DEBRECENI EGYETEM

BIZTONSÁGI IGAZGATÓSÁG

INFORMATIKAI BIZTONSÁGI KÖZPONT

Informatikai biztonsági kézikönyv

Tartalom

1. Dokumentum menedzsment

1.1. Dokumentum leíró adatok

Intézmény megnevezése:	Debreceni Egyetem, Kancellária, Biztonsági Igazgatóság, Informatikai Biztonsági Központ
Dokumentum címe:	Informatikai biztonsági kézikönyv
Dokumentum adatosztályozási besorolása:	Belső használatra
Dokumentum állapota:	Jóváhagyva
Dokumentum leírása:	A Debreceni Egyetem elektronikus információs rendszerei bizalmasságának, sértetlenségének és rendelkezésre állásának teljeskörű védelme biztosítása érdekében felhasználói informatikai biztonsági kézikönyv
Dokumentum kódja:	DE-IBK-IBT_Book-01/202305
Dokumentum felülvizsgálata:	Legalább évente, vagy jelentősebb támadási formák megjelenése során

1.2. Dokumentum változásai

Verzió	Dátum	Készítette	Jóváhagyta	A változások leírása
v. 1.0	2022.04.28.	Tóth Attila Központvezető DE Kancellária Biztonsági Igazgatág Informatikai Biztonsági Központ		Első kiadás
v. 2.0	2023.03.31.	Tóth Attila Központvezető DE Kancellária Biztonsági Igazgatág Informatikai Biztonsági Központ	Kovács Ferenc Főigazgató DE Kancellária Biztonsági Igazgatóság	Szervezeti változás

2. Felelősség

2.1. Dokumentum elkészítése, felügyelete, felülvizsgálata

Név	Szervezet	Beosztás
Tóth Attila	Informatikai Biztonsági Központ	Központvezető
	Debreceni Egyetem	Információbiztonsági felelős

2.2. Dokumentum szakmai tartalma

Név	Szervezet	Beosztás
Tóth Attila	Informatikai Biztonsági Központ	Központvezető

2.3. Szabályozás szakmai végrehajtása

Név	Szervezet	Beosztás
Tóth Attila	Informatikai Biztonsági Központ	Központvezető
	Debreceni Egyetem	Információbiztonsági felelős

3. Bevezető – Előszó helyett

Az informatika mindent átszövő fejlődésével az informatikai biztonság az egyik legfontosabb szakterületévé vált. A biztonság hiánya súlyos anyagi és erkölcsi károkhoz vezet, ennek tükrében egyértelmű, hogy mennyire kiemelt fontosságú az információ és az informatikai biztonság megvalósítása.

Az informatikai biztonság egyszerre van jelen az informatika minden területén, átgondolt, az összes célterületre kiterjedő kialakítása, alkalmazása, működtetése túlmutat az informatikai eszközökön.

Az informatikai biztonság nem képzelhető el egy dobozos „termékként", amelyet megvásárolunk, beüzemelünk és hagyjuk tenni a dolgát.

Az informatikai biztonságot a környezetre, sajátosságokra, különlegességekre, egyedi speciális megjelenésekre szabva kell kialakítani, megvalósítani és működtetni.

A mögötte álló elméleti és gyakorlati szakismeret csak az érintettek együttes, néhol konszenzus kész hozzáállásával áll össze, válik teljessé.

Az informatikai biztonság „szellem" terület, hiszen megléte nem látható, nem érzékelhető, hiánya azonban, akár kis incidens megjelenése alkalmával is hamar kockázatossá válhat.

Az információ, legyen az bármilyen formában, tartalomban megjelenő adat, jelentős eszmei értéket képvisel. Különösen igaz ez napjainkban, amikor az informatikai rendszerek hatalmas mennyiségű információt kezelnek, tárolnak, állítanak elő és továbbítanak, nem egyszer államhatáron túlra is. A bennük áramló információ titkossága, sértetlensége és elérhetősége létfontosságú.

Figyelembe véve a Debreceni Egyetem szervezeti növekedését, az ez által használt rendszerek és szolgáltatások robbanásszerű fejlődését, az információ, adat és az azt kezelő, kiszolgáló infrastruktúra védelme, kiemelten és magas prioritással kezelendő.

A vállalati stratégia részét kell képeznie az Informatikai Védelmi intézkedéseknek, mivel az támogatja, kiszolgálja és védi a pénzügyi, marketing, HR, innovációs, szolgáltatás valamint logisztikai, stratégia célokat.

Az informatikai biztonságot csak egy előre megtervezett, majd a terv alapján felépített védelmi rendszer garantálhatja, mely teljes körű, zárt és a kockázatokkal arányos.

Ahhoz, hogy informatikai biztonságról beszéljünk, ezzel kapcsolatosan bármineműt cselekedjünk, fizetőeszközt adjunk ki, a „Zéró tolerancia", „Zéró bizalom" és a „Ne bízz senkiben" vezérelv kell, hogy érvényesüljön.

Nem szabad automatikusan megbízni semmilyen belső vagy külső szereplőben, legyen az felhasználó, fizikai eszköz vagy szoftver, mivel az feltételezhetően lehet rosszindulatú szereplő. A rendszerekhez csatlakozni próbáló valamennyi felhasználót, eszközt ellenőrizni kell, mielőtt bármilyen szintű hozzáférést kap. Ezért olyan hozzáférési stratégia eljárásrend kidolgozása szükséges, ami lényege, hogy szakítsunk meg minden kapcsolatot addig, amíg ki nem derül, ki, mi az, ami, a hozzáférést kezdeményezi. Nem megengedhető hozzáférés IP-címekhez, számítógépekhez, szerverekhez, adatbázisokhoz, szoftverekhez, amíg nincs ellenőrizve, ki, mi a kapcsolódási kezdeményező és van-e jogosultsága, ha igen az milyen szintű!

Ezt a szigort ki kell terjeszteni, a biztonságot meg kell követelni mindazon felhasználói szoftvergyártótól, szolgáltatótól is, akik a Debreceni Egyetem bármilyen adatát kezelik, használják, dolgoznak vele. Szigorú user autentikáció kell minden szoftver beléptetéshez, és alkalmazni, ki kell követelni a „passzivitási kiléptetés" elvét (egy időkorlát alatt nem történik a billenytűn leütés vagy nincs egérrel végrahajtott tevékenység).

Nem szabad abba a hibába esni, hogy csak a peremek megvédésére fókuszálunk, mert az incidensek jelentős része belülről is történhet és az erős várfalak (tűzfalak) itt már nem nyújthatnak biztonságot, védelmet,

Sőt. Belülről a kapuk is könnyebben, különösebb ellenállás nélkül nyithatók, amik újabb állandó támadásoknak, veszélyeknek nyit szabad utat.

Az informatikai védelmi stratégia nem egy bombabiztos, bonyolult, már-már követhetetlen rendszer megvalósítása, hanem egy „mélységi védelmi rendszer" létrehozása, ami egy többrétegű védelmi modell kiépítése.

Az informatikai védelmi célok különösen érzékeny területe a felhő alapú szolgáltatások igénybevétele. Amíg nem szükséges, addig mellőzni kell, mivel a „távoli" védelemre az egyetemnek hatása nincs.

3.1. Jövőkép

A kiberbűnözők egyre kifinomultabb módszereket dolgoznak ki, használnak, amiknél nagyon fontos lépés a rövid felderítési idő és az erre reagáló védelmi technológiai megoldás kidolgozása.

A mai kiberbiztonsági megoldások területén a mesterséges intelligenciára (AI –Atificial Intelligence) és a gépi tanulásra (machine learning – ML) így jelentős feladat hárulhatna.

A Debreceni Egyetem, mint az ország egyik legkiemelkedőbb tudásbázissal rendelkező tanintézménye lehetne az első, aki az informatikai védelem biztonságos, hatékony, naprakész (leginkább pillanat kész) támogatására maga mellé állítaná, a Mesterséges Intelligenciát, a gépi tanulást.

Természetesen csak erre támaszkodó védelem, saját kardba dőlés lenne, mivel ezeket a technológiákat valószínűsíthetően a rosszakarók is használni, és kihasználni fogják.

Ezek a megoldások természetesen kiegészítésként növelnék a hatékony védekezést, amiket folyamatos átképzéssel, tanítással lehetne okosítani, a harc frontvonalában tartani, de leplezetten, szellemként működve, hogy ne kerülhessenek a támadások célkeresztjébe. (4. Ábra)

A leghatékonyabb „humán password" alkalmazásának lehetőségeit kell megvizsgálni és alkalmazni a gyakorlatban, mivel a biometriai azonosítás, mint az ujjlenyomat, az írisz lenyomat vagy az arckép a legegyedibb és lemásolhatatlan (itt el kell felejteni a sci-fi és a 007-es ügynök filmeket) és feltörhetetlen.

3.2. Hogyan?

Egy IT bölcselet szerint az informatikai problémák legnagyobb része a billentyűzet és a szék között van.

Sajnos az informatikai védelem leggyengébb láncszeme, „AZ EMBER"

Az informatikai támadásoknak csak 20%-a történik rosszul beállított informatikai rendszerek gyengeségeinek, hiányainak kihasználásával. A maradék 80% vagy belső támadás, vagy kiszivárgó belső információ (pl. jelszó) segítségével elkövetett támadás.

Ezért íródott ez a kézikönyv.

3.3. Ok.

A Debreceni Egyetem polgárainak Informatikai Biztonság tudatosságának, öntudatosságának növelése.

Ne az ember legyen a leggyengébb láncszem.

A 80% ne legyen, vagy a legminimálisabb mértékre legyen leszorítva.

3.4. Miért?

Az informatika a mindennapi életünk, lassan nélkülözhetetlen részévé vált, de használata során információink, adataink, eszközeink számtalan veszélynek vannak kitéve.

Milyen hatással lehetnek a számítógépes veszélyek adatainkra és tulajdonunkra?

Számtalan módon lehetnek az információs rendszerekre ható veszélyek hatással ránk és a szervezetünkre. A hatásuk a jelentéktelentől akár a katasztrofálisig is terjedhet és jóval túlmutathat az egyénen, illetve egyes esetekben az egyetem határain is.

Lehetséges esetek;

- 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, honlapok-, más szervezetek támadása)
- üzleti titkok, vagy minősített információk sérülhetnek
- üzleti titkok, vagy minősített információk kerülnek illetéktelen birtokába
- fizikailag eltulajdoníthatják eszközeinket, értékeinket

3.5. Mi a cél?

Megismertetni ezeket a veszélyeket, és az ellenük való védekezés lehetőségeit, formáit, módjait, hogy nyugodt szívvel meg tudjunk bízni az informatikában, hogy rá merjük bízni a kiszolgálásainkat saját magunk és munkahelyünk érdekében.

Hogyan?

Nem elvont tudományos nyelven, hanem „közérthetően magyarul" és egy kis ismeretterjesztés, hogy érthető legyen a tudományoskodó médiatájékoztatás szövegkörnyezete.

És...

Máshogyan.

A megszokott kiadványoktól eltérően legyen e kézikönyv a gondolatébresztésen, figyelemfelkeltésen, rádöbbentésen túl közös „termék".

Minden olvasó legyen társszerző. Tegyük interaktívvá, úgy hogy az olvasó „kíváncsisága", véleménye, ötlete írja, bővítse, tegye teljessé a kézikönyvet.

Tegyenek fel kérdéseket, legyenek ötleteik, akár (mi is, emberek vagyunk) pontosításokat is fogalmazzanak meg. Legyenek kíváncsiak, hogy miről-, vagy bővebben informálódni egy-egy témában, témakörben.

Ahol ezt megtehetik.

ibk@unideb.hu elektronikus levelezési címen.

3.6. Mit kell elérni, és azt hogyan?

Alap tézis és mottó.

Definíció

Biztonsági tudatosság

A szervezet kultúrájának része.

Olyan gondolkodás- és magatartásmód, amely biztosítja, hogy a munkatársak személyes elkötelezettségből elismerik a biztonsági intézkedések jogosságát, betartják-, betartatják és másokkal is megismertetik azokat.

Egy cél érdekében.
Jó közösségnek, egy és közös a célja.

A Debreceni Egyetem hatékony Informatikai védelmének megvalósításához és fenntartásához a jog-, és szabálykövető magatartás kell, hogy legyen minden egyetemi polgár öntudatossága és lojalitása.

4. A lényegi mondanivaló, avagy kezdjünk neki.

4.1. Mi a biztonság?

Leggyakoribb tévedés!

Az adatvédelem és az adatbiztonság NEM ugyanazt jelentik.

Adatvédelem alatt a személyes és érzékeny adatok jogszabályi védelmét érti a jogalkotó, **adatbiztonság** alatt pedig a számítógépes rendszerekben tárolt, feldolgozott, vagy továbbított adatok biztonságának fenntartására kell gondolnunk.

GDPR alapelvek.

Bizalmasság

Sértetlenség

Rendelkezésre állás

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.

4.2. Miért fontos az IT és az információbiztonság?

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 vagyon-tárgyaknak 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.

4.3. Mi az elvárás az informatikai rendszerrel szemben?

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.

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.

Az informatikai rendszer biztonságának megléte nem érzékelhető, csak annak a hiánya.

Ahhoz, hogy egy szervezet, vagy egy információs rendszer biztonságát meg tudjuk valósítani, pontosan ismernünk kell a rendszer célját és a releváns kockázatok mértékét, és azzal arányos védelmi rendszert kell kialakítani.

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 is lefedi.

Az MSZ ISO/IEC 27001 célja, hogy modellként szolgáljon információbiztonsági irányítási rendszerek (ISMS) kialakításához, megvalósításához, működtetéséhez, figyelemmel kíséréséhez, átvizsgálásához, fenntartásához és fejlesztéséhez. Tartalmazza továbbá 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 szabványok-hoz hasonlóan, a teljes körű informatikai biztonság megteremtéséhez szükséges szervezési, szabályozási szempontrendszert adja meg.

A szabvány a védelmi intézkedéseket az alábbi logikai csoportokba szervezi:

a) kockázatelemzés;
b) biztonságpolitika, szabályzati rendszer;
c) biztonsági szervezet;
d) vagyontárgyak kezelése;
e) személyi biztonság;
f) fizikai és környezeti biztonság;
g) kommunikáció és üzemeltetés biztonsága;
h) hozzáférés-ellenőrzés;
i) információs rendszerek beszerzése, fejlesztése és karbantartása;
j) incidenskezelés;
k) üzletmenet-folytonosság;
l) megfelelőség.

4.4. Információs rendszerek elemei

Az informatikai irányítás nemzetközi sztenderdje – a Cobit – az információs rendszerek elemeit négy csoportba sorolja:

1) információ,
2) infrastruktúra,
3) alkalmazói rendszer, és
4) emberi erőforrás.

Az infrastruktúra és az alkalmazói rendszerek ismertetése közérthetően:

hardver:

- szerver;
  - több felhasználó munkáját kiszolgáló központi számítógép
- munkaállomás/PC/desktop;
  - egy felhasználó munkáját kiszolgáló asztali számítógép
- hordozható számítógép/laptop/notebook;
  - a PC hordozható változata, ami saját akkumulátorról is üzemel)
- mobiltelefon;
  - ma már kézi számítógép
- táblagép;
  - a hordozható számítógépeket egyszerűbb, billentyűzet nélküli érintőképernyős változata, kézi számítógép
- adathordozó, adattároló egység/HDD/NAS/Storage;
  - 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 (firewall), 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.

4.5. 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 léphetünk.

QR-kód:

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.

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.

4.6. Biztonsági kultúra kialakítása

Az alábbi kérdésekre adott válaszok határozzák meg, hogy milyen területen és 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?

4.7. 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 szintjének fenntartása, vagy emelése önmagában is védelmi intézkedés.
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.
Alapvető módszer az, ha felkészítik a felhasználókat, szervezet 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, ezen ismerető.

4.8. Biztonsági kultúra megvalósításának alapelvei

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.

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, észlelják, illetve reagáljanak a váratlan biztonsági

eseményekre. Ahol lehetséges, ez akár határokon keresztüli információcserével és együttműködéssel is járhat.

4. Az 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. A 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. A 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 biztonság- menedzsment 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.

5. A biztonsági kultúra megteremtését, fejlesztését kezdjük a veszélyek és azok kezelésének a megismerésével.

5.1. Mik ezek a veszélyek?

Főbb csoportok

a. Személyes adatokat érintő incidensek
b. E-mail fenyegetettségek, kártékony programok és botnetek
c. Mobileszközök fenyegetettségei
d. Zsarolóvírusok (Ransomware)

Számítógépes incidensek

a. jogosulatlan adathozzáférés, módosítás
b. jelszavak feltörése
c. kéretlen levelek (spam)
d. hamis lánclevelek (hoax)
e. vírusok
f. féreg (worm)
g. trójaik
h. rootkit-ek (rendszermagot fertőző kártevő)
i. zombihálózat (botnet)
j. reklámprogramok (adware)
k. kémprogramok (spyware), kártevő programok (malware)
l. hamis szoftverek (rogue software, scareware)
m. adathalászat (phising)
n. fertőző honlapok
o. adatforgalom eltérítése (Man-in-the-middle)
p. túlterheléses támadás (DoS, DDoS)
q. hálózati letapogatás (network / port scanning)
r. távoli adminisztrátor eszközök
s. adatvesztés
t. rendszerfrissítések hibái, hiánya

Fizikai incidensek

a. jelszavak ellesése (observing passwords attack)
b. megtévesztésen alapuló csalások (Social engineering) .
c. IT személyiséglopás (megszemélyesítés eltulajdonítása információs rendszerekből)
d. eszközök és adathordozók eltulajdonítása
e. szemétbe dobott információ (kukabúvárkodás)
f. személyes / munkahelyi adatok megosztása közösségi hálózatokon

5.2. Amennyiben incidens következik be (az előzőeket észleli, tapasztalja, vagy gyanuja van) kinek kell jelezni?

Személyes adatok (természetes személy adatai, GDPR irányelvek)

Debreceni Egyetem Adatvédelmi Központ

Telefon:

Levelezési cím:

Minden egyéb esemény (incidens)

Debreceni Egyetem Informatikai Biztonsági Központ

Telefon:

Levelezési cím:

5.3. Mikor kell gyanakodni a biztonság megsértésére, incidens bekövetkeztére?

Jelenség.

A megszokottól eltérő működést tapasztalunk a számítógépes eszközeink használata során. A rendszer elindulásának, a rendszer működésének vagy az internetezés sebességének jelentős lassulása, a rendszerek összeomlása, a böngészés során felugró ablakokban reklámok megjelenése, ismeretlen feladóktól érkező-, személyes adatainkat kérő levelek.

5.4. Mi a teendő?

Tájékoztatni kell az Informatikai Szolgáltató Központ ügyfélszolgálatát, ha van a helyi informatikust, vagy az Informatikai Biztonsági Központ ügyfélszolgálatát, ügyeletét.

5.5. Veszélyek

Veszély:

Jogosulatlan adathozzáférés, módosítás

Mi ez?

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

Mi a veszély?

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.

Prevenció (megelőzés)

A jogosulatlan adathozzáférés megelőzésére több módszert párhuzamosan kell alkalmazni.

a. 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.
b. 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.
c. Az információs rendszerek tervezése során olyan kontrollokat kell előírni és megvalósíttatni, mely megakadályozza, hogy érvényesen lehessen adatokat módosítani az információs rendszer felhasználói felületét megkerülve.
d. Magukat az adatokat lehet például egy „borítékba" zárni digitális aláírás technológia felhasználásával.

Mit kell tenni, ha bekövetkezik?

Haladéktalanul értesíteni kell az egyetem informatikai biztonsági vezetőjét! Az adatokhoz való jogosulatlan hozzáférés, és azok jogosulatlan módosítása komoly biztonsági probléma magában, de a védelmi rendszer nagyobb hiányosságait is jelezheti egy jogosulatlan hozzáférés.

Veszély:

Jelszavak feltörése

Mi ez?

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.

Mi a veszély?

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.

Prevenció (megelőzés)

Használjunk összetett és kellően hosszú jelszavakat, sőt sokkal inkább jelmondatokat, amelyek könynyen 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 osszuk mefg senkivel, hogy milyen logika szerint választunk jelszavakat!

Ne használjuk mindehol ugyanazt a jelszót.

Fő szabály, hogy a privát szféra, így legfőbbképpen a közösségi oldalak és a munkahelyi jelszó jelentősen különbözzön!

Mit kell tenni, 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.

Veszély:

Kéretlen levelek (spam)

Mi ez?

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.

Mi a veszély?

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.

Prevenció (megelőzés)

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 kell tenni, 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 (Nemzeti Média- és Hírközlési Hatóság) részére.

Veszély:

Hamis lánclevelek (hoax)

Mi ez?

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.

Mi a veszély?

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.

Prevenció (megelőzés)

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 kell tenni, ha bekövetkezik?

Honnan ismerhetjük fel a láncleveleket? 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 láncLevelekkel 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 láncLevelekről szóló oldalt fogunk kapni.

Veszély:

Vírusok

Mi ez?

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.

Mi a veszély?

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.

Prevenció (megelőzés)

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, aktivizálódásuk, káros ténykedésük megelőzése.

Mit kell tenni, 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.

Veszély:

Féreg (worm)

Mi ez?

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.

Mi a veszély?

Felhasználó: teljesen "kitöltik", így blokkolják a számítógépe 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.

Prevenció (megelőzés)

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

Mit kell tenni, 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.

Veszély:

Trójaik

Mi ez?

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.

Főbb típusai:

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

Mi a veszély?

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.

Prevenció (megelőzés)

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

Mit kell tenni, 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.

Veszély:

Rootkit-ek (rendszermagot fertőző kártevő)

Mi ez?

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 rendszerállományokat 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.

Mi a veszély?

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.

Prevenció (megelőzés)

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 kell tenni, 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 kereséssel, speciális biztonsági szoftverekkel lehetséges azonosítani, és eltávolítani.

Veszély:

Zombihálózat (botnet)

Mi ez?

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.

Mi a veszély?

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.

Prevenció (megelőzés)

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 kell tenni, 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).

Veszély:

Reklámprogramok (adware)

Mi ez?

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.

Mi a veszély?

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.

Prevenció (megelőzés)

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.

Ehhez jó eszköz a tartományvezérelt user-, autentikáció és kezelés, az Active Directory.

Mit kell tenni, 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.

Veszély:

Kémprogramok (spyware), kártevő programok (malware)

Mi ez?

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.

Mi a veszély?

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.

Prevenció (megelőzés)

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

Mit kell tenni, 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.

Veszély:

Hamis szoftverek (rogue software, scareware)

Mi ez?

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.

Mi a veszély?

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.

Prevenció (megelőzés)

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 kell tenni, 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!

Veszély:

Adathalászat (phising)

Mi ez?

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.

Mi a veszély?

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.

Prevenció (megelőzés)

Az adathalászatot a felhasználók és az ügyfelek képzésével, biztonságtudatosításával előzhetjük meg.

Emellett több böngészőhöz telepíthető olyan kiegészítő, amely jelez adathalász oldalra lépéskor.

Mit kell tenni, 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.

Veszély:

Fertőző honlapok

Mi ez?

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.

Mi a veszély?

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.

Prevenció (megelőzés)

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 (WoT11), 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 szükséges.

Mit kell tenni, 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.

Veszély:

Adatforgalom eltérítése (Man-in-the-middle)

Mi ez?

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.

Mi a veszély?

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.

Prevenció (megelőzés)

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 kell tenni, 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.

Veszély:

Jelszavak ellesése (observing passwords attack)

Mi ez?

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.

Mi a veszély?

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.

Prevenció (megelőzés)

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.

A PARANOIA NEM SZÉGYEN!

A jelszó megszerezhető az „áldozat" válla, feje felett, a munkahelyre rálátó ablakon keresztül is.

NÉZZEN A HÁTA MÖGÉ JELSZAVA BEÍRÁSA ELŐTT!!!

Mit kell tenni, 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!

Veszély:

Megtévesztésen alapuló csalások (Social engineering)

Mi ez?

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.

Jóhiszeműséget kihasználó álcák.

a. Szerződéses partner cég alkalmazottja
b. Külső alkalmazott (más campus dolgozója)
c. Karbantartó
d. Ügyfél
e. Postás
f. Futár
g. Fontos személy
h. Új alkalmazott, aki még nem ismeri ki magát, nincs helyismerete az új munkakörnyezetében, nem tudja még megfelelő magabiztossággal kezelni az „adatokat, információkat tálcán kínáló" rendszert és természetesen így (szegény) segítségre szorul.
i. „IT nagy tudású" segítőkész embertárs

Mi a veszély?

Felhasználó: az azonosítók és jelszavak kiadása különféle következménnyel járhat, a személyes adataink megszerzésétől kezdve, a munkahelyi 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.

Prevenció (megelőzés)

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 kell tenni, 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.

Veszély:

IT személyiséglopás (megszemélyesítés eltulajdonítása információs rendszerekben)

Mi ez?

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

Mi a veszély?

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.

Prevenció (megelőzés)

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 kell tenni, ha bekövetkezik?

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

Veszély:

Eszközök és adathordozók eltulajdonítása

Mi ez?

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.

Mi a veszély?

Felhasználó: a számítógépes eszközünk, és az adathordozónk értéktárgy, ellopásuk vagyoni kárt okoz, de a rajta levő adatok elvesztése gyakran nagyobb veszteséget, az anyagi értéken túl erkölcsi értékvesztést is 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 ad lehetőséget.

Prevenció (megelőzés)

Az ellopott adathordozókon keresztüli adatvesztést az adatok, illetve az adathordozók titkosításával előzhetjük meg. Ne tároljunk szükségtelenül adatokat hordozható eszközökön. Amennyiben munkaköréből adódóan ez elkerülhetetlen, használjon többszörös (titkosítás és kód) védelmet biztosító eszközt.

Mára már a legtöbb USB pen drive gyártó, eszközéhez előre telepített titkosító szoftvert „mellékel", ami jelszavas vagy intelligens kártyás védelemmel kódoltan (rejtjelezve) védi az adathordozó tartalmát, írási-olvasási hozzáférését.

De vannak, más internetről ingyenesen letölthető megbízható titkosító szoftverek is (TrueCrypt, BitLocker, Rohos Mini Drive).

A Kingston DataTraveler 2000 USB tár, egy elegáns készülék, amivel egy komplett hardveres védelmet kaphat adatai titkosítására, így annak védelmére, mivel billentyűkódos védelemmel van ellátva.

Főbb jellemzői.

a. fém tok
b. mérsékelten por és vízálló
c. PIN kódos lezárás
d. az adat titkosítással tárolódik (AES-256)
e. Illetéktelen próbálkozások sora után, véglegesen és vissza-állíthatatlanul törlődik

Ami nagyon fontos. A készülék CSAK AKKOR NYÚJT VÉDELMET, ha a biztonsági PIN kód nincs rá írva, nincs a közelében feltüntetve.

Mit kell tenni, 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.

Veszély:

Eszközök selejtezése, kidobása

Mi ez?

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.

Mi a veszély?

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.

Prevenció (megelőzés)

Az eszközök selejtezése előtt visszaállíthatatlanul töröljünk minden adatot, vagy ha ez nem lehetséges, fizikailag semmisítsük meg az adathordozókat. Ez rongálást jelent, az dathordozót át kell fúrni, el kell törni.

Mit kell tenni, 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.

Veszély:

Szemétbe dobott információ (kukabúvárkodás)

Mi ez?

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

Mi a veszély?

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.

Prevenció (megelőzés)

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 kell tenni, ha bekövetkezik?

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

Veszély:

Személyes / munkahelyi adatok megosztása közösségi hálózatokon

Mi ez?

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.

Mi a veszély?

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.

Prevenció (megelőzés)

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 kell tenni, 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.

Veszély:

Túlterheléses támadás (doS, ddoS)

Mi ez?

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 elérhetetlen-ségéhez, vagy leállásához vezet.

Mi a veszély?

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.

Prevenció (megelőzés)

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 kell tenni, 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.

Veszély:

Hálózati letapogatás (network / port scanning)

Mi ez?

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.

Mi a veszély?

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.

Prevenció (megelőzés)

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 kell tenni, 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.

Veszély:

Távoli adminisztrátor eszközök

Mi ez?

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

Mi a veszély?

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.

Prevenció (megelőzés)

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 kell tenni, 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!

Veszély:

Adatvesztés

Mi ez?

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.

Mi a veszély?

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.

Prevenció (megelőzés)

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 kell tenni, 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.

Veszély:

Rendszerfrissítések hibái, hiánya

Mi ez?

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.

Mi a veszély?

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.

Prevenció (megelőzés)

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

Mit kell tenni, ha bekövetkezik?

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

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

6. 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.
Az alábbiakban pár olyan módszert mutatunk be, amik az informatikai biztonsági kockázatot csökkenthetik.

6.1. 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 célszerűminden 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.

6.2. 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 íváncsiskodástól, 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.

6.3. 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 mappatitkosítást 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 (internetről ingyenesen letölthető és korlázozás nélkül használható) 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.

6.4. Microsoft 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. A titkosítatlan levél tartalmát, amerre eljut a hálózaton, bárki elolvashatja.
b. Naptárbejegyzéseket, vagy azok tárgyát olvashatják azok a munkatársak is, akikkel nem osztottuk meg teljes körűen az elfoglaltsági adatainkat.
c. 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 újabb verziói 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.

6.5. 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 (munkahelyi, vagy saját) munkavégzés célú használatát. Csak olyan eszközre tegyünk munkahelyi adatokat, amelyre engedélyezett!

A szinkronizálás során felmerülhet, hogy a munkahelyi adatokat, nem csak az egyetem által jóváhagyott alkalmazásokban tároljuk (például: gmail, facebook), általában ez az egyetemi 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.

Az 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.

6.6. 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.
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.

6.7. Autentikációt igénylő szoftver hosszabb időre történő „elhagyása”.

Munkakörtől függően vannak helyzetek, amikor egy másfajta tevékenység végzése miatt ott kell hagyni azt a számítástechnikai eszközt, amibe saját adataival lépett be.
Amennyiben eltávolodik a helyszíntől a belépésével aktivált szoftver lehetőséget biztosít más kollégának vagy idegen személynek arra, hogy a rendszerben az Ön nevével „kalózkodhat”. Bármit tesz, azt az Ön nevében teszi és incedens bekövetkezése esetén a naplóállományokból az fog kiderülni, hogy Ön tette, azt, ami az incidens eseményt kiváltotta.

Ma már védelmi okokból sok szoftver van felkészítve arra, hogy egy bizonyos idő elteltével, ha inaktivitást észlel (nincs billenytűzethasználat) kilépteti a felhasználót, aki ismételt belépést követően „visszakapja" a munkafelületét.
Ha az Ön szoftvere, nincs felkészítve ilyen funkció biztosítására, erre Önnek kell figyelnie.
Ez a **kényszerített kiléptetés**.
Ha, hosszabb időre, vagy csak el kell távolodnia úgy a beviteli informatika eszköztől, hogy arra rálátása nincs, biztonsági okból és a saját védelme érdekében lépjen ki.
Soha ne engedje meg, még a legjobb munkatársának sem, hogy az Ön belépési adataival dolgozzon. Nem tud senki olyan indokot felhozni mentségére, hogy ne a saját, hanek az Ön neve alatt tevékenykedjen.
Az egészségügyi rendszerekben időbélyeges naplózás történik, ami minden „mozdulatát" rögzíti.

6.8. Asztalon „hagyott", asztalon felejtett" információk

Egy-egy cetli, feljegyzés, emlékeztető, vagy munkaköréből adódó "beszédes" információt tartalmazó dokumentum, mind-mind értéket jelentenek, jelenthetnek a támadóknak.
Legyen az gazdasági-, természetes személy-, orvosi-, tudományos-, (uram bocsá') belépési-, bérügyi-, munkaügyi adat felhasználható, másolható, így visszaélésra okot adó információ lehet.
Ezért, minden munkavégzést követően az asztalóról ezeket a "lehetőségeket" tegye-, zárja el.
Amennyiben olyan helyen van a munkavégzése (pl. nővérpult), ahol közforgalom van, ilyen jellegű iratokat egyáltalán ne tartson-, ne hagyjon szem előtt.

6.9. Informatikai eszközök áramtalanítása

Ugyanúgy kell eljárnia, mint az otthonában a saját tulajdonú eszközei tekintetében. Érezze, hogy a munkavégzéséhez szükséges informatikai eszöz az Ön gondjaira van bízva, bánjon is így vele.
Minden munkaidő lejárta után, amennyiben elhagyja a munkavégzés helyét és az informatikai eszközt nem kell átadni másnak munkavégzésre, áramtalanítsa a készüléket.
Kapcsolja le az elosztó kapcsolóját, ha ilyenre nincs lehetősége húzza ki a konnektorból.
A miért.
Fizikai védelem.

Ezzel hosszabbítja az eszköz élettartamát, megelőzi a tönkremenetelét egy nagyobb áramlökés (áramszünet utáni visszakapcsolás, vihar) esetén, és takarékoskodik, mivel

a készülék stand by üzembentartása is áramfelhasz- nálással jár (érdekes, hogy ezt otthol mindenki tudja).

Biztonság.

A bekapcsolt számítógépet el lehet érnie egy hackernek, vagy egy rosszindulatú, haragos belső munkatársnak, de nem hinné el, vannak megoldások, hogy a kikapcsolt (stand by állapotú) számítógépeket is "fel lehet ébreszteni alvó állapotukból". És az eszközről, már a védelem (firewall vagy tűzfal) védett oldalán van a rosszindulatú támadó, hacker.

6.10. Jelszó, mint alfatámadási célpont

A támadók célja lehet, hogy jelszót, jelszavakat megszerezve hozzáférjenek a célszervezet számítógépes rendszeréhez. A támadóknak sokszor elegendő, ha csupán egy felhasználó jelszava feltörhető, megszerezhető a rendszerben.

A megszerzett hozzáférési kulccsal a támadó a teljes rendszert kompromittálhatja vagy „ugródeszkaként" használhatja más rendszerek eléréséhez.

Ami Önre nézve „kínos" lehet, amennyiben az Ön hozzáférése lett az áldozat.

A rendszer szemszögéből olyan, mintha Ön hajtaná végre az adott műveleteket, így amit a támadó tesz, az Ön nevében teszi, így kerül rögzítésre a rendszer naplóállományaiban.

A tapasztalat szerint gyakran a gyenge jelszavak okoznak informatikai incidenseket, amennyiben nem elvárás követőek.

Például az 1234 jelszó nem kreatív, nem átgondolt így nem felelősségteljes, ez gondatlanság.

A jelszavainkat gondosan kell megválasztanunk és körültekintően kell kezelnünk.

Hogyan válasszon erős jelszót?

a. ne legyen Önre jellemző, mert kevés információ birtokában is könnyen kitalálható (pl.: családtag neve, születési dátum egy rövid kereséssel a közösségi oldalakon kideríthető;
b. nem szerencsés, ha a jelszó csak egy szóból áll (például az „almafa" szó biztosan szerepel egy támadó által kipróbálandó jelszavak listájában);
c. jó, ha a jelszó hosszú és több féle karaktert (kisbetű, nagybetű, szám, írásjel) tartalmaz, mert ezzel megnehezíti a lehetséges kombinációk végigpásztázása (nyers erő vagy brute force) technikával való feltörést;
d. a legjobb, ha néhány szóból álló jelmondatot választunk, amelyben van kisbetű, nagybetű, szám és írásjel is. Ezt könnyű megjegyezni, azonban nehéz kitalálni, brute force technikával feltörni pedig szinte lehetetlen.

Jelszavak kezelése.

a. ne adja „kölcsön" a jelszavát,
b. ne írja fel a jelszavát, ez elveszhet, könnyen illetéktelen kezekbe kerülhet;

c. ne használja mindenhol ugyanazt a jelszót, ha a támadók egyet feltörnek, minden más rendszeréhez, az Ön által használt munkahelyi hálózathoz hozzáférhetnek;

d. rendszeresen, akár random időszakonként változtassa meg a jelszavát, mert, ha a támadónak minél több ideje van próbálkozni, annál nagyobb valószínűséggel tudja megszerezni a hozzáférésünket.

Belegondolt már? Amennyiben még nem kérjük, tegye meg!

Igen nagy veszélyt rejt magában, ha például ugyanazzal a jelszóval lép be a munkahelyi hálózatába is, mint amit a közösségi oldalakon is használ.

Miért?

Amennyiben a közösségi oldalakon megadott jelszavát feltörik, ellopják, a profiljában megadott munkahelye már potenciális célponttá is vált.

„Ide lőjetek". A támadás helyét, annak kiválasztását, Ön határozta mega támadóknak.

7. Támadók, kiber bűnözők, hackerek

Sokat, sokszor emlegettük a **támadók**at az előzőekben.

Kik ők?

Ellenség, aki láthatalan, mindig Ő van lépéselőnyben, és minden célpont lehet, ahol informatikai megoldással vezérelt szolgáltatásnyújtás van.

Szokásos nyílvántartó, könyvelő, pénzügyi rendszereken túl, okos ház, okos autó, okos telefon, egészségügyi eszközök.

Mik lehetnek a céljaik?

Adat-, információlopás, rendszerek működésének lassítása, rendszerek működésének leállítása, „váltságdíj" követelés (lekódolt rendszer feloldó kulcsáért), bűnözés, kémkedés.

Honnan támadnak?

A fenyegetettség a kiber (cyber) térből érkezhet.

"A **kibertér** globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti."

Az infokommunikációs rendszerek elleni kiber támadások arra irányulnak, hogy megzavarják vagy gátolják a megtámadott rendszer működését, illetve hogy megszerezzék vagy módosítsák annak adatait.

A támadások többségét politikai és vallási aktivisták, gazdasági bűnözői csoportok, terrorista szervezetek, illetve egyes államok titkosszolgálatai követik el.

Ez a **„Cyber war"**

Ami, egy **XXI. századi „hidegháború"** ahol **MINDENKI** potenciális **ÁLDOZAT LEHET.**

Gondoljon bele, hogy a „háború" jelző mennyire helytálló.

A Debreceni Egyetem működésének egyik nagyon jelentős ágazata, területe, az egészségügyi ellátás és gyógyítás. Itt jelen vannak olyan informatikai eszközök, megoldások, amik életek fenntartását, műtétetek-, diagnózis meghatározások támogatását szolgálják, SZOFTVERES VEZÉRLÉSSEL.

Szoftveres vezérléssel, ami egy kódsorozat, amibe „bele lehet nyúlni, át lehet írni", „magyarul" meg lehet hackelni.

Ezen eszközök szoftvereinek **a hackelése lehetőséget ad, biztosít, lő-, vegyi-, biológiai-, atomfegyver nélkül is, akár emberi élet, életek kioltására is.**

Egy eklatáns példa, miért is kötelező ennyire komolyan venni az informatikai védelmet, a prevenciót, az öntudatos odafigyelést, a ne bízz senkiben-, légy gyanakvó és körültekintő alapelvet.

8. Fogalommagyarázatok és definíciók

Adat

Az információ megjelenési formája, azaz a tények, elképzelések nem értelmezett, de értelmezhető közlési formája.

Adatállomány

Valamely informatikai rendszerben lévő adatok logikai összefogása, amelyet egy névvel jelölnek. Ezen a néven keresztül férhetünk hozzá a tartalmazott adatokhoz.

Adatátvitel

Adatok informatikai rendszerek, rendszerelemek közötti továbbítása.

Adatbiztonság

Az adatok jogosulatlan megszerzése, módosítása és tönkretétele elleni műszaki és szervezési intézkedések és eljárások együttes rendszere.

Adatkezelés

Adatok feltérképezése, gyűjtése, felvétele, tárolása, rendszerezése, feldolgozása, hasznosítása, sokszorosítása, továbbítása (hozzáférhetővé tétele harmadik fél számára), átadása, ábrázolása, nyilvánosságra hozatala, bárminemű megváltoztatása, további felhasználásuk megakadályozása, illetve törlése – a jogszabályi és a belső szabályozási követelmények betartásával.

Adatok biztonsági osztályba sorolása

Az adatok tudatos értékelése és minősítése az érzékenységi fok és a kritikusság alapján.

Az egyes biztonsági osztályok:

a) alapbiztonsági osztály,

b) fokozott biztonsági osztály,

c) kiemelt biztonsági osztály.

Minden rendszert minősíteni kell az általa kezelt adatok minősítésének figyelembe vételével. Amennyiben egy rendszer több kategóriába eső adatot kezel, a legmagasabb kategóriát kell a rendszer minősítésének tekinteni.

Adatvédelem

Az adatok kezelésével kapcsolatos törvényi szintű jogi szabályozás formája, amely az adatok valamilyen szintű, előre meghatározott csoportjára vonatkozó adatkezelés során az érintett személyek jogi védelmére és a kezelés során felmerülő eljárások jogszerűségeire vonatkozik.

Alapfenyegetettség

A fenyegető tényezők olyan csoportosítása, amely a biztonsági alapfunkciók valamelyikének kiesését okozza:

a) a működőképesség elvesztése;

b) a hitelesség elvesztése;

c) a bizalmasság – titkosság elvesztése;

d) a sértetlenség – integritás elvesztése;

e) a rendelkezésre állás elvesztése.

Alkalmazás

Olyan program, amelyet az alkalