha csak a célközönséggel osztjuk meg, de veszélyt jelenthet, ha bárki számára elérhetővé tesszük.

Mit tegyünk, ha bekövetkezik?

Ha veszélyt észlelünk, akkor mielőbb töröljük az üzenetet, információt, képet, vagy akár a profilunkat, majd értesítsük a biztonsági területet, hogy a szükséges intézkedéseket megtehessék. Értesítsük azokat is, akiket veszélyeztethet az információ nyilvánosságra hozatala.

Ha még olvasna erről:

https://en.wikipedia.org/wiki/Privacy_concerns_with_social_networking_services
http://www.biztonsagosinternet.hu/tippek/adatbiztonsag-kozossegi-oldalakon
http://www.infoter.eu/cikk/veszelyes_jatszoter_a_kozossegi_oldal

Biztonságos irodai alkalmazások

IRODAI ALKALMAZÁSOK BIZTONSÁGTUDATOS HASZNÁLATA

Az irodai IT kockázatok csökkentésének leghatékonyabb módszere a megelőzés. Minden felhasználói csoportnak fontos ismernie, hogyan védje az információt, és hogy hol kerülhetnek ki érzékeny adatok egy irodai munkakörnyezetben. A külső eredetű veszélyekre korábbi fejezetekben részletesen felhívtuk a figyelmet, most azok közül a veszélyek közül mutatjuk be a legfontosabbakat, amelyekkel az elterjedt irodai alkalmazások használata során akár tudtunk nélkül személyes adatot, vagy más védendő információt tehetünk közzé. Ezek az alkalmazás funkciók kikapcsolhatóak, illetve tudatos használatukkal csak a jóváhagyott információ kerülhet nyilvánosságra.

Az irodában dolgozó munkatársaknak ismerniük kell az általuk használt irodai szoftvercsomagok működését, a napi munkában jól kihasználható funkciókat. Jelen kiadványnak nem célja a funkciók ismertetése, de néhány, nem feltétlenül közismert adatbiztonsági és adatvédelmi funkcióra fel kívánjuk hívni a figyelmet a következő oldalakon.

Az alábbi tematikus oldalakon képernyőképekkel illusztrálva mutatjuk be a jó gyakorlatokat, amelyek alapvető számítógépes ismeretekkel is alkalmazhatók.

A példák többsége a Microsoft Office 2010 változata alapján készült. Ezek a funkciók általában más változatokban is elérhetőek, bátorítjuk az olvasót, hogy a gyártó oldalán keresse meg a pontos beállításokat, ha szüksége van rá. A Word alkalmazásra vonatkozó információkat például itt találja: http://office.microsoft.com/hu-hu/word-help/.

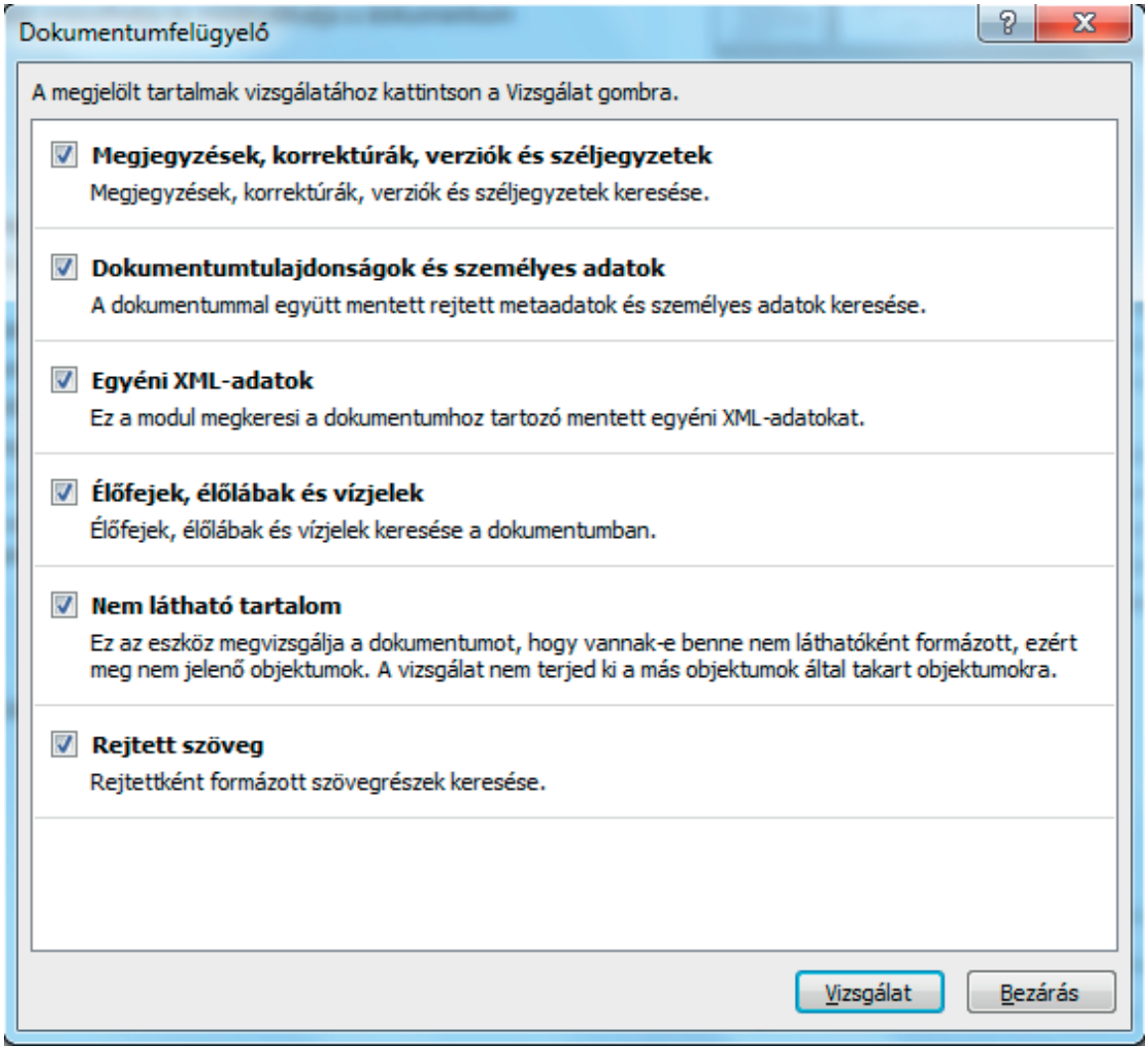
A személyes adatok törlése a dokumentumokból

Az irodai rendszerek, mint például a Microsoft Office, magukban a dokumentumokban tárolnak olyan adatokat, amelyek alapján beazonosítható, hogy melyik gépen készült, és ki készítette. Ha ezt valamiért nem szeretnénk, például meg szeretnénk osztani egy dokumentum elektronikus másolatát a munkatársainkkal, vagy ügyfelekkel, akkor ellenőrizni kell, hogy a dokumentum nem tartalmaz-e rejtett adatokat, személyes információkat (például a dokumentumtulajdonságok fülön). A rejtett

információk, a szervezetre vagy dokumentumra vonatkozóan olyan adatokat tehetnek nyilvánossá, amelyek kárt okozhatnak. Például egy munkaanyag megjegyzései nem tartozik a nyilvánosságra, vagy egy szervezet nevében készült dokumentumról sem feltétlen kívánják közzétenni, hogy ki készítette, ezért ajánlatos ezeket az adatokat eltávolítani.

A Word alkalmazás Dokumentumfelügyelő szolgáltatásával megtalálhatók és eltávolíthatók a dokumentumokban elrejtett információk. A funkció a Fájl menü, Információ menüpont, Problémák ellenőrzése gomb, Dokumentum vizsgálata ikonnal hívható elő:

A Dokumentumfelügyelő ablakban hat különböző helyen tárolt személyes adatok azonosítására és törlésére van lehetőség, az adatokat törölhetjük mindenhonnan, vagy szelektáltan. Nem célszerű minden törlési lehetőséget gondolkodás nélkül alkalmazni. Általában a végleges anyagban a korrektúrákra és megjegyzésekre nincs szükség, de a fejlécekre és láblécekre igen.



Végül ne felejtsük el azt sem, hogy maga a dokumentum fájl neve is hordoz információkat. Ott is szerepelhet a szerző, vagy a szervezet neve, készítés dátuma. Javasoljuk, hogy a közzétételre készített dokumentumok fájl nevét is úgy válasszák meg, hogy segítse a fájl könnyű azonosítását. Például a szervezet rövidítése, a dokumentum rövid címe, verziószáma, és a közzététel dátuma. Lehetőleg nem használva ékezetes és speciális karaktereket. Jelen kiadvány esetében ez például lehet: 'KIFU _biztonsagtudatositas_v1_2013.pdf'.

Ha még olvasna erről:

http://office.microsoft.com/hu-hu/word-help/rejtett-adatok-es-szemelyes-informaciok-eltavolitasa-a-dokumentumokbol-HA010354329.aspx

A dokumentumok jelszavas védelme

Az Office dokumentumok beépített jelszavas dokumentum védelme, különösen az Office XP előtti változatoké, ma már alacsony szintű védelmet jelent, még akkor is, ha a gyártó oldalán jelenleg is az szerepel, hogy adataink elérése lehetetlenné válik, ha a jelszót elfelejtjük.

Jó gyakorlat azonban a fájlokhoz rendelt jelszavak biztonságos helyen való tárolása. Sok bosszúságtól megkímélhet minket a jövőben, ha készítünk úgynevezett jelszó széfet. Az interneten többféle ingyenes alkalmazás is elérhető erre a célra, amelyek erős titkosítás mellett tárolják el a jelszavainkat. Itt lényegében elég a jelszó széfet elindító jelszót megjegyeznünk, a további jelszavak a széfből kinyerhetőek.

Bár az Office alapértelmezett titkosítási algoritmusai viszonylagosan erősek, a mai számítási kapacitás, és fejlett kódfejtő eljárások segítségével lehetségessé vált az Office 2003 és korábbi változataival létrehozott fájlok tartalmának megismerése, függetlenül a jelszó hosszától és bonyolultságától. Erre már online szolgáltatások is elérhetőek, akár magyar nyelven is.

A későbbi Office verziókban növelték a jelszavas védelem biztonságát, ezért megfelelően összetett és hosszú jelszavak esetén kellően sok időbe telik a jelszavas védelem visszafejtése. A rendszergazdák az az adott szervezeten belül az Office központi beállításaival (csoportházirend-szabályok) megkerülhetetlenné tehetik biztonsági igényeknek nem megfelelő jelszavak használatát, így erős jelszóházirend valósulhat meg. Fontos még tudni, hogy a számítógépek a jelszavakban megkülönböztetik a kis és nagybetűket, ezért nagyon pontosan szükséges megjegyezni, illetve eltárolni azokat.

Bár az Office beépített dokumentum védelme nem tökéletes, mégsem érdemes rögtön elvetni a használatát. A jelszavas védelem az egyszerű kíváncsiskodástól, és a véletlen módosítások ellen is védi a dokumentum tartalmát. A jelszavas dokumentumvédelem beállítása ráadásul egyszerű. A Fájl menü, Információ menüpontban a Dokumentumvédelem gomb Titkosítás jelszóval funkcióját kell kiválasztanunk. Összességében minősített információ védelmét nem biztosítja az Office titkosítása, de a fenti célok elérésére praktikusan használható.

Ha még olvasna erről:

http://office.microsoft.com/hu-hu/excel-help/a-jelszohazirend-HA010355926.aspx

A dokumentumok titkosítása

A dokumentumok titkosítására több lehetőség áll a felhasználók rendelkezésére. Lehetséges például a vállalati Windows verzióban a teljes fájlrendszer titkosítása, így minden dokumentum titkosításra kerül. Ennek az az előnye, hogy például egy eltulajdonított laptopról nem nyerhetők ki az adatok.

Az ismert informatikai biztonsági szoftvergyártók általában rendelkeznek dokumentum- és mappa-titkosítást lehetővé tevő szoftver modulokkal is, ezeket vagy a vírusvédelemre megvásárolt licencünk tartalmazza, vagy kedvezményes megvásárlását teszi lehetővé. A szervezeteknél való széleskörű kiterjesztése az adott megoldás tesztelését és oktatását igényli. Érdeklődjön szervezete biztonsági vezetőjénél a támogatott titkosítási módszerekről!

Ha a szervezetnél nincsen hivatalosan támogatott dokumentum titkosítási megoldás rendszeresítve, és a belső szabályozás nem tiltja a titkosítást, akkor lehetőségünk van a dokumentumok titkosítására akár nyílt forráskódú szoftverrel is.

Az egyik legnépszerűbb program, a Truecrypt, lehetővé teszi teljes merevlemezek, USB memóriák, de akár egyedi dokumentumok titkosítását is. Titkosító programokat, mint általában bármilyen programot is, csak megbízható helyről töltsünk le. Ilyen például a hivatalos oldala: http://www.truecrypt.org/downloads.

Érdemes a titkosítást úgy végezni, hogy olyan, a használt dokumentum méretnek megfelelő méretű tárolót (volume) készítünk, amely a levelező programok méretkorlátjába is belefér, 2-5 Mbyte méretűt. Ezt hozzáadva a rendszerhez (mount) a gyakorlatban egy új rendszer merevlemez meghajtóként látszik. A tároló titkosítva tárol minden belehelyezett állományt, másik számítógépen is csak a Truecrypt segítségével olvasható, a jelszó ismeretében.

Ha még olvasna erről:

http://www.truecrypt.org/faq
http://hvg.hu/tudomany/20080828_usb_titkositas
http://computerworld.hu/cio/titkositott-hordozhato-adattarolok.html

Outlook használat biztonsági kockázatai

Az Outlook a csoportmunkát támogatja, ezért beépített információmegosztó képességekkel rendelkezik. Ha ennek a felhasználó nincs tudatában, sérülhet az információ biztonsága.

Néhány példa:

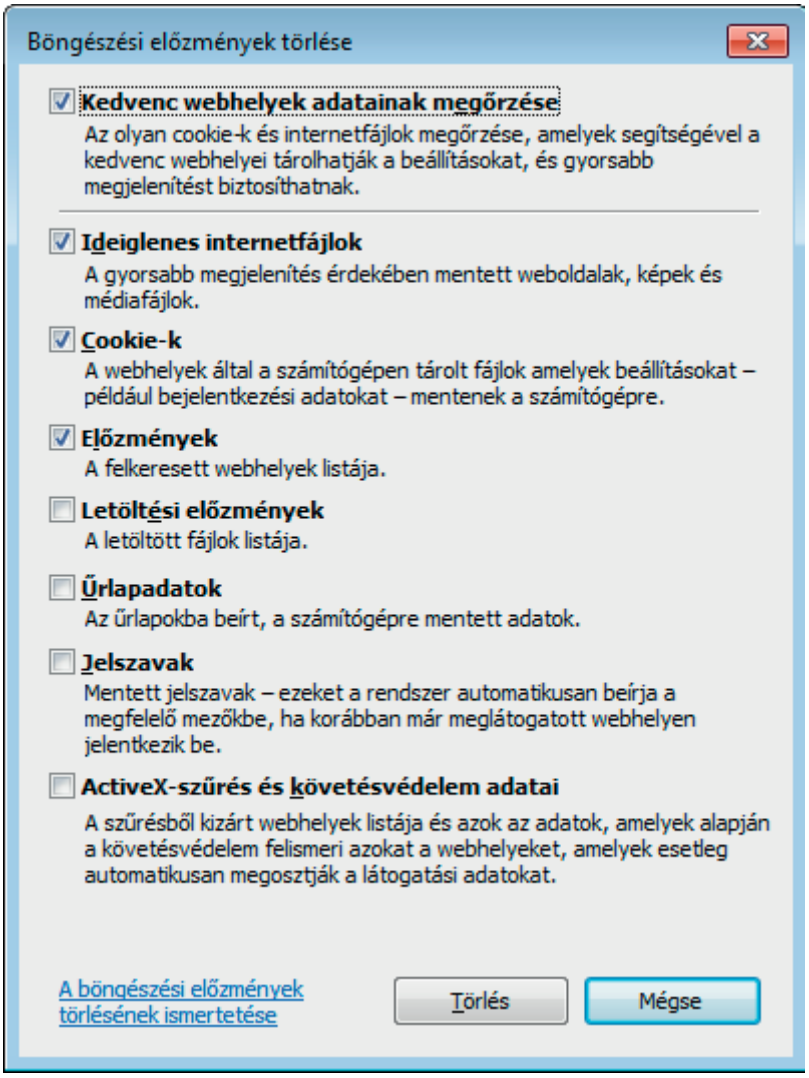
- A titkosítatlan levél tartalmát, amerre eljut a hálózaton, bárki elolvashatja.
- Naptárbejegyzéseket, vagy azok tárgyát olvashatják azok a munkatársak is, akikkel nem osztottuk meg teljes körűen az elfoglaltsági adatainkat.
- Üzenetek tárgyát olvashatják a kéretlen levél szűrőt kezelő informatikusok.

Az elektronikus levelekben zajló kommunikációs során tehát tudatában kell lennünk, hogy nem feltétlenül csak mi és az üzenet címzettje olvashatja az információt. Ebből kifolyólag például nemzeti minősített adatokat nem szabad a levelező rendszerben üzenetek szövegében küldeni, de üzleti titok esetén is célszerű az információ titkosítása.

Hasznos a címzettek figyelmét a levélben szereplő adatok bizalmas jellegére. Ám ha azokat titkosítás nélkül küldjük, felhívjuk a támadók figyelmét, hogy az üzenet releváns, értékes információt tartalmaz.

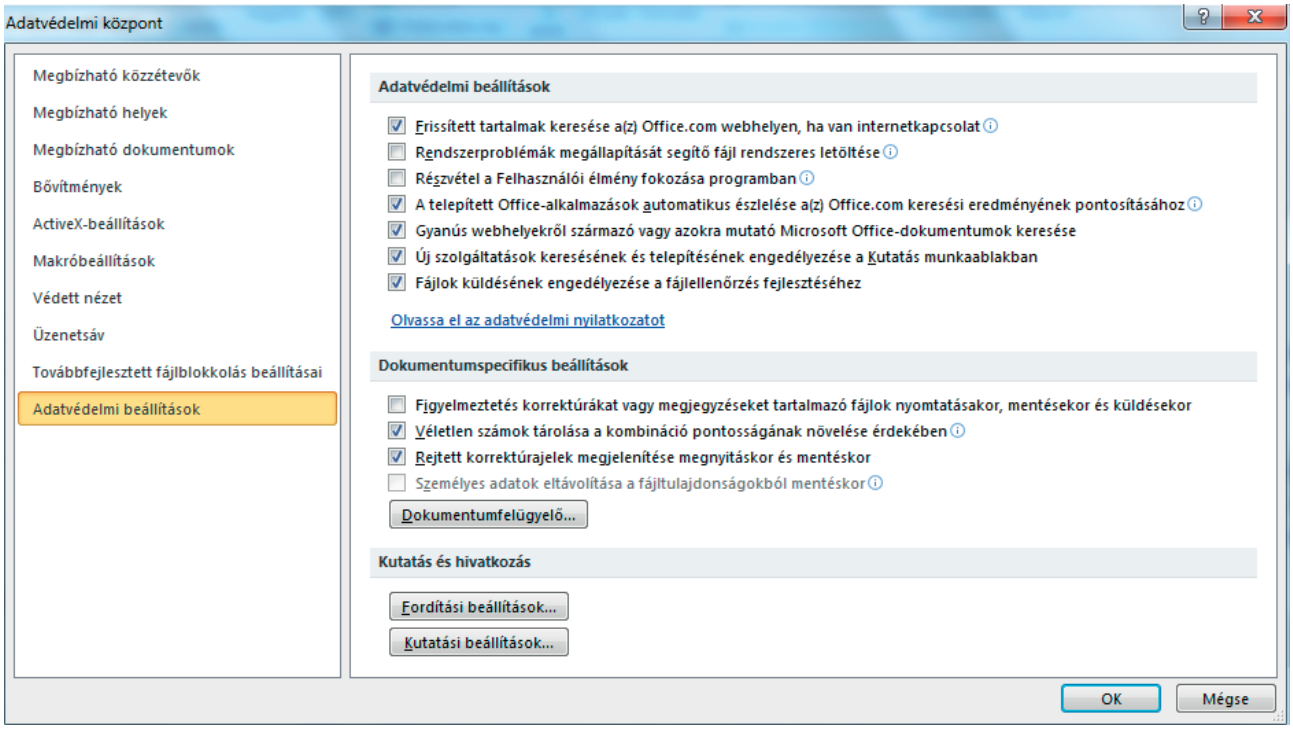
Távoli hozzáférés esetén fontos, hogy biztonságos számítógépről használjuk a rendszereket azért, hogy a jelszavunkat ne lophassák el. Ha az elektronikus levelezésünkhöz olyan számítógépről vagyunk kénytelenek hozzáférni, amelynek a biztonságáról nem tudunk meggyőződni, akkor a gyakori billentyűzetlopó programokat könnyedén „kicselezhetjük". Ha a Start menü Futtatás ablakába beírjuk az 'osk' parancsot, akkor egy virtuális billentyűzet jelenik meg a képernyőn, amelyen egy egér segítségével írhatjuk be a jelszavunkat, vagy akár rövidebb leveleket is írhatunk vele.

Az Internet Explorer böngészőben a böngészésünk nyomait az Eszközök menü Böngészési előzmények törlése menüpontban törölhetjük. A felugró ablakban választhatunk, hogy pontosan mely elemeket szeretnénk eltávolítani, az ideiglenes fájloktól kezdve egészen a beírt, elmentett jelszavakig törölhetünk adatokat.



Fontos funkció még az adatvédelmi beállítások köre, amely befolyásolja, hogy milyen információt küld az Office a gépünkről a Microsoftnak, illetve hogy mi milyen adatokat tölthetünk le a Microsofttól.

A különböző Office programokban és programverziókban eltérő lehet a beállítások köre, illetve a menük pontos elnevezése. Általában a Fájl menü Beállítások pontját kell kiválasztani, majd az Adatvédelmi központ Adatvédelmi beállítások funkcióválasztó menüben módosíthatunk a beállításon.



Az Office 2010-es programjai esetében, például ha a felhasználó bejelöli a Frissített tartalmak keresése az Office.com webhelyen funkciót, akkor internetkapcsolat megléte esetén mindig letöltheti a legfrissebb súgótartalmakat az Office.com oldalról. A program csak azokat a súgókat tölti le, amelyek a Keresés eredményében szerepelnek. Itt kapcsolhatjuk ki például, hogy információkat küldjön-e a gépünk a Microsoftnak a felhasználói szokásainkról (Felhasználói élmény fokozása program).

Ha van lehetőségünk saját programokat futtatni, akkor ingyenes szoftverek segítségével is törölhetjük a számítógépen végzett tevékenységünk nyomait. Ilyen program a Ccleaner, amely az ideiglenes állományokat, a megtekintett dokumentumokat, a gépen tárolt sütiket, és az internetezési előzményeket is képes gombnyomásra törölni. Van lehetőség ezek manuális törlésére is, azonban a teljes körű törléshez haladó felhasználói ismeretek szükségesek (például Windows registry kulcsok módosítása), ezért erre most nem térünk ki bővebben.

Amikor az Outlook információit telefonra, vagy számítógépre szinkronizáljuk, ne feledkezzünk meg arról, hogy onnantól azokat az eszközöket is az üzenetekben tárolt adatok védelmi szintjének megfelelően védenünk kell. Célszerű néhány napra korlátozni azt az időtartamot, ameddig az eszköz tárolja az üzeneteket, így csökken a kár mértéke, ha elhagyjuk az eszközöket. Ha más alkalmazások számára is engedélyezzük az adatokhoz hozzáférést, akkor könnyen eljuthatunk oda, hogy ingyenes levelező rendszerekbe betöltjük a teljes partner adatbázisunkat.

Ha még olvasna erről:

http://office.microsoft.com/hu-hu/word-help/az-adatvedelmi-beallitasok-megtekintese-HA010354327.aspx
http://www.piriform.com/ccleaner/builds

Eszközök közötti adatszinkronizálás kockázatai

Egyre több különböző eszközt használunk munkánk során, már ügyintézői szinten is megjelenik a telefonokon való elektronikus levelezés igénye, vezetői szinteken pedig a hordozható számítógépek és táblagépek munkavégzés célú használata.

Az okostelefonok, kéziszámítógépek és táblagépek használata során kézenfekvő felhasználói igény a munkaállomások és a mobil eszközök közötti adatszinkronizáció. Ez azzal jár általában a gyakorlatban, hogy a levelezés, a naptár, és bizonyos dokumentum könyvtárak előre meghatározott szabályok szerint szinkronizálnak, azaz átmásolja a rendszer őket minden eszközre. Amennyiben itt nem állítanak be szűkítéseket, úgy a mobil eszközök elvesztése, vagy eltulajdonítása esetén jelentős kárt okozhat az adatok illetéktelen kezekbe kerülése.

Adatszinkronizálás beállítása előtt meg kell győződni arról, hogy a szervezet belső szabályai lehetővé teszik-e az adott eszköz (hivatali, vagy saját) munkavégzés célú használatát. Csak olyan eszközre tegyünk hivatali adatokat, amelyre engedélyezett!

A szinkronizálás során felmerülhet, hogy a hivatali adatokat, nem csak a hivatal által jóváhagyott alkalmazásokba tároljuk (például: gmail, facebook), általában ez a hivatali szabályokkal nincsen összhangban, ezért erről is meg kell előzetesen győződni!

Jó gyakorlat a szinkronizálás korlátozása a ténylegesen szükséges adatkörökre (nem minden könyvtár), és időtartamra (például az elmúlt 1 hét adataira), beleértve a levelező program beállításait is.

A okostelefonok, és táblagépek beépített védelmi funkcióit célszerű alkalmazni (pl. jelszó, képernyő zárolás), így illetéktelenek nem férhetnek olyan könnyen hozzá az adatainkhoz.

Amennyiben van mobil eszköz védelmi szoftver telepítve az eltulajdonított gépen, akkor lehetséges az eszköz adattartalmának távoli törlése, és az eszköz földrajzi helyzetének meghatározása (GPS lokalizáció). Ezt általában a szervezet biztonsági vezetője végezheti el.

Ha még olvasna erről:

http://support.apple.com/kb/HT1296?viewlocale=hu_HU&locale=hu_HU
http://www.windowsphone.com/hu-hu/how-to/wp8/people/sync-contacts-and-calendars-from-outlook-on-my-pc-to-my-phone
http://computerworld.hu/computerworld/mobil-eszkozok-menedzselese-avagy-mire-is-figyeljunk-a-byod-eseten.html

Vezeték nélküli internet (WiFi) használat kockázatai

A WIFI hálózatok korábban elképzelhetetlen rugalmasságot biztosítanak informatikai hálózatokhoz való kapcsolódásra, ugyanakkor a biztonságos beállítások és a biztonságtudatos használat hiányában korlátlan hozzáférést biztosíthatnak adatainkhoz egy támadó számára.

A nyilvános WiFi hálózatok több kockázatot hordoznak magukban, egyrészt például egy külső támadó lehallgathatja a hozzáférési ponthoz csatlakozó felhasználók adatforgalmát, illetve ha saját hozzáférési pontot működtet, akkor web oldalak eltérítésével további adatokat szerezhet meg a felhasználók megtévesztésével. Különösen fontos ezért nyilvános helyeken ügyelni arra, hogy milyen kapcsolaton keresztül internetezünk. Bizalmas információkat, jelszavakat például sosem adjunk meg ilyen kapcsolaton keresztül, ha biztonságban szeretnénk tudni értékeinket, és adatainkat. Különösen fontos ez nagy forgalmú helyeken (pl. szálloda, repülőtér, külföldi konferencia), mert itt a bűnözők mellett adott esetben akár idegen államok hírszerzői igyekszenek információs igényüket kielégíteni.

A leggyakoribb kockázat az otthoni működtetés szempontjából az, hogy elmulasztják újrakonfigurálni a hálózati beállításokat, azaz az alapbeállításokkal működtetik. Az illetéktelen bejutás ilyenkor nagyon egyszerű, mivel a gyári beállítások ismertek a betörők számára. A beállítás során hálózat védelme érdekében a biztonsági funkciókat be kell kapcsolni, például erős titkosítást kell engedélyezni (WPA2), továbbá a hozzáféréshez szükséges jelszót megfelelően kell megválasztani. A jelszó hossza, és összetettsége növeli a jelszó feltörésének idejét, a jelenlegi műszaki megoldásokkal általában egy egyszerű támadónak egy hónapra van szüksége egy összetett WiFi jelszó feltörésére, ezért jó gyakorlat, ha 30 naponta cseréljük.

Hivatali, illetve vállalati környezetben WiFi hálózatot csak indokolt esetben javasolt engedélyezni, és akkor is megfelelő szintű biztonságot garantáló megoldások telepítése szükséges (pl. CISCO, ARUBA). Van tehát biztonságos WiFi, akár katonai szintű biztonság is elérhető vele.

Ha még olvasna erről:

http://hu.wikipedia.org/wiki/Wi-Fi
http://www.tutorial.hu/wifi-halozatunk-biztonsagossa-tetele/
http://infoter.eu/cikk/repulotereken_kockazatos_a_wifi_hasznalata
http://computerworld.hu/cio/biztonsagos-vallalati-wi-fi-halozatok.html

Biztonságos üzemeltetés

A RENDSZERGAZDÁKAT FENYEGETŐ VESZÉLYEK

Az információs rendszerek biztonságos üzemeltetéséről részletes módszertanok, egyetemi specializációk, és nemzetközi szakmai vizsgák szólnak. Jelen tájékoztató nem kíván ezekkel versenyezni, azonban fel kívánja hívni a figyelmet a közelmúltban tapasztalt lényeges kockázatokra.

Különösen a nemzetközi és hazai tapasztalatok függvényében fontos, hogy az információs rendszerek működtetéséért felelős munkatársak tisztában legyenek a felelősségeikkel, és máshol már bekövetkezett hibák hatásaival.

A közszférában például a Nemzeti Biztonsági Felügyelet, a Nemzeti Hálózatbiztonsági Központ, és az Alkotmányvédelmi Hivatal végez tájékoztató tevékenységet. A nemzetközi és a hazai biztonsági szakmai szervezetek is számos rendezvényen, és kiadványok formájában biztosítják a figyelem felhívását, és a szakemberek tájékoztatását. Ilyen az ISACA, a KIBEV, és a HTE rendezvényei, de üzleti konferenciák témáján is rendszeresen szerepel.

A biztonságos üzemeltetés képességének megvalósítása a szervezet első számú vezetőjétől indul, fontos hogy ezt célként határozza meg a szervezet számára, biztosítsa az ehhez szükséges eszközöket, és szakembereket.

A gyakorlatban az üzemeltetés biztonsága viszont a rendszereket működtető informatikus szakembereken, a rendszergazdákon, és közvetlen vezetőiken múlik. Fel kell készíteni a szakembereket a munkájuk végzésére:

- az alapvető információbiztonsági ismeretekkel rendelkezniük kell,
- a biztonságos üzemeltetéshez szükséges alapvető ismeretekkel rendelkezniük kell,
- és a felelősségi körükbe tartozó rendszerek pontos működését, és biztonsági funkcióit ismerniük kell.

Önmagában egy felkészült rendszergazda nagyon fontos, de nem elégséges a biztonságos üzemeltetéshez, biztosítani kell a helyettesíthetőségét és az elvégzett üzemeltetési tevékenységek dokumentálást.

Ha még olvasna erről:

http://www.kibev.hu/index.php/sans-top-20-kibev-poszter

Veszélyek: túlterheléses támadás (DoS, DDoS)

Jellemző hatása: Alacsony, Közepes, Magas

Miről beszélünk?

Egy kiszolgáló gép, vagy például egy szervezet kiszolgálói által kezelt honlapok csoportjának a célzott leterhelése, gyakran zombi hálózatok segítségével. DoS támadás esetén rövid időn belül olyan sok információkérés érkezik a szolgáltatást kiszolgáló szerverhez, hogy fizikailag nem képes rá válaszolni. Ez a rendszerek túlterheléséhez és a szolgáltatások átmeneti elérhetetlenségéhez, vagy leállásához vezet.

Mit veszélyeztet?

- Felhasználó: a felhasználók nem képesek elérni az érintett szolgáltatást.
- Rendszerműködés: sérül a rendszerek rendelkezésre állása, akár hosszabb időre is elérhetetlenné válhat.
- Információbiztonság: esetenként a túlterheléses támadást összetett kibertámadás részét képezi, ilyenkor például a rendszerekben levő adatokat is megszerezhetik, amíg a biztonsági szakemberek a leterhelések elhárításán dolgoznak.
- Nemzetbiztonság: amennyiben a közszféra rendszereit éri a támadás, nemzetbiztonsági következményei is lehetnek.

Példák:

Az Anonymous kormányzati honlapokat is támadott a közelmúltban tiltakozásképpen bizonyos kormányzati intézkedésre, illetve a média figyelmét is ennek segítségével sikerült felkelteniük.

A Sony internetes játékrendszere elleni összetett támadás során a rendszert feltörték, és hozzáfértek a felhasználók adataihoz. Azonban az adatok megszerzését a védelmi rendszer nem tette lehetővé, amíg egy összehangolt túlterheléses támadás nem bénította meg a működését. Amíg a biztonsági szakemberek a rendszereket próbálták életben tartani, addig a támadással járó nagy forgalom elleplezte a személyes adatok letöltését a rendszerből.

Hogyan előzzük meg?

A rendszerek tervezésekor szükséges olyan rendszer környezetet kialakítani, amely a szolgáltatást ért terheléseket megosztja a szolgáltatást biztosító több kiszolgáló között.

Ugyancsak a tervezéskor kell biztosítani olyan biztonsági funkciókat, például betörés megelőző rendszer (IPS) megvalósítását, amely képes a támadó számítógépről jövő forgalom felismerésébe, és a támadóktól jövő tranzakciók eldobására, így tehermentesítve a szervereket.

Javasolt még intézkedési tervek kidolgozása DoS támadás esetére, amely útmutatást biztosít az üzemeltetők részére a támadás során, és azt követően megteendő intézkedésekről.

Mit tegyünk, ha bekövetkezik?

Több oldalról kell megközelítenünk a támadás elleni védekezést. Lehetséges további kapacitások biztosításával a nagy terhelés ellenére életben tartani a szolgáltatást. A tűzfal és IPS beállítások módosításával kizárni a támadóktól érkező forgalmat. Ebben segítségükre lehet az internetszolgáltató, és a hálózatbiztonsági központok segítsége is.

A Nemzeti Hálózatbiztonsági Központ útmutatója részletes segítséget biztosít DoS támadások kezelésére.

Ha még olvasna erről:

http://tech.cert-hungary.hu/sites/default/files/uploads/nhbk_vedekezes_a_dos_tamadasokkal_szemben.pdf
http://hu.wikipedia.org/wiki/Szolg%C3%A1ltat%C3%A1smegtagad%C3%A1ssal_j%C3%A1r%C3%B3_t%C3%A1mad%C3%A1s
http://infoter.eu/cikk/informatikai_tamadas_europai_szimulacios_gyakorlata_-_cyber_europe_2012

Veszélyek: hálózati letapogatás (network / port scanning)

Miről beszélünk?

Jellemző hatása: Alacsony, Közepes, Magas

Az internetre csatlakoztatott rendszerek előtt levő biztonsági szoftverekben (tűzfal, IPS) rendszeresen találkozhatunk olyan jellegű információkérési próbálkozásokkal, amelyeknek az a célja, hogy az adott rendszerről minél több információt gyűjtsenek be.

Mit veszélyeztet:

- Felhasználó: a felhasználók általában csak az otthoni számítógépük tűzfal naplójában találkozhatnak ezzel, ha elmélyednek benne.
- Rendszerműködés: a célzott hálózat letapogatás és felderítés a szolgáltatás minőségének csökkenéséhez vezethet átmenetileg. Ha a letapogatás nem talál ismert hibát és nem követi betörés, vagy jelszófeltörési próbálkozás akkor nincsen hatása.
- Információbiztonság: a rendszerekre vonatkozó információk segítségével eredményes betörésekre kerülhet sor, ekkor vezethet az információbiztonság sérüléséhez.
- Nemzetbiztonság: idegen államok által végzett tevékenységként veszélyeztetheti a nemzetbiztonságot.

Példa:

Számos technikai módszer és program elérhető a hálózatok letapogatására, és megelőzési célból is használhatjuk saját rendszerünk gyenge pontjainak felderítésére.

Sok esetben az ismeretlen forrásból érkező hálózati kérések, ún. hálózat letapogatások egy jövőbeni támadás lehetőségét foglalják magukban. Így kívánnak információt gyűjteni a rendszerünk gyenge pontjairól, illetve rendszereink ismert sérülékenységeiről.

Hogyan előzzük meg?

A korszerű tűzfalaknak figyelniük kell az egyes hálózati portokon folyó forgalmat. Érzékelniük kell, ha valaki letapogatja a nyitott portokat (port scanning), és képesnek kell lennie az egyes portok lezárására, vagy a letapogatást végző felől jövő teljes forgalom kizárására.

A rendszereink biztonsági frissítése csökkenti a külső támadások eredményességét, ezért itt is jó megelőzési módszer. Mert azt az információt jelzi a támadónak vissza, hogy a rendszerünk nem támadható ismert módon.

Mit tegyünk, ha bekövetkezik?

Önmagában még a letapogatás általában nem okoz kárt. Ha a hálózatunk letapogatásának gyakorisága, vagy intenzitása megnő, akkor fokozott figyelemmel indokolt figyelni a hálózati biztonsági szoftvereink jelzéseit.

Ha még olvasna erről:

https://en.wikipedia.org/wiki/Port_scanner
https://en.wikipedia.org/wiki/Vulnerability_scanner
http://www.center.hu/tudastar/cikkek/a_port_scan_muveszete.html

Veszélyek: távoli adminisztrátor eszközök

Miről beszélünk? **Jellemző hatása:** Alacsony, Közepes, Magas

A számítógépek távoli felügyeletét és karbantartását a Windows beépített funkciói, és egyéb távoli adminisztrációt lehetővé tevő szoftverek is biztosítják. Ezek nagyban könnyítik és gyorsítják a hibaelhárítást, azonban nem megfelelő beállításuk biztonsági kockázatokat hordoz magában, mert jogosulatlan távoli hozzáférést tehet lehetővé.

Mit veszélyeztet?

- Felhasználó: felhasználók rendszeréhez és adataihoz való hozzáférést tehet lehetővé, ha nem megfelelő a beállítása.
- Rendszerműködés: a rendszerek távoli vezérlése véletlenül, vagy szándékos károkozás esetén a működést veszélyeztetheti.
- Információbiztonság: a rendszerekhez való teljes körű hozzáférés az ott külön védelem nélkül tárolt információkat is veszélyezteti.
- Nemzetbiztonság: hírszerzők is előszeretettel alkalmaznak olyan eszközöket, hátsó ajtókat, amelyek távoli hozzáférést tesznek lehetővé. Ezek veszélyeztethetik a nemzetbiztonságot.

Példa:

Számos trójai program rendelkezik hátsó ajtó funkcióval, ami távoli adminisztrációt tesz lehetővé. Olyan funkcióik vannak, mint például:

- fájlok átnevezése, letöltése;
- rendszerbeállítások módosítása;
- jelszavak ellopása;
- vírusok telepítése;
- képernyőkép ellopása.

Hogyan előzzük meg?

A távoli hozzáférést biztosító szoftverek megfelelő beállítása megelőzheti azt, hogy illetéktelenek hozzáférjenek.

Ebben az esetben is fontos a számítógépek végpontvédelme és a hálózatok alapvető biztonsága, hogy a kártevőként települő távoli adminisztrációs programokat települését megakadályozzuk, illetve mielőbb feltárjuk és törölhessük.

Mit tegyünk, ha bekövetkezik?

A szoftverek biztonsági beállításait vizsgáljuk felül, a jogosulatlanul telepített eszközöket töröljük le, és átfogó víruskeresést végezzünk a teljes rendszerünkben.

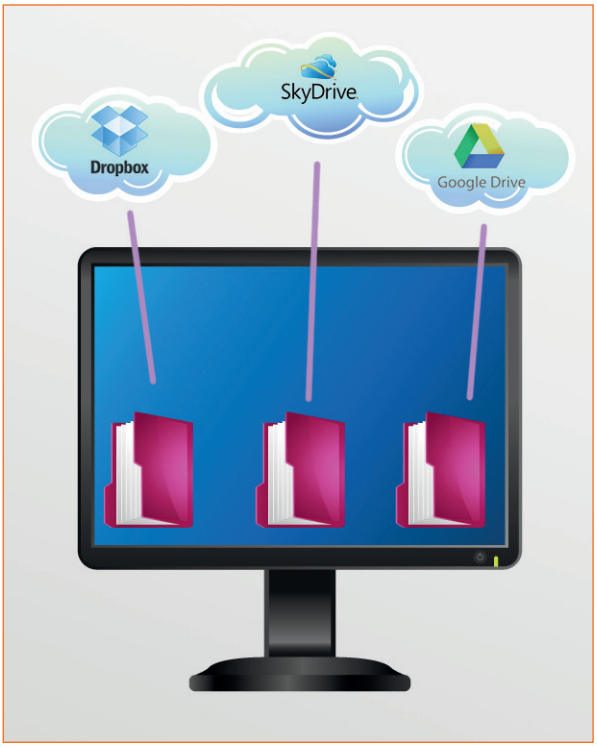
Ha kárt is szenvedtünk a támadás eredményeként, akkor figyeljünk arra, hogy támadás időszakának rendszernaplóit mentsük le további vizsgálatokhoz!

Ha még olvasna erről:

http://en.wikipedia.org/wiki/Remote_administration_software
http://www.microsoft.com/hu-hu/windowsserver2012/remote.aspx

Veszélyek: adatvesztés

Jellemző hatása: Alacsony, Közepes, **Magas**



Miről beszélünk?

A rendszereink által kezelt adatok mentését, ha nem megfelelően tervezzük meg, vagy a mentések megvalósítása hibás, akkor rendszerhiba, véletlen esemény, vagy szándékos károkozás esetén elveszhetnek adatok.

Mit veszélyeztet?

- Felhasználó: gyakori, hogy a számítógépünkön tárolunk egyedül valamilyen adatot, egy példányban. Ez könnyen sérülhet, elveszhet.
- Rendszerműködés: a munkahelyi rendszerek mentésének hiányosságai jelentős kárt okozhatnak.
- Információbiztonság: mentés hiányában az egy példányban meglevő adatok sérülékenyek, módosításuk, vagy törlésük jelentős kárt okozhat.
- Nemzetbiztonság: közszféra rendszerei esetén kiemelten fontos az adatok megfelelő védelme.

Példa:

Hardver hiba miatt volt már példa arra, hogy megsérült adathordozókon a sérült adatok a biztonsági tartalék adathordozóra is automatikusan átmásolásra kerültek (RAID).

Ha a minimálisan szükséges mentendő adatmennyiség (RPO) nem megfelelően kerül meghatározásra, akkor a működést veszélyeztethet akár egy műszaki hiba is, amely adatvesztéssel jár, mivel ebben az esetben csak az előző mentésből állítható vissza az adat, ami egy hét, vagy egy nap teljes munkájának pótlásával is járhat.

Hogyan előzzük meg?

Fontos a rendszereinkben kezelt adatok körének pontos ismerete, azokra vonatkozó mentési követelmények azonosítása és vezetői jóváhagyása. Ennek ismeretében végezheti el az üzemeltetés a megfelelő mentési megoldások kialakítását.

A felhasználók tudatosítása is szükséges az adatmentés megelőzése érdekében. Általában a felhasználók által használt asztali, vagy hordozható számítógépek merevlemezét központilag nem mentik, ezért nem is szabad fontos adatokat tárolni rajtuk. A felhasználó, vagy a szervezeti egység központi meghajtóját szükséges használni a munkavégzés során. Így biztosítható az adatok visszaállíthatósága.

Mit tegyünk, ha bekövetkezik?

Ideális esetben vegyük elő az utolsó mentést, amelyet az üzleti igényeknek megfelelően határoztunk meg, így elviselhető mértékű az adatvesztésünk, amelyet néhány túlórában a szervezet képes pótolni.

Ha szerencsénk van, akkor nem dolgoztunk az adattal az előző mentés óta, így az informatika adatvesztés nélkül vissza képes állítani.

Ha azt tapasztaljuk, hogy mégsem az szervezet igényeinek megfelelő a mentési szabályzat, akkor vizsgáljuk felül azt, hogy a jövőben nem kerüljünk ismét ilyen helyzetbe!

Ha az adathordozónk sérülése miatt van adatvesztésünk, akkor megpróbálkozhatunk az adatmentő szolgáltatás igénybevételével, ezeknek azonban jelentős költségük van, így csak indokolt esetben javasolt igénybevételük.

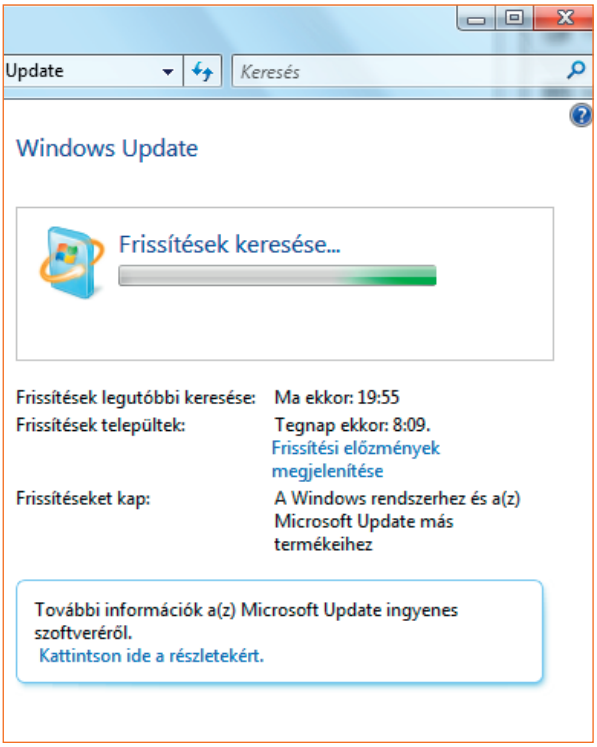
Ha még olvasna erről:

http://hu.wikipedia.org/wiki/Adatment%C3%A9s
http://computerworld.hu/computerworld/nincs-orvossag-az-adatvesztesre-20090212.html
http://www.infoter.eu/cikk/ot_tanacs_a_katasztrofa-helyreallitasi_terv_felepitesehez

Veszélyek: rendszerfrissítések hibái, hiánya

Miről beszélünk?

Jellemző hatása: Alacsony, Közepes, Magas



A támadók számára a legkézenfekvőbb támadási módszer a rendszerek ismert hibáinak kihasználása. Sok esetben célzott támadást lehetővé tevő programok készülnek, amelyeket a rendszerek frissítésének hiányában sikeresen alkalmazhatnak. Fontos ezért a rendszerek hibáit javító frissítések rendszeres telepítése.

Mit veszélyeztet?

- Felhasználó: az otthoni felhasználókat is veszélyezteti a hibás szoftverek használata, különösen az operációs rendszer és a JAVA környezet frissítésének hiánya okozott problémákat.
- Rendszerműködés: súlyos kárt okozhat a frissítések hiánya, távolról akadályozhatják a rendszer működését, vagy le is állíthatják.
- Információbiztonság: a rendszerek hibáit kihasználva hozzáférhetnek a rendszerekben kezelt adatokhoz is.
- Nemzetbiztonság: közszférában használt rendszerek esetében fokozottan indokolt a rendszerek frissítése, hogy hiányukból fakadó kockázatok csökkenthetőek legyenek.

Példa:

A JAVA futtatókörnyezetben a közelmúltban feltárt hibák olyan biztonsági kockázatot jelentettek, hogy a védelmi szakemberek a teljes letiltásukat javasolták addig, amíg nem javítják a hibát.

Az ingyenes web szerverek pl. Apache ismert hibáit kihasználva, akár weboldalakat is megfertőzhetnek, így akaratunk ellenére vírusok és kártevő programok terjesztőivé válhatunk.

Hogyan előzzük meg?

Célszerű a rendszerfrissítéseket automatizálni. Az otthoni felhasználás esetén általában több előnnyel jár a frissítés telepítése, mint elmulasztása.

A szervezetek rendszereiben javasolt a frissítések ütemezett telepítése, azaz néhány tipikus gépre telepítsük először, vizsgáljuk felül, hogy van-e valamilyen hatása a szokásosan használt informatikai rendszerekre, és ha nem okoz hibás működést, akkor terjesszük ki a többi gépre.

A szokásos Windows frissítések mellett nagyon fontos a szerverek frissítése, különösen a külső hálózatra kötött gépeké, de nem kevésbé fontos a belső hálózaton levőké sem, mert ha a határvédelmen átjön egy támadó, akkor a belső rendszerek felől is képes támadni az informatikai szolgáltatásokat.

Mit tegyünk, ha bekövetkezik?

Ha elmulasztottunk egy rendszert frissíteni, akkor mielőbb frissítsük, ha tudomásunkra jut.

Működtethetünk automatizált sérülékenység vizsgáló szoftvert, amely rendszeresen feltárja a hiányzó frissítéseket.

Ha még olvasna erről:

http://en.wikipedia.org/wiki/Windows_Update
http://hu.wikipedia.org/wiki/Nulladik_napi_t%C3%A1mad%C3%A1s

Biztonságtudatos vezetés

MIT TEHETNEK A VEZETŐK AZ INFORMÁCIÓBIZTONSÁGÉRT

A menedzsment módszertanok a biztonsági kultúra eredményes megvalósítását lehetővé tevő sikertényezők között első helyen tartalmazzák a felső vezetés elkötelezettségét. Sőt, több módszertan odáig megy, hogy azt mondja, ennek hiányában neki kezdeni sem érdemes, mert eleve kudarcra van ítélve a kezdeményezés.

Biztonságirányítás követelményei

A következő négy alfejezetben ismertetjük az ISACA nemzetközi felmérésén alapuló követelményeket, amelyeket az információbiztonsági irányítással szemben a szervezeteknek támasztaniuk kell.

Információbiztonság irányítása

A szervezetnek olyan információbiztonság irányítási keretrendszert és erre épülő működési folyamatrendszert kell kialakítania és fenntartania, amely biztosítja az információbiztonsági stratégia összhangját a szervezet céljaival, kötelező és vállalt feladataival, a szervezetet veszélyeztető kockázatokkal, továbbá a megvalósítására biztosítható forrásokkal.

- Az információbiztonság irányítását a szervezet irányítási rendszerének szerves részéve kell tenni, és irányítási módszert (keretrendszert) kell alkalmazni.
- Meg kell szerezni a szervezet vezetője (felső vezetés) támogatását az információbiztonsági stratégia sikeres megvalósítása érdekében.
- Az információbiztonsági stratégiát a szervezet stratégiájából (kötelező feladataiból) levezethető célokhoz illeszkedve kell kialakítani.
- Az információbiztonsági stratégia megvalósítását folyamatos információbiztonsági programként kell végrehajtani.
- Információbiztonság irányítását és menedzselését szét kell választani.

- Az információbiztonsági beruházásokról szóló döntést támassza alá részletes megtérülés vizsgálat (business case).
- Az információbiztonságra hatással levő külső és belső tényezőket rendszeresen azonosítani és értékelni kell.
- Meg kell határozni a szervezet minden szintjén az információbiztonságért való felelősségeket, szerepeket a felső vezetéstől a beosztott munkavállalók szintjéig.
- Olyan visszamérési mutatószámrendszert kell kialakítani, amely biztosítja a kockázatok feltárását (KRI) az előrehaladás mértékének meghatározását (KPI), és a célok elérését (KGI), ezáltal eredményesen biztosítva az információbiztonsági stratégia elérését, és a szervezet kötelező és vállalt feladatainak végrehajtását.

Információs kockázatkezelés és megfelelés az előírásoknak

Az információs rendszereket veszélyeztető kockázatokat olyan módon kell kezelni, hogy azt a jogszabályok által előírt és a szervezet vezetője által elfogadott szinten tartsuk.

- Az információs vagyonelemek értékelésére és biztonsági osztályba sorolására folyamatokat kell kialakítani, azért, hogy a vagyonelemeknek az értéküknek megfelelő védelmet biztosítsuk.
- Meg kell határozni az információs rendszerekkel kapcsolatos összes elvárást (jogszabályi, hatósági, tulajdonosi, szerződéses és más követelmények), ezért hogy a követelmények nem teljesítésének kockázatát kezelhessük.
- Rendszeresen el kell végezni a sérülékenységek, fenyegetések felmérését az információt fenyegető kockázatok azonosítása érdekében.
- A kockázatvállalási szintnek megfelelő kockázatkezelési intézkedéseket kell alkalmazni.
- Értékelni kell az információbiztonsági kontrollokat, hogy megfelelőek-e a kockázatok csökkentésére, és ténylegesen megfelelően működnek-e.
- A jelenlegi kockázati szint és az elvárt kockázati szint közötti különbséget meg kell határozni.
- Az információbiztonsági kockázatok kezelésének tevékenységeit be kell építeni a szervezet minden működési folyamatába annak érdekében, hogy egységes legyen a kockázatok kezelése.
- Folyamatosan figyelemmel kell kísérni a kockázatoknak, és a kockázatok mértékének a változását, hogy megfelelően kezelhessék őket.
- A szervezet megfelelő szintjén lévő vezetőket tájékoztatni kell a kockázatok változásáról, és a követelmények esetleges sérüléséről azért, hogy megalapozott döntéseket hozhassanak.

Információbiztonsági program kidolgozása és megvalósítása

Az információbiztonsági programot az információbiztonsági stratégiával összhangban kell kialakítani és megvalósítani.

- Biztosítani kell az információbiztonsági program információbiztonsági stratégiával való összhangját.
- Az integráltság növelése érdekében a szervezet alap- és működési folyamataihoz illeszkedve kell az információbiztonsági programot megvalósítani.
- Az információbiztonsági program végrehajtásához szükséges belső és külső erőforrásokat azonosítani, rendelkezésre állásokat pedig biztosítani és menedzselni kell. Az információbiztonsági program végrehajtásának megfelelő információbiztonsági architektúrát (emberek, folyamatok, műszaki megoldások) ki kell alakítani és fenn kell tartani.
- A szervezet információbiztonsági szabványait, eljárásait, útmutatóit és más, vonatkozó dokumentumokat az információbiztonsági politikának megfelelően kell kialakítani, kommunikálni és karbantartani.
- A biztonságos környezet, és a ténylegesen biztonságtudatos szervezeti kultúra elősegítésére információbiztonság-tudatosítási programot és képzési rendszert kell kialakítani és fenntartani.
- A szervezet alapvető biztonsági szintjének fenntartása érdekében az információbiztonságból fakadó követelményeket bele kell építeni a szervezet folyamataiba (pl.: változtatások felügyelete, katasztrófa helyreállítás, stb.).
- A szervezet alapvető biztonsági szintjének fenntartása érdekében a harmadik felekkel (pl. informatikai szolgáltató, takarító cég) kötendő szerződésekbe be kell építeni az információbiztonsági követelményeket.
- Az információbiztonsági program eredményességének és hatékonyságának értékelésé érdekében meg kell teremteni a program végrehajtásának feltételeit és ki kell dolgozni a működést mérő mutatószám rendszert. A mutatószámok alakulását figyelemmel kell kísérni, és a vezetés számára időszakonként jelentéseket kell készíteni.

Információbiztonsági rendkívüli eseménykezelés

A szervezetet érő károk csökkentése érdekében meg kell tervezni, megvalósítani és menedzselni az információbiztonsági események azonosításának, kivizsgálásának, rájuk való reagálásnak és a helyreállításuknak a képességét.

- A rendkívüli információbiztonsági eseményekre való reagálás akciótervét ki kell alakítani és karban kell tartani azért, hogy minden eseményre eredményesen és időben legyen képes reagálni a szervezet.

- A rendkívüli információbiztonsági események kezelésének folyamatát ki kell alakítani azért, hogy időben azonosíthatóak legyenek.
- Ki kell alakítani és karban kell tartani a rendkívüli információbiztonsági események kivizsgálásának és jegyzőkönyvezésének folyamatát azért, hogy megfelelő választ adhassunk az eseményekre, valamint minden esetben meg kell határozni az események okát a jogi, hatósági és szervezeti követelmények szerint.
- Ki kell alakítani és karban kell tartani a rendkívüli eseményekről való tájékoztatás rendszerét és azok eszkalálásának a folyamatát azért, hogy a rendkívüli eseményekre adott válaszok meghatározásába és végrehajtatásába az érintetteket a szervezet be tudja vonni.
- Meg kell szervezni, ki kell képezni és fel kell szerelni a rendkívüli információbiztonsági eseményekre időben és eredményesen reagálni képes csapatot.
- Időszakonként tesztelni kell, és felül kell vizsgálni a rendkívüli eseménykezelési tervet azért, hogy az információbiztonsági rendkívüli eseményekre eredményes választ adhassunk és javítsuk a reagálási képességet.
- Ki kell dolgozni és karban kell tartani a kommunikációs tervet és folyamatot azért, hogy a belső és külső érintettekkel való kommunikációt kézben tudjuk tartani.
- A rendkívüli események elhárítását követően felülvizsgálatot kell tartani;meg kel határozni az információbiztonsági rendkívüli események gyökér okát, a helyesbítő intézkedéseket, újra fel kell mérni a kockázatokat, újra kell értékelni az elhárítás eredményességét és, ha szükséges, megfelelő helyesbítő intézkedéseket kell hozni.
- Ki kell alakítani és karban kell tartani a rendkívüli eseménykezelési tervek, a katasztrófa elhárítási tervek, és az üzletfolytonossági tervek integrációját.

A következő oldalakon a felső vezetői elkötelezettség fontos elemeit mutatjuk be és kívánunk gyakorlati tanácsokat adni annak eredményes megvalósítása érdekében.

Személyes példamutatás

A felsővezetők tudatos elkötelezettsége fontos kezdete a biztonságtudatos vállalati kultúra kialakításának, ugyanakkor ez csak a kezdet. Fel kell figyelnie a vezetőknek arra, hogy a biztonsággal kapcsolatos tevékenységeiket körültekintően végezzék.

Több olyan rossz gyakorlat, vezetői szokás van, amely hátráltatja a biztonsági kultúra fejlődését:

- Ha egy problémát figyelmen kívül hagyunk, attól nem oldjuk meg. Könnyen lehet, hogy sokkal nagyobb kárt okozva fog ismét felmerülni!
- Ha tűzoltás jelleggel, rövidtávú megoldásokkal kezelünk problémákat, akkor újra felbukkanhatnak!

- Ha úgy gondoljuk, hogy mindenki elengedi a füle mellett, ha véletlenül a szervezetünkről nyilvánosságra kerül egy biztonsági esemény, akkor tévedünk! Népszerű sajtóhír lesz belőle!
- Ha egyszeri alkalommal ruházunk be a biztonság érdekében, de spórolunk a karbantartáson és a működtetésen, akkor nem biztosítjuk a biztonság fenntartását!
- Ha azt gondoljuk azért mert a biztonsági rendszer egy elemét, például a tűzfalat egy nagyobb összegért rendbe raktuk, akkor biztonságos a rendszer, tévúton járunk. Az újabb támadások vígan keresztülmennek a tűzfalakon legitim forgalomnak álcázva magukat. A rendszer egyen szilárd védelmére kell törekednünk!
- Ha a szervezet védelmének kialakítása során a fizikai biztonságot tartjuk előtérben, akkor nem ismerjük fel a szervezet működésének prioritásait! Sokkal jelentősebb lehet a gyenge információbiztonsági szabályok következménye!
- Ha névleg jelöljük csak ki az információbiztonsági felelőst, de nem biztosítjuk a folyamatos képzést számára, vagy biztosítjuk a feladat végrehajtásához szükséges kapacitást, akkor nem tudjuk a kellő mértékben kézben tartani a biztonsági kockázatokat!

Összességében, ha nem foglalkozunk a biztonsággal, ha kampányszerűen veszünk egy biztonsági eszköz, vagy ha úgy teszünk, mintha foglalkoznánk vele, de nem szánjuk rá a szükséges kapacitást és anyagi forrásokat, akkor nem járunk el kellő gondossággal, és a vonatkozó jogszabályoknak sem felelünk meg az elektronikus információbiztonság, a belső kontroll rendszer kialakítása vagy például a létfontosságú infrastruktúra elemek védelme tekintetében.

Tájékoztatás, belső szervezeti kultúra fejlesztése

A biztonság tudatosság növelése irányába tett lépéseket stratégiai befektetésnek kell tekintenünk. Az emberi tűzfal, vagyis a munkatársak tudatos viselkedése az, amelynek kialakítása és folyamatos fejlesztése a legfontosabb, legjobban megtérülő befektetés. Minden érintett csoportnak saját tevékenységéhez kapcsolódóan fel kell hívni a figyelmét a jellemző biztonsági kockázatokra, és kezelésük jó gyakorlataira.

A képzés rendszerét az elvárt elsajátítandó készségek, valamint a számonkérés szintjén célcsoportonként definiálni kell, és az ehhez szükséges erőforrásokat a szervezetnek folyamatosan biztosítania kell dolgozói számára. Ez azt jelenti, hogy egy általános felkészítés mellett az informatikai szakembereket az informatikai üzemeltetési és fejlesztési biztonsági kockázatokra kell felkészíteni, a gazdasági terület dolgozóinak például a beszámoló készítéshez kapcsolódó biztonsági kockázatokra kell felhívni a figyelmet. Vezetők részére pedig jó megoldás gyakorlati példákon keresztül a biztonságra vonatkozó ismeretek átadása vezetői értekezletek napirendi pontjaként.

A belső kommunikációs csatornákon, belső hírlevélben rendszeresen fel kell hívni a kollégák figyelmét az aktuális biztonsági kockázatokra, és választ is kell adni arra, hogyan reagáljon a kolléga, ha ilyen

helyzetbe kerül. A legjelentősebb kockázatokra külön figyelemfelkeltő posztereket készíttethetünk, és a belső hálózaton tájékoztatást tehetünk közzé. Az egyik legnépszerűbb biztonságtudatossági módszer a tájékoztatásra épülő kérdőív volt, amely sikeres megválaszolói között kisebb nyereményeket (pl. toll, egéralátét) sorsoltak ki.

A biztonságtudatossági oktatás eredményességének fő sikertényezője, hogy a hallgatók számára releváns, érdekes és információban gazdag legyen, és megfelelő legyen a motiváció a képzésen való részvételre és az ismeretanyag elsajátítására. Általában olyan vizsgát célszerű a résztvevők számára előírni, amely mögött olyan kérdésadatbázis van, amelyből véletlenszerűen teszi fel a rendszer a kérdéseket. Szintén segíti a tudás bevéséődését, ha a munkatársak tisztában vannak vele, hogy a szabályok megsértésének következménye (szankció), esetleg a betartásának előnye (bónusz) van.

A szervezetek biztonsági szintjét többféle modell szerint lehet értékelni, jelen tájékoztató céljának leginkább a CMM[12] szerinti érettségi modell felel meg:

érettségi szint		képesség	eredmény
0	nem létező	a képesség hiányzik	-
1	kezdeti / ad-hoc	a szervezet felismerte a biztonsági kultúra fontosságát, de nem tudatosan készíti fel a munkatársakat	megindult a biztonsági kultúra fejlesztése
2	ismétlődő	a szervezet vezetése elvárja a biztonsági kultúra kialakítását, de nem törekszenek tervszerűen rá.	törekszenek a jogszabályi megfelelésre
3	szabályozott	a szervezet létrehozta a biztonsági kultúra fejlesztési programot, de korlátozottak a megvalósítás eszközei	jogszabályoknak megfelelés valószínű
4	menedzselt	eredményes a program megvalósítása, tudatosan részt vesznek benne a felhasználók	szabályok szerint folyamatosan megfelelő szinten menedzselt
5	optimalizált	a biztonsági kultúra fejlett, áthatja a szervezetet, és a kultúra fejlesztése beépült a szervezet folyamataiba	mutatószám rendszer segítségével irányított és fejlesztett

[12] Capability Maturity Model (Képesség-érettség modell) A modellben öt fokozat található, amely alapján kiértékelhető egy szervezet fejlettsége a szabványos folyamatok kifejlesztése és követése tekintetében.

Az alapelveket figyelembe vevő, a szükséges biztonsági szint elősegítését szolgáló szervezeti biztonsági kultúrát az alábbi felsorolás szerint célszerű megvalósítani.: A Vasvári György által javasolt, jelen dokumentum bevezető részében ismertetett, egyéni és szervezeti kultúra jellemzők meghatározása segíthet személyre szabni a fejlesztési programot.

1. A személyiségjegyek feltárása: az egyének és a szervezetek személyiségjegyeinek azonosítása történhet kérdőívek kitöltésével, illetve személyes beszélgetések útján. Amennyiben nem anonim módszert alkalmazunk, szükséges a munkatársak hozzájárulása a személyes adatok kezeléséhez.

2. A személyiségjegyek értékelése: az egyének személyiségjegyeinek azonosítása a szervezet számára legkedvezőbb személyiségjegyek figyelembe vételével történhet, ennek függvénye lehet a személyi összetétel módosítása, és a szervezetfejlesztés meghatározása.

3. A teendők megállapítása:az egyének típusjegyeinek fejlesztése a szervet számára legkedvezőbb összetétel elérése érdekében, célirányos terv alapján.

A kockázatkezelés

Tökéletes biztonságot akkor tudunk elérni, ha beszüntetjük az összes tevékenység végzését, azaz nem csinálunk semmit. Belátható, hogy ez ritkán választható megoldás. Azonban a veszélyek és lehetőségek ismeretében eredményesen kezelhetjük a tevékenységek végzéséből fakadó kockázatokat a szükséges kontrollok kialakításával, és működtetésével. A belső kontroll rendszer kialakítása során különféle védelmi intézkedések kombinációjaként alakítják ki a biztonsági szakemberek azt a kontroll rendszert, amely a felső vezetés által felvállalt kockázat vállalási szintnek megfelelő védelmet biztosítja a szervezet számára.

Kontroll alatt az ellenőrzési szakma (COBIT 4.1[13] alapján) olyan irányelveket, szabályzatokat, eljárásokat, módszereket és szervezeti struktúrát ért, amelyet azért hoztak létre, hogy ésszerű bizonyosságot adjanak a szervezeti célkitűzések elérésére, a nemkívánatos események megelőzhetőségére, felismerhetőségére, és helyesbíthetőségére. Ez tehát egy tágabb megfogalmazás, ugyanakkor fontos korlátozásokat tartalmaz: az ésszerű bizonyosság nem jelent teljes bizonyosságot. Annyit jelent, hogy a bevált módszerekkel, és a rendelkezésre álló erőforrások felhasználásával a kontroll kialakítását a legjobb módon végezték el. Másik korlátozás, hogy a kontrollnak a szervezet célkitűzéseit kell szolgálnia, azaz az öncélú biztonsági intézkedéseknek nincs helye egy jól kontrollált szervezetben.

[13] http://www.mtaita.hu/hu/Publikaciok/ISACA_HU_COBIT_41_HUN_v13.pdf

Az információbiztonság szempontjából kockázat alatt az adott információs rendszer, vagy az információ fenyegetettségének mértékét értjük. A kockázat elemzés során fel kell tárni a rendszerek gyenge pontjai (sebezhetőség) és az azt érő fenyegetéseket, majd meg kell határozni a bekövetkezés valószínűségét és a várható kárát.

Az információs rendszer sebezhetősége a rendszer tervezésének, megvalósításának, vagy működésének olyan gyengesége, amely a rendszer elleni támadás során kihasználható, és emiatt fennáll a biztonság sérülésének lehetősége.

Az információs rendszer szempontjából fenyegetésnek tekintünk minden olyan körülményt vagy eseményt, amely az adatok, vagy információs rendszerek biztonságát fenyegethetik. Ide soroljuk például a személyektől eredő támadásokat (pl. számítógépes betörés), és a külső behatásokat (pl. földrengés).

A közigazgatási információs rendszerek működésében tapasztalt tipikus biztonsági kockázatok:

- egy új rendszer a beüzemelést követő néhány héten belül több napra megbénul;
- vezető munkatársak adathordozói illetéktelenek kezébe kerülnek a rajta levő személyes levelezéssel, nem nyilvános adatokkal;
- a munkájában el nem ismert rendszergazda az üzemeltetési feladatok naprakész pontos dokumentálása nélkül távozik;
- a munkatársak áthelyezésüket követően is hozzáférnek a korábbi szervezeti egységük anyagaihoz.

Mi okozza a biztonsági kockázatok növekedését:

- az informatikai szolgáltatásoktól és az adatkapcsolat folyamatosságától való függés;
- a szándékos károkozás megnövekedett motivációja;
- a nagy informatikai beruházást is tartalmazó projektek kudarcai;
- a hardver, illetve szoftver eszközök meghibásodása;
- a virtuális vállalatok terjedése;
- az időjárás változása.

Az információbiztonsági kockázatok kezelésének négy alapmódszere van:

- a tevékenységek beszüntetése (kockázat megszűnik);
- a tevékenység kockázataira biztosítás kötése (kockázatot áthárítottuk a biztosítóra);
- a felelős vezető a kockázatot megismeri és nem tart további intézkedést szükségesnek (kockázatot a szervezet felvállalta);
- a felelős vezető védelmi intézkedéseket (kontroll) valósít meg, vagy szüntet meg (kockázati válasz meghatározása és megvalósítása).

Akkor tekintjük jónak a védelmi rendszert, ha egy kellően nagy időintervallumon belül – ami jellemző a szervezet tevékenységére – a kockázatok csökkentésére fordított költségek (védelem) arányosak a kockázat bekövetkezéséből fakadó várható kár mértékével.

Megfelelés az előírásoknak

Megfelelés (compliance) alatt a közigazgatási szervezetek kötelezettségei bemutatásának, és a kötelezettségteljesítés bemutatásának képességét értjük, amely által a jogszabályi, hatósági, belső szabályozásból fakadó, illetve a szerződéses előírásokat, elvárásokat folyamatosan teljesíti.

A követelmények azonosítása és a megfelelés biztosítása a belső védelmi vonalak részét képező belső kontroll funkció, amely elősegíti a szervezet prudens, megbízható az előírásoknak megfelelő működését. Feladata a megfelelőséget veszélyeztető kockázatok azonosítása és kezelése.

Az előírásoknak megfelelés érdekében az összes szakterületnek együtt kell működnie az alábbi tevékenységek végrehajtásában. Szervezetenként eltérő, hogy mely szakterület irányítja, illetve végzi ezeket:

- megfelelőségi kockázatok meghatározása; mérése, kontrollkörnyezet értékelése;
- megfelelőségi program tervezése és megalkotása (felülvizsgálata);
- szervezet megfelelőségi tevékenységének figyelemmel kísérése;
- felügyeleti és hatósági kapcsolattartás;
- tanácsadás a felső vezetés számára;
- munkatársak képzése;
- pénzmosás és csalás megelőzés;
- összeférhetetlenség kezelése.

Szervezetek felelős irányítása és a biztonságirányítás

A vállalatirányítás fogalmát – az OECD definíciója szerint – úgy határozhatjuk meg, hogy mindazon irányelveknek, folyamatok és vezetési gyakorlatoknak az összessége, amelyek segítségével a társaságok igazgató tanácsa, vagy felső vezetése a társaságot igazgatja és kontrollálja. Kiterjed a szervezetben érintettek (ügyfelek, menedzsment, alkalmazottak, tulajdonosok, kormányzat, helyi közösség) közötti jogok és felelősségek megosztására. Az állami tulajdonú társaságokra is alkalmazzák az OECD ajánlásait, például az MNV Zrt. a Felelős vállalatirányítási ajánlásait ez alapján készítette el. Ezeknek az irányítási gyakorlatoknak része a működési és biztonsági kockázatkezelés is.

Az információbiztonsági irányítás fogalomköre a CISM ISACA tanúsítványok megszerzéséhez szükséges ismeretanyag részévé vált 2004-ben. Az informatikai irányítási és kontroll módszertanokba az informatika feletti irányítás gyakorlatainak szélesebb körű elterjedését, az informatikai irányítás modelljének beépülését 2008-ban a COBIT 4.1, majd 2011-ben a COBIT 5 hozta meg, amely a hazai információbiztonsági szabályozásba is beépült. Szintén tartalmazza a témakör ismeretanyagainak jelentős részét az ISC2 CISSP nemzetközi vizsgája, ez szakértői szintű vizsga (nem vezetői). További nemzetközi vizsgák is léteznek, ezek az általánostól (pl. CompTIA Security+) a nagyon speciális részterületig (pl. CISCO CCNA Security), illetve a védelmi szakember jellegű vizsgától a támadó szakember – sérülékenység vizsgáló - biztonsági vizsgákig terjednek. A vizsgákra épülő tanúsítványok mutatják a szakmai iránti elkötelezettségek, igazolják a szakismeretet és bizonyítják, hogy tulajdonosuk képes értéket teremteni a szervezet számára.

Jelen fejezet „Információbiztonság irányítása" alfejezetében felsoroltuk a biztonságirányítás teendőit, alapkövetelményeit. Azonban sok esetben a szervezetek vezetői nem tudják pontosan meghatározni – szakszerű támogatás, és vezetői biztonságtudatosítási képzések hiányában – hogy mit is értenek információ biztonsági alapkövetelményeken. Ennek következményeként gyakran már csak akkor történnek lépések, amikor már késő. Valamilyen nem várt rendkívüli biztonsági esemény ébreszti rá a vezetést arra, hogy megfelelő vezetői szinten és a kockázatokkal arányos intézkedésekkel szükséges kezelni az információbiztonsági kockázatokat. A jelenlegi környezetben, ahol a szervezet számára rövid távú célok kerültek leginkább meghatározásra, a rövid távú megtérülést felmutatni nem tudó, vagy a megtérülésüket számszerűsíteni nem tudó beruházások háttérbe kerülnek. Ha az a kérdés, hogy új informatikai szolgáltatást valósítsunk meg, vagy a teljes rendszer működésének biztonságát növeljük, gyakran az előbbire esik a döntés. A biztonsági vezetők feladata, hogy a szervezet vezetőjét döntési helyzetbe hozzák a működést veszélyeztető kockázati tényezők, és a kezelésük legmegfelelőbb módjának tudatosításával. Ekkor hozható felelős döntés – a szervezet kockázattűrő képességének ismeretében – az általuk felvállalt kockázat mértékéről.

Biztonsági szabályozási és kontroll rendszer

Az önállóan alkalmazott biztonsági funkciók kialakítása és fenntartása aránytalanul drága, ugyan akkor nem biztosít hatékony védelmet. A biztonság kialakítását rendszer szinten kell kialakítani, azaz az informatikai kontrollok mellett a fizikai és humán kontrollokat egyaránt alkalmazni kell, törekedve a kontrollok egyenszilárdságára.

A biztonsági szabályozási és kontroll rendszert integrált módon, bevált szabványok és ajánlások felhasználásával kell megvalósítani. Az így kialakított védelmi rendszert információbiztonság irányítási rendszernek (IBIR) nevezzük.

Az információbiztonsági szabályozási rendszer felépítése háromszintű:

1. a szervezet vezetése által megfogalmazott irányelvek, magas szintű elvárások (információbiztonsági irányelv / politika, IBP);
2. az információbiztonsági irányelvek megvalósítását meghatározó operatív szabályozás, (információbiztonsági szabályzat);
3. az egyes gyakorlati kérdések részletes szabályozását tartalmazó eljárásrendek, munkautasítások, ellenőrző listák, amelyek az IBSZ részeként lehetnek kötelezőek, vagy ajánlottak.

A kontroll rendszer megvalósítása során, a kockázatok ismeretében három alapvető kontroll típus kombinációját kell alkalmazni:

- megelőző kontroll: olyan ellenőrzési eljárás, amely megelőzi, vagy korlátozza egy hiba bekövetkezését, mint például a fizikai hozzáférés megakadályozása, vagy a szoftverek jogosultságainak korlátozása;
- feltáró kontroll: olyan ellenőrzési eljárás, amely lehetőség szerint mielőbb feltárja a bekövetkezett hibákat, hiányosságot, mint például az ellenőrző összeg a számítási műveleteknél;
- helyesbítő kontroll: olyan ellenőrzési eljárás, amely a bekövetkezett hibákat, hiányosságokat segít megszüntetni, hatásukat csökkenteni , az informatikai katasztrófa-helyreállítási terv alapján.

A kontroll rendszer tervezése során minden tevékenységben rejlő kockázatot (benne rejlő kockázat) a szervezet vezetője által elfogadhatónak tartott szintre kell csökkenteni.

Biztonsági monitoring

Amikor egy új házat felépíttetünk, természetes, hogy nem csak a funkcionális követelményeket határozzuk meg, hanem elvárjuk azt is, hogy az folyamatosan karbantartható legyen, és a szükséges védelemmel el legyen látva az illetéktelen látogatókkal szemben. Az informatika területén viszont gyakran szembesülhetünk azzal, hogy egy új szolgáltatás bevezetése során a kifejlesztés és telepítés végeztével magunkra hagy a szállító. A házépítés analógiájával élve ez azt jelenti, hogy lakható a ház, de egy csavarhúzó, vagy pajszer segítségével másodpercek alatt betörhetnek.

A telepítés pillanatában ismert és elvárható biztonsági beállítások elvégzését a rendszer telepítőjétől kell elvárni, azonban önmagában ez nem nyújt sokáig védelmet. A védelmi rendszerbe folyamatosan be kell illeszteni az újonnan megjelenő védelmi szolgáltatásokat és intézkedni kell a felmerülő kockázatok kezeléséről.

Általában a gyakorlatban a biztonságot annak hiányával mérjük, az adott időszakban bekövetkezett rendkívüli információbiztonsági események száma megmutatja, hány alkalommal sérülhetett a biztonság. A feltárt belső visszaélések száma jó mutató lehet az etikus és biztonságtudatos magatartás

szintjének megítéléséhez. Ezek a mutatók azonban nem tekinthetők objektívnek. A rendkívüli események számát befolyásolja például, hogy milyen az ellenőrzési rendszerünk megbízhatósága, azaz, ha magas színvonalú a hálózatfelügyeleti rendszerünk, akkor észreveszünk minden lényeges biztonsági eseményt, ezáltal a feltárt biztonsági események száma megnő, de a biztonság kevésbé sérül . Ugyancsak befolyásolja a nyilvántartott biztonsági események számát, hogy minden eseményt bevezetnek-e a nyilvántartásba.

A cél az, hogy mind a rendszerek működését, mind a bekövetkezett biztonsági eseményeket figyelemmel kísérjük. Erre egyrészt a hagyományos rendszer- és hálózatfelügyeleti szoftverek használata, másrészt a biztonsági események elemzéséhez központi naplógyűjtő rendszer és naplóelemzési jelentések kialakítása szükséges, amely a lényeges kockázatok szoros felügyeletét teszi lehetővé. A fejlett biztonsági monitoring része ma már az automatikus sérülékenység vizsgáló eszközök alkalmazása, amelyek segítik a rendszerek naprakész frissítését, és javaslatot tesznek a szükséges változtatások telepítésére.

Új rendszerek bevezetésének tervezésekor nem szabad elfelejtkezni a biztonsági kontroll és monitoring funkciók szükségességétől. Korszerű szervezetirányítási rendszerek (pl. SAP, ORACLE) olyan beépített kontrollokat tartalmaznak, amelyek bizonyos feltételek esetén (pl. 10 MFt feletti tranzakció, törzsadat változás) azonnali, vagy napi jelentést küldhetnek a felhasználó felettesének. A biztonsági, vagy ellenőrzési terület igényeit is képesek ezek a rendszerek kielégíteni, ún. folyamatos kontroll monitoring funkciókkal, amelyek lehetővé teszik ellenőrzési szempontok minden egyes tranzakción való valós idejű futtatását.

A tervezéskor igényelt biztonsági funkcionalitás lényegesen olcsóbban megvalósítható, mint annak utólagos fejlesztése, vagy kiegészítő funkcióként való megvalósítása.

Adatgazdai szerep, Adatok biztonsági osztályozása

Egy információs rendszer adatgazdájának a szervezetnek azt a vezetőjét, vagy a vezetője által felhatalmazott munkatársat tekintjük, aki jogosult az információs rendszerben kezelt adatok minősítésére, és biztonsági osztályba sorolására.

A biztonsági osztályba sorolás olyan értékelési tevékenység, amely során a kockázat mértékét az adatok értékét, az adatok kezelésének módját, körülményeit, a védelem eszközeit figyelembe véve meghatározzák a védelmi szintet. A közigazgatás keretén belül védelmi szinteket az Ibtv. végrehajtási rendelete határoz meg.

Az információs rendszerek védelmi intézkedéseit annak megfelelően kell meghatározni, hogy azokban tárolt, feldolgozott vagy közvetített adatokat milyen biztonsági osztályba sorolták az adatgazdák.

A biztonsági osztályba sorolás során meghatározzák, hogy milyen kategóriába (pl. alacsony, fokozott, kiemelt) kerülnek bizalmasság, sértetlenség, és rendelkezésre állás szempontjából. Ezen szempontok aggregálása során a legszigorúbb kategóriát kapja maga az információs rendszer. Azaz amennyiben bizalmasság, és sértetlenség szempontjából alacsony kategóriába soroltuk az adatokat, de a rendelkezésre állás szempontjából közepes kategóriába került, akkor a rendszert közepes kategóriába kell sorolni.

A biztonsági osztályba sorolás során ugyanazon kategóriába sorolt vagyonelemeket célszerű hasonló védelemmel ellátni. Az ingatlanok, és az információs rendszerek védelme esetén is beszélhetünk különböző védelmi szintről. A védelmet ezek szerint biztonsági zónákra lehet osztani. Így beszélhetünk fő kategória szerint nyilvános zónáról, korlátozott hozzáférésű, és fokozottan védett zónáról. Esetenként ezeken belül további kategóriák kialakítása indokolt lehet.

Folyamatos működés biztosítása

A szervezetek folyamatos működési biztonsága a szervezetek alapvető érdeke. A közszféra szervezetei esetén ez jogszabályi kötelezettség is.

A szervezetek működésfolytonosságának biztosítására külön irányítási rendszert kell kialakítani, ez a működésfolytonossági irányító rendszer (BCMS), amelynek fő része a működésfolytonossági terv (BCP). A BCMS célja a szervezet kritikus üzleti folyamatainak legalább minimálisan elvárt szinten való fenntartása rendkívüli helyzetben is. Ezáltal a szervezet működési folyamataival kapcsolatos kockázatokat tervezett módon képes kezelni azokban az előre meghatározott esetekben (kockázati forgatókönyv), amelyekre a működésfolytonossági tervek elkészültek, és a működtetésük feltételeit kialakították. A tervezés során feltárt szükséges intézkedéseket a tervek megvalósíthatóságára való felkészülés szakaszában kell megvalósítani. Látható, hogy a folytonosságtervezés nem egy egyszeri tevékenység, alapos előkészítést és felkészülést követően, a szervezeti változtatásokat követve és a működéshez használt környezet változásait figyelembe véve rendszeresen felül kell vizsgálni, és szükség szerint módosítani kell.

A működésfolytonossági tervezés főbb lépései:

- működésfolytonosság irányítási rendszer kialakítása (szabályozás, szervezet);
- működési folyamatok feltérképezése;
- működési folyamatok kiesésének hatásvizsgálata (BIA): meg kell becsülni a kiesés várható hatását, meg kell határozni a folyamatok fontosságát, a helyreállítás sorrendjét;
- kritikus folyamatokat veszélyeztető kockázatok elemzése: jellemző kockázati forgatókönyvek bekövetkezése esetén szükséges teendőket el kell végezni, megelőző intézkedések újra kell vizsgálni;

- a működésfolytonossági tervek elkészítése;
- a tervek működtetéséhez szükséges felkészülés (pl. oktatás, katasztrófa-helyreállítási tervek [DRP]), és intézkedések végrehajtása;
- a tervek tesztelése;
- a tervek életbe léptetése.

A működésfolytonossági kezdeményezések fontos eleme a kritikus informatikai szolgáltatások folytonosságának biztosítása, amelyet a szervezet informatikai részlege, illetve informatikai szolgáltatója által kidolgozott és tesztelt informatikai katasztrófa-helyreállítási tervek (DRP), és azok működtetését segítő folyamatok biztosítják, amelyeket a működésfolytonosság tervezéshez szükséges felkészülés keretében kell megvalósítani. Fontos, hogy a rendszerek és szervezeti folyamatok változásait figyelembe véve módosítani kell a terveket.

A tervezés során célszerű a KIB 25 és KIB 28 ajánlások figyelembe vétele, és a vonatkozó ISO szabványok, különösen az ISO 22301:2012 alkalmazása.

Belső ellenőrzés szerepe – IT audit és tanácsadás

A közszféra belső kontroll rendszerét a költségvetési szervek esetén a 370/2011. kormányrendelet határozza meg. A közszféra gazdasági társaságai esetén is javasolt ennek az alkalmazása, mivel előremutató gyakorlatokat tartalmaz, és sok esetben az állami gazdasági társaságok belső kontroll gyakorlata kevésbé fejlett. A belső kontroll rendszerek kialakítása során a vezetői ellenőrzés, a folyamatokba épített ellenőrzés, és az informatikai rendszerekbe épített ellenőrzések megfelelő kiválasztásával történik, a szervezetre értelmezhető kockázatok várható hatásának figyelembe vételével.

A szervezeteknél a belső kontroll rendszerben részt vevő szervezeti funkciók feladatait pontosan meg kell határozni, és külön kell választani. Az információbiztonság szempontjából például a szabályozási feladat a Biztonsági terület feladatkörébe tartozik, az üzemeltetési tevékenység az informatikai üzemeltetés feladatkörébe, az üzemeltetés biztonságának felügyelete szintén a biztonsági terület feladata, és végül a szabályszerűség, és eredményesség vizsgálata a belső ellenőrzés feladatkörébe. A következőkben a belső ellenőrzés szerepét mutatjuk be az információbiztonság szempontjából.

A számítástechnika alkalmazásának első évtizedeiben az ellenőrzési szakterület a számítástechnikai rendszerektől függetlenül zajló üzleti tranzakciók nyomon követésével foglalkozott, fő célja az adatokkal való visszaélés megelőzése volt. A feladat a nyolcvanas évektől kezdve folyamatosan bővült, mivel a tranzakciók egyre nagyobb része zajlik a számítógépes rendszerekben. Megerősödött a számítógépes rendszerekben zajló tranzakciók biztonságának fenntartására vonatkozó igény

az adatok biztonságának igénye mellett. Ennek érdekében az ellenőrzések során a vizsgálatokat eltérő mélységben végzik a vizsgálat céljának megfelelően:

- A megfelelőségi teszt (compliance) azt vizsgálja, hogy a vizsgálat tárgya összhangban van-e a rá vonatkozó jogszabályokkal, szabályzatokkal, szabványokkal, szerződésekkel.
- A lényegi teszt (substantive) azt vizsgálja, hogy egy megadott időszakban milyen minőségben működött a kontroll rendszer. Információs rendszerben adott tranzakciók meglétére, pontosságára, minőségére, illetve teljességére vonatkozik.

Általában gyakoribbak és olcsóbban a megfelelőségi vizsgálatok, azonban ezek csak jól működő kontroll rendszerek esetében alkalmazhatóak. Ha nem találja az ellenőrzés kielégítőnek a kontroll rendszer működését, akkor széles körű lényegi tesztelést kell végezni a kockázat pontos mértékének meghatározása érdekében.

Az ellenőrzés mellett végezhet a belső ellenőrzés szakértői tevékenységet is abban az esetben, ha ez nem összeférhetetlen az ellenőrzési feladataival. Általában szakmai véleményt mondhat szabályzatokról, rendszerek követelményspecifikációjáról, vagy felmerült biztonsági kérdésekről. Szükség esetén külső szakértőt vonhat be, ha nem áll rendelkezésre a szaktudás, vagy a kapacitást.

Meg kell említenünk az ellenőrzési kockázat fogalmát, amely annak a kockázata, hogy egy szakszerűen megtervezett és végrehajtott informatikai rendszerellenőrzés során egy lényeges hiányosság feltárása nem történik meg. Ez minden ellenőrzési tevékenység velejárója. Az oka lehet, hogy az ellenőrzést a sokaság egy részén mintavételezéssel végezték, nem vizsgáltak meg minden elemet, illetve a vizsgálati módszert nem megfelelően tervezték meg, vagy valósították meg.

A számítógéppel támogatott ellenőrzési módszerek (CAAT) segítségével növelhető az ellenőrzési tevékenységek hatékonysága és eredményessége. Ilyen eszköz például egy szakértői rendszer, tesztadat generáló rendszer, stb.

Kiszervezés

Az elmúlt évtizedben egyre több szervezet, intézmény szervezi ki az alaptevékenységéhez szorosan nem kapcsolódó tevékenységeket más szervezetekhez. Ezt feladat vagy erőforrás kiszervezésnek, „outsourcing”-nak nevezzük. Előnye, hogy a szervezetek magas színvonalú, az elvárásaiknak megfelelő szolgáltatást kapnak versenyképes költség szinten, amely összességében alacsonyabb, mintha saját maguk alakították volna ki, és végeznék el a tevékenységet.

Fontos tudni, hogy a feladat kiszervezése nem jelenti a felelősség kiszervezését, az elsődleges felelősség továbbra is a szervezet vezetőjét vagy menedzsmentjét terheli, amelyet később polgári peres úton a szerződött cég felé is érvényesíthet.

Az kiszervezés lényege, hogy bizonyos feladatokat vagy annak egy részét átadja egy másik, erre specializálódott szervezetnek, vagy vállalkozásnak. Legfontosabb előnyei:

- A szolgáltatások rendelkezésre állását a szolgáltató biztosítja.
- Az erre specializált szervezet hatékonyabb, rugalmasabb és biztonságosabb szolgáltatást garantálhat.
- A költségek előre tervezhetőek.
- Nincs jelentős kialakítási (beruházási) költség.
- Az amortizáció nem terheli a szervezetet.
- A munkaerő felvétele, és a munkaerő bérköltsége nem a megrendelőt terheli.
- A munkatársak képzése, helyettesítése is a szolgáltató feladata.
- A szolgáltató érdekelt a korszerű műszaki megoldások megvalósításában.

A kontroll rendszerrel szemben támasztott elvárásokat a szervezet harmadik féllel kötött szerződéseibe is be kell építeni; így különösen informatikai szolgáltatás igénybevétele esetén elő kell írni a szolgáltatási szerződés, vagy szolgáltatási szint megállapodás részeként az általános (pl. rendelkezésre állás) és speciális (pl. kommunikációs csatornák titkosításának módja) biztonsági követelményeket, azok mérésének módszerét, gyakoriságát, és a jelentéskészítés módját.

Fel kell hívni a szolgáltató figyelmét, hogy a megrendelőre érvényes jogszabályi követelményeket neki is és az alvállalkozóinak is be kell tartania. Különösen az informatikai kiszervezésekkel kapcsolatban fontos a szükséges biztonsági intézkedések megtervezése és folyamatos működtetése (pl. naplóállományok gyűjtése és elemzése, személyes adatok védelme).

A közszférában bizonyos informatikai szolgáltatások nyújtása esetén már a jogalkotó élt a kiszervezés lehetőségével, sőt esetenként (pl. Nemzeti Távközlési Gerinchálózat, NTG) kötelezővé is tette ilyen szolgáltatások igénybevételét. Ebben az esetben a szolgáltatások igénybevételének feltételei jellemzően szabályozottak, de fontos a szervezet speciális igényei alapján áttekinteni, hogy szükséges-e azok módosítása, vagy kiegészítése.

Ha még olvasna erről:

http://www.pszaf.hu/data/cms2151158/Kiszervezesi_palyazat_PRAUDIT_2010_04_07_v10.pdf

Munkaügy szerepe

Az emberi tényező

Az informatikai rendszerekben általában a legnagyobb kockázati tényező az ember. Nem csak a szervezetben informatikai rendszert használó munkatársak, hanem a rendszerek tervezői, megvalósítói, üzemeltetői, a külső szolgáltatók munkatársai, és mindazok, akik valamilyen módon hatással vannak a rendszerre. A kockázat fakadhat hozzá nem értésből, véletlen hibából, jó szándékból, vagy károkozás céljából.

A személyek által okozott adatvesztés jellemző okai a következőek:

- Gondatlanság: például a Horváth Gergely Krisztiánnak küldendő levelet ugyanannál a szervezetnél egy Horváth Gergely nevű másik munkatársnak küldi valaki, annak, aki nem lenne jogosult a levél tartalmának megismerésére.
- Fokozott terhelés, családi problémák, stressz: stressz következtében csökkenhet a koncentráló-képességünk, és hibát vétünk egy adatrögzítés során, vagy a törlendő állományok helyett mást törlünk le.
- Ismerethiány: új szabályozás, vagy módosult rendszer működés ismeretének hiányában hibásan rögzítünk egy parancsot, vagy nem minden berögzített adatot mentünk el.
- Hibásan megtervezett folyamatok, a kontrollok hiánya: általában új rendszerek elindulásakor fordul elő, hogy nem minden lényeges és ésszerű kontrollt építettek be a rendszerbe, például adatrögzítéskor hagyja a rendszer, hogy hibásan rögzítsük az ügyfél nevét, ha azt a törzsadatokkal nem veti össze.
- Hibás rendszerműködés: számos lehetőség van a rendszerek működése során a hibára, például egy lejárt tartozás késedelmi kamatszámításakor nem megfelelő kamatlábbal számol.
- Szándékos szabályszegés: például jelentős munkát igénylő, de kevéssé kontrollált tevékenységek elvégzése elmaradhat, anyagi előnyért cserébe egy felhasználó információt adhat ki, vagy a rendszer beállításait módosíthatja.
- Hiányos biztonságtudat: gyakran a valós veszélyek fel nem ismerése vezet el egy biztonsági eseményhez. Például egy parkolóban talált memória kártya hivatali gépbe való beolvasása kártevő szoftvert képes a rendszerbe juttatni a felhasználó számára észrevétlen módon.
- Túl komplikált kezelés: egy információs rendszerben általában a bonyolultsággal arányosan nő a hibák száma, például, ha több aloldalon kell az adatokat rögzíteni, akkor elmaradhat az oldal elmentése, vagy kimaradhat 1-1 lépés.
- Szándékos károkozás: egy konfliktus helyzet (pl. fegyelmi eljárás, mások előtti megalázás) következtében az elégedetlen munkatár, a megfelelő jogosultságok, vagy a helyzet adta lehetőségek kihasználásával jelentős kárt képes okozni.

Mindezek felhívják a figyelmet arra, hogy a munkaügy, vagy más néven a humán erőforrás kezelési szakterület munkája nem elhanyagolható része az információbiztonságnak. A munkatársak megfelelő kiválasztása, felkészítése, motiválása, és szankcionálása ezen okokat jó eséllyel képes megelőzni, illetve a hatását csökkenteni.

Alkalmazást megelőző átvilágítás

A munkaügyi funkció és a vezetők felelőssége, hogy a felvételi eljárás során egy pozícióra ne alkalmazzanak olyan munkatársat, akinek domináns személyiségjegyei a munkakörtől elvárt képességekre nem igazán teszik alkalmassá. A biztonság megvalósítása szempontjából ez is megelőző intézkedés.

A munkaügyi és a biztonsági szakterületek közös feladata meggyőződni a jelölt korábbi tevékenységéről, eredményeiről. Ennek mélysége eltérő, általában az adott pozíció jelentőségével arányos. Beosztotti, kevés felelősséggel járó munkakörben elég lehet erkölcsi bizonyítványt kérni és elbeszélgetni a jelölttel, következő lépés lehet például referencia levelet kérni korábbi vezetőitől, és felhívni a referenciát adó vezetőt, hogy megerősítse a levélben leírtakat.

A közigazgatásban nemzetbiztonsági átvilágítást követel meg a törvényhozó a fontos beosztásban dolgozó munkatársaktól. Ezen a körön kívül felső vezetői, vagy fokozott kockázattal járó pozíciókban akár magánnyomozói átvilágítást is végeztetnek azért, hogy a legmegfelelőbb jelöltet válasszák az adott pozícióra, extrém esetben előfordulhat a hazugságvizsgálattal egybekötött felvételi beszélgetés is.

Felelősségek szétválasztása és egyéb humán kockázat csökkentési módszerek

Az emberi tényező okozta kockázatok csökkentésének viszonylag egyszerűen kivitelezhető módszere az, hogy a feladatok szervezésével, és kontroll pontok beépítésével csökkentjük az egy személy tevékenységéből fakadó kockázatok mértékét.

A négy szem elvének alkalmazása azt jelenti, hogy az információs rendszerben a magasabb kockázatú tevékenységeket egyetlen felhasználó nem tudja végigvinni . Adott esetben rögzítheti az adatokat, előkészítheti a tranzakciót, de a végrehajtáshoz egy másik felhasználó (pl. az osztályvezető) jóváhagyása szükséges.

Az összeférhetetlen tevékenységek meghatározása és megszüntetése segítségével szintén megelőzhetjük a károkozást. Példának okáért, ha a pénzügyi területen a pénztáros munkatársnak utalványozási joga is van, akkor a két tevékenység kontroll nélkül összeférhetetlen.

Fokozott kockázatú területen elterjedt megoldás a kötelező szabadság elrendelése. Két hét szabadság elég hosszú idő arra, hogy kiderüljön, mennyire képes helyettesíteni a szervezet az adott munkatársat (kulcsember kockázat), illetve ha visszaélt valamivel, akkor várhatóan ennyi idő az esemény feltárható.

Ha a szervezet létszáma nem teszi lehetővé a feladatok teljes körű szétválasztását, akkor kiegészítő kontrollokkal csökkenthető a kockázat mértéke. A tevékenységek kellő részletességgel való dokumentálása segíti az ellenőrzést. Ha a tevékenységeket az információs rendszerek nem módosítható módon naplózzák, akkor teljes bizonyosságot szerezhetünk a naplóban szereplő eseményekről.

Biztonságtudatos viselkedést elismerő motivációs rendszer

A biztonsági kultúra megteremtése a vezetői példamutatáson múlik leginkább. Ennek része az, hogy milyen módon képes a vezetés erősíteni a biztonságtudatos magatartást.

Gyakori kérdés és biztonsági kockázat a számítógéphez való hozzáférés megakadályozása. Műszaki megoldásokkal természetesen automatikussá lehet tenni a képernyő lezárását, azonban itt is fontos, hogy a munkavégzést ne akadályozzuk, ezért általában 10 percre szokták állítani, és a felhasználókra bízzák, hogy amikor elhagynák a munkahelyüket, akkor zárják le a képernyőt. Ez sokszor nem történik meg. Az adott munkatárs számítógépes jogosultságaitól függően akár nagy kockázatot is jelenthet: ügyfélszolgálaton, vagy pénzügyi területen dolgozó munkatárs érzékeny és személyes adatokhoz fér hozzá, ezért itt fokozottan be kell tartatni az alapvető információbiztonsági lépéseket is.

Egy nagy informatikai szolgáltató vállalat biztonsági vezetése például bevezette azoknak a jutalmazását, akik feltárják a biztonságot veszélyeztető viselkedést, illetve más kockázatokat. Ezt nem az 1950-es évek besúgó rendszereként kell elképzelni, hanem olyan gyakorlati megoldásként értékelni, amely játékos, egyben jelentős szóbeszédet keltett a szervezetben, így a kollégák gyorsan elsajátították a biztonsági lépéseket. Egy nagyobb informatikai részlegben például aki anélkül hagyta ott a közös irodateret, hogy jelszóval védte a számítógépe képernyőjét, annak a nevében bárki küldhetett egy elektronikus levelet egy központi címre, és ezáltal jogosulttá válik arra, hogy a hibát elkövető munkatárs egy Túró Rudival ajándékozza meg. Rövid idő alatt beépült kollegák rutinjába a képernyők zárolása, ha felálltak az asztaltól.

Kisebb szervezetnék történt meg, hogy az egyik biztonságtudatos kollega úgy hívta fel munkatársai figyelmét, hogy a lezáratlan gépeken megnyitotta a rajzoló programot és egy halálfej jelet rajzolt a képernyő közepére. Ez is eléggé mély benyomást okozott a munkatársaknak, és segített számukra tudatosítani a képernyők jelszóval való védelmének szükségességét.

Biztonságot veszélyeztető tevékenységek következetes szankcionálás

Közvetve a nagy szolgáltató vállalatok léte függ attól, hogy képesek-e az ügyfeleik bizalmát megszerezni és megtartani. A bizalom fontos összetevője a biztonság kívánatos szintjének fenntartása. Jogosan várhatja el egy ügyfél, hogy a szervezet és annak munkatársai érzékeny és személyes adatait csak az arra jogosult munkatársak, és csak a munkavégzésükhöz szükséges mértékben ismerik meg. A bizalmat alapvetően áshatja alá, a fenti példánál maradva, ha a munkatársak a számítógépük képernyőjét nem zárják le, vagy a felhasználónevüket átadják másnak, esetleg az íróasztalukon érzékeny információkat tárolnak.

Alapvetően a pozitív motiváció, azaz a helyes viselkedés jutalmazása humánusabb és eredményesebb módszer. Mégis, a pozitív motiváció sem hatékony, ha nincs szankcionálása a jelentős kockázatot jelentő szabálysértő viselkedésnek. Kisebb szankció lehet a szabályt megsértő munkatárssal való felső vezetői elbeszélgetés, vagy továbbképzésére küldése. További lehetőségeket a Munka törvénykönyve tartalmaz. Gyakorlatban a szóbeli figyelmeztetés, írásbeli figyelmeztetés, visszaminősítés / lefokozás / áthelyezés, illetve a felmondás jöhet még szóba, ebben a sorrendben.

Az egyik szervezet gyakorlata, ahol kiemelt fontosságú a biztonság, egy szabályozott szankcionálási folyamat, amelyet a humán szakterület folytat le: három írásos figyelmeztetést adnak a belső szabályokat megsértő munkatársaknak és ezt követően a munkatársakat elbocsátják, ha ismét szabályt sértenek.

Jogszabályok

ELEKTRONIKUS INFORMÁCIÓBIZTONSÁGOT ÉRINTŐ FONTOSABB JOGSZABÁLYOK A KÖZSZFÉRÁBAN (2013.06.30-án hatályos)

1 Melléklet

A közszféra jelentős része számára kötelező a költségvetési szervek belső kontrollrendszeréről és belső ellenőrzéséről szóló 370/2011. (XII. 31.) Korm. rendelet (továbbiakban: Bkr.), valamint ezek alapján az államháztartásról szóló, többször módosított 1992. évi XXXVIII. törvény (a továbbiakban: Áht.), az államháztartás működési rendjéről szóló, többször módosított 292/2009. (XII.19.) Korm. rendelet (a továbbiakban: Ámr.), előírásainak megfelelően, mint a közpénzek felhasználásában, az állami vagyon kezelésében résztvevő szervezet köteles belső ellenőrzési rendszert működtetni abból a célból, hogy a szervezet vezetője számára bizonyosságot nyújtson az általa kiépített és működtetett belső kontrollrendszerek megfelelőségét illetően.

Az adatkezelőkre vonatkozóan számos jogszabály tartalmaz előírásokat. Az állami és önkormányzati szervezetek esetében 2013 hozta meg az áttörést a részletes szabályozásban:

- Magyarország Kiberbiztonsági Stratégiája rögzíti, hogy az elsődleges cél a kibertérben jelentkező és a kibertérből érkező fenyegetések és az ezzel járó kockázatok kezelése, az ehhez szükséges kormányzati koordináció és eszköztár erősítése a megelőzésre épülő hatékony védelmi intézkedéseken keresztül.
- Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényre (továbbiakban: Ibtv.) és végrehajtási rendeleteire (továbbiakban: Vhr.) azon szervezetek is építhetik az információbiztonsági kezdeményezéseiket, akikre nézve ez a szabályozás nem kötelező. Az Ibtv. hatálya alá nem eső szervezetek használhatnak nemzetközi és hazai szabványokat, ajánlásokat is. A minősített adatok kezelését a 2009. évi CLV. törvény szabályozza, amely fokozottan megköveteli az informatikai rendszerekben kezelt minősített adatok védelmét.

A minősített adatok kezelését a 2009. évi CLV. törvény szabályozza. Az informatikai rendszerekben kezelt minősített adatok védelmét fokozottan megköveteli.

Az adatok kezelésének, gyűjtésének, továbbításának jogszabályi alapjait az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény fekteti le.

309/2011. (XII.23.) Kormányrendelet a központosított informatikai és elektronikus hírközlési szolgáltatásokra vonatkozóan határoz meg központi kontroll feladatokat.

A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény a kritikus infrastruktúra védelmének alapvető szabályozása. A kapcsolódó kormányrendeletekkel együtt az infrastruktúra elemek kijelölését, védelmének szabályait és hatósági ellenőrzését tartalmazza. A közszféra gazdasági társaságaira további jogszabályok vonatkoznak:

A gazdasági társaságokról szóló 2006. évi IV. törvény;
A cégnyilvánosságról, a bírósági cégeljárásról és a végelszámolásról szóló 2006. évi V. törvény;
Az állami vagyonról szóló 2007. évi CVI. törvény nevesíti az állami adatvagyon védelmét;
A köztulajdonban álló gazdasági társaságok takarékosabb működéséről szóló 2009. évi CXXII. törvény;
A számvitelről szóló 2000. évi C. törvény.

További információk

TOVÁBBI HAZAI ÉS NEMZETKÖZI FORRÁSOK A BIZTONSÁG TUDATOSÍTÁS TÉMAKÖRÉBEN

2

Melléklet

Nemzetközi szervezetek, módszertanok, útmutatók rövid ismertetése és a kapcsolódó hivatkozások:

- Európai Hálózatbiztonsági Ügynökség (ENISA) URL: http://www.enisa.org
- Gazdasági Együttműködési és Fejlesztési Szervezet (OECD), információbiztonsági bizottság, URL: http://www.oecd.org/internet/ieconomy/informationsecurityandprivacy.htm
- SANS biztonság tudatosító honlap, URL: https://www.securingthehuman.org/ouch

Az Állami Számvevőszék informatikai ellenőrzési módszertana (2004):

ÁSZ Módszertan az informatikai rendszerek kontrolljainak ellenőrzéséhez, alapvetően a számítógépes rendszerekben tárolt és kezelt adatok megbízhatóságát, sértetlenségét és rendelkezésre állását vizsgálja azok pénzügyi beszámolóra gyakorolt hatásának szempontjából.

ITB - KIB – KIETB ajánlások (2008, 2009)
KIB 25 - MIBA (Magyar Informatika Biztonsági Ajánlások, 2008)

A Magyar Informatikai Biztonsági Ajánlás (MIBA) a Közigazgatási Informatikai Bizottság 25. számú ajánlássorozata, amely az Informatikai Tárcaközi Bizottság korábbi 8, 12 és 16 számú ajánlásait váltja ki. Az ajánlások a 2008-ban hatályos (és azóta többször lényegesen megváltozott) elektronikus közigazgatásra vonatkozó követelményrendszert követték amelyek a nemzetközi bevált gyakorlatok honosítása során a magyar közszféra korlátait is figyelembe vették.

Az ajánlások hatóköre az általános célú érzékeny információk, és üzleti titkok védelme. Nem terjed ki a hazai, vagy külföldi minősített adatot feldolgozó informatikai rendszerekre,ezekre külön jogszabályok vonatkoznak, amelyek előírják a vonatkozó követelményeket, és felelősségeket. Az ajánlások szabályzatok, eljárásrendek, és a kapcsolódó dokumentációk elkészítését teszik lehetővé, és az értékelés- illetve tanúsítás is elvégezhető ezek alapján.

MIBA nemzetközi szabványokon alapul többek között az MSZ ISO/IEC 27001, MSZ ISO/IEC 27002, amely a Common Criteria fontosabb elemeit is tartalmazza, felépítése a PDCA elvet követi. Alkalmazását gyakorlati útmutató is segíti.

A MIBIK a biztonsági politikából és kockázatelemzésből kiindulva segít megfogalmazni az informatikai termékekkel, szolgáltatásokkal szemben támasztott biztonsági követelményeket, amelyet fel lehet használni a MIBÉTS kötet által definiált biztonsági előirányzat biztonsági és garanciális elvárásai megfogalmazásánál.

Az ajánlások együttes alkalmazásával, a szervezet sajátosságait is figyelembe véve érhető el a kívánt biztonság. Adott esetben egy termékből hiányzó biztonsági funkciót kiegészítő termékkel, vagy egy szabályozási intézkedéssel pótolva érhetjük el a megfelelő megoldást.

Az IBIV egy MSZ ISO/IEC 27001:2005 szabvány szerinti megfelelést bizonyító tanúsítvány megszerzésére való felkészülés alapja lehet, ami által csökkenthető a külső felkészítőtől igénybe veendő szükséges kapacitás, felkészült belső szakemberek rendelkezésre állása esetén.

URL: http://www.ekk.gov.hu/hu/kib/ajanlasok

KIB 28 – E-Közigazgatási Keretrendszer

Az E-Közigazgatási Keretrendszer projekt eredményeként állt elő szintén 2008-ban a KIB 28. számú ajánlása, amely az elektronikus közigazgatás fejlesztéséhez szükséges teljes eszköztárat tartalmazza, azaz az informatikai biztonsági követelményeken túlmenően a funkcionális és a módszertani követelményeket egyaránt. Az eszköztár kidolgozása során kiemelt cél volt, hogy az önállóan megvalósuló szakágazati és önkormányzati rendszerek között az együttműködés (interoperabilitás) képessége biztosított legyen.

URL: http://www.ekk.gov.hu/hu/kib/ajanlasok

A Pénzügyi Szervezetek Állami Felügyelete is több ajánlást és módszertani útmutatót dolgozott ki az informatikai rendszerekkel kapcsolatban:

- 10/2001. számú ajánlás a pénzügyi szervezetek működésének biztonsági feltételeiről;
- 2/2003. számú ajánlás a hitelintézetek, a befektetési szolgáltatók, az árutőzsdei szolgáltatók és a biztosítók adatkezelési szabályairól;
- 7/2011. számú módszertani útmutató az internetbanki szolgáltatások biztonságáról;
- 6/2013. (III. 11.) számú ajánlás a belső védelmi vonalak kialakításáról és működtetéséről, a pénzügyi szervezetek irányítási és kontroll funkcióiról.

Hogyan mondjuk magyarul

ANGOL-MAGYAR ELEKTRONIKUS INFORMÁCIÓBIZTONSÁGI KISSZÓTÁR

A dokumentumban található szakszavak, és a rövidítések jegyzéke és magyarázata

3

Melléklet

Antivirus software	vírusvédelmi szoftver
Application controls	alkalmazás-kontrollok
Application security	alkalmazás-biztonság
Assurance	bizonyosságnyújtás
Awareness	tudatosság
Backup	mentés
Biometrics	biometria
Black box testing	feketedoboz tesztelés
Botnet	zombihálózat
Browser	böngésző
Brute force attack	nyerserős támadás
Business continuity	üzletfolytonosság,
Business impact analysis (BIA)	üzleti hatáselemzés (BIA)
Capability Maturity Model CMM)	képesség érettségi modell (CMM)
Certificate (Certification) authority (CA)	hitelesítés-szolgáltató (HSZ)
Change management	változáskezelés
Ciphertext	rejtjelezett szöveg
Cleartext	nyílt szöveg (nem rejtjelezett)
Compensating control	kiegészítő kontroll
Completely Automated Public Touring test to tell Computers and Humans Apart (CAPTCHA)	teljesen önműködő nyilvános Touring teszt számítógépek és emberek megkülönböztetésére (CAPTCHA)
Compliance testing	megfelelőség-tesztelés
Computer emergency response team (CERT)	Hálózatbiztonsági Központ (CERT)
Computer-assisted audit technique (CAAT)	számítógéppel támogatott ellenőrzési módszerek (CAAT)
Control	kontroll
Control risk	kontroll kockázat
Corporate governance	felelős vállalat-irányítás
Corrective control	helyesbítő kontroll
Critical infrastructure	Létfontosságú infrastruktúra
Cryptography	kriptográfia
Data classification	adatosztályozás
Data security	adatbiztonság
Decryption	rejtjelfejtés
Denial-of-service attack (DoS)	szolgáltatás-megtagadással járó támadás (DOS)
Detective control	feltáró kontroll
Digital signature	digitális aláírás
Disaster	katasztrófa
Disaster recovery plan (DRP)	katasztrófaterv (DRP)
Encryption key	titkosító kulcs
Enterprise risk management (ERM)	vállalati kockázatkezelés
Event	esemény
Forensic examination	törvényszéki vizsgálat
Honeypot	mézesbödön
Incident response	rendkívüli eseményre adott válaszintézkedés

Information security	információbiztonság
Internal control environment	belső kontrollkörnyezet
Intrusion detection system (IDS)	behatolás-észlelő rendszer (IDS)
IT risk	IT kockázat
Key performance indicator (KPI)	kulcsfontosságú teljesítménymutató
Log	naplóállomány
Malware	rosszindulatú programkód
Man-in-the-middle attack	közbeékelődéses támadás
Maturity model	érettségi modell
Outsourcing	kiszervezés
Password	jelszó
Password cracker	jelszótörő (program)
Penetration testing	behatolás-tesztelés
Personal identification number (PIN)	személyes azonosító kód (PIN)
Phishing	adathalászat
Policy	irányelv
Preventive control	megelőző kontroll
Procedure	eljárás
Process	folyamat
Public key	nyilvános kulcs
Public key encryption	nyilvános kulcsú titkosítás
Quality	minőség
Reputation risk	hírnevet veszélyeztető kockázat
Residual risk	maradványkockázat
Risk factor	kockázati tényező
Risk tolerance	kockázattűrés
Root cause analysis	gyökérok-elemzés
Security incident	biztonsági rendkívüli esemény (biztonsági incidens)
Sign-on procedure	bejelentkezési eljárás
Social engineering	megtévesztés
Spyware	kémprogram
Substantive testing	lényegi tesztelés
Telecommunications	távközlés
Token	hitelesítő eszköz
Total cost of ownership (TCO)	tulajdonlás teljes költsége (TCO)
Trojan horse	trójai faló
Two-factor authentication	kétfaktoros hitelesítés
Validity check	érvényességi ellenőrzés
Virtual private network (VPN)	virtuális magánhálózat (VPN)
Vulnerability	sebezhetőség

Rövidítések jegyzéke

BCMS – business continuity management system, ISO 22301 szerinti menedzsment rendszer a folyamatos működés (üzletfolytonosság) fenntartására,

BCP – business continuity plan, A folyamatos működés fenntartására vonatkozó terv egy működési folyamatra vonatkozóan (üzletfolytonossági terv),

BMIS – Business model for information security, az ISACA holisztikus információbiztonság menedzsment módszertana, mely beépült a COBIT 5 keretrendszerbe.

CAAT – computer assissted audit tool, számítógépes támogatást biztosító ellenőrzési szoftver, amelyet biztonsági vagy ellenőrzési szakemberek használnak.

CERT – hálózatbiztonsági központok, amelyek fő feladata a hálózatbiztonsági incidensek kezelése, az állami szféra vagy egyes ágazatok informatikai rendszereinek hálózatbiztonsági támogatása. A CERT-ek megfelelő technikai háttérrel rendelkeznek ahhoz, hogy időben reagáljanak és kezeljenek minden hálózatbiztonságra és létfontosságú információs infrastruktúrára veszélyes eseményt. A bejelentett eseményeket a központok bizalmasan vezetik.

CIA elv – Az informatikai biztonság az informatikai rendszer olyan kedvező állapota, amelyben a kezelt adatok bizalmassága (confidentiality), sértetlensége (integrity) és rendelkezésre állása (availability) biztosított, valamint a rendszer elemeinek biztonsága szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.

CISA – Certified information systems auditor, tanúsított információrendszer ellenőr cím, melyet az ISACA szakmai vizsga és a tanúsítási feltételek teljesítése esetén, folyamatos továbbképzés, a szakmai és etikai szabályok betartása mellett viselheti a tanúsított személy, az ISACA szakmai szervezet tanúsítványa.

CISM – Certified information security manager, tanúsított információbiztonsági vezető cím, melyet az ISACA szakmai vizsga és a tanúsítási feltételek teljesítése esetén, folyamatos továbbképzés, a szakmai és etikai szabályok betartása mellett viselheti a tanúsított személy, az ISACA szakmai szervezet tanúsítványa.

CISSP – Certified information systems security professional – tanúsított informatikai biztonsági szakértő, az ISC2 szakmai szervezet tanúsítványa,

CMM – Capability Maturity Model (Képesség-érettség modell) A modellben öt fokozat található, amely alapján kiértékelhető egy szervezet fejlettsége a szabványos folyamatok kifejlesztése és követése tekintetében.

COBIT – Az ISACA, mely az információrendszer ellenőrök, az információbiztonsági, informatikai irányítási és informatikai kockázatkezelési szakemberek nemzetközi szervezete az informatikai irányítás, kockázatkezelés, információbiztonság irányítás és informatikai ellenőrzés jó gyakorlatait magába foglaló keretrendszer. A módszertan elsősorban a szakmai vezetőknek ad segítséget ahhoz, hogy felmérhessék, és elfogadható szintre csökkenthessék azokat a kockázatokat, amelyeket az informatika üzleti folyamatokba épülése jelent. Iránymutatásokat tartalmaz egy IT kontroll rendszer kialakításához és annak a folyamatos működtetéséhez. www.isaca.org

DoS támadás – A szolgáltatásmegtagadásos (Denial of Service vagy DoS) támadás egy meghatározott alkalmazás, operációs rendszer ismert gyengeségeit, vagy valamilyen speciális protokoll tulajdonságait (gyengéit) támadja meg. Célja, hogy az alkalmazás, vagy rendszer elérésére feljogosított felhasználókat megakadályozza a számukra fontos információk, a számítógép-rendszer vagy akár a számítógép-hálózat elérésében.

DDoS támadás – elosztott, azaz számos különböző helyről egy időben indított DoS támadás.

DRM – Digital Rights Management, digitális jogkezelő eljárás jogvédett adatok védelme érdekében.

DRP – Disaster recovery plan – (informatikai) Katasztrófa-terv

IBP – Informatikai Biztonsági Politika,

IBSZ – Információbiztonsági szabályzat

MIBA – Magyar Informatikai Biztonsági Ajánlások, a KIB 25. része,

MIBIK – Magyar Informatikai Biztonság Irányítási Keretrendszer, a KIB 25. része,

NEIH – Nemzeti Elektronikus Információbiztonsági Hatóságot,

OECD – Organisation for Economic Co-operation and Development - Gazdasági Együttműködési és Fejlesztési Szervezet

WoT: Web of trust – megbízhatósági hálózat. Olyan oldalak gyűjteménye, amelyet a felhasználók kártékonynak találtak.

Irodalomjegyzék

A szakmai tartalom összeállítása során felhasználták a témára vonatkozó oktatási anyagokat, internetes szakmai forrásokat, és hírforrásokat.

Hatóságok ajánlásai, tájékoztató anyagai:

- ENISA európai információbiztonsági ügynökség
- NIST amerikai kormányzati szabványügyi testület
- PSZÁF magyar pénzügyi felügyelet

Internetes információforrások:

- Wikipedia, közösségi enciklopédia (www.wikipedia.com, www.wikipedia.hu)
- Buhera Blog (buhera.blog.hu)
- Mysec portál (www.mysec.hu)

Szakmai szervezetek kiadványai:

- ISACA (www.isaca.org, www.isaca.hu)
- ISC2 (www.isc2.org)
- CERT Hungary (www.cert-hungary.hu)
- OWASP (www.owasp.org)
- INFOTÉR (www.infoter.eu)

Internetes hazai sajtótermékek:

- www.index.hu
- www.origo.hu
- www.hirado.hu
- www.itbusiness.hu
- www.computerworld.hu

Felsőoktatási tananyagok és segédletek:

- VASVÁRI GYÖRGY, CISM, A BIZTONSÁGI KULTÚRA ÉS AZ EGYÉN, AJÁNLÁS v2.6, 2008, INFORMÁCIÓS TÁRSADALOMÉRT ALAPÍTVÁNY, BIZTONSÁGMENEDZSMENT KUTATÓCSOPORT
- Horváth Gergely Krisztián, Adatbiztonság és IT audit eLearning oktatási anyag, BGF, 2013

Nemzeti Fejlesztési Ügynökség
www.ujszechenyiterv.gov.hu
06 40 638 638

MAGYARORSZÁG MEGÚJUL

A projekt az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósul meg.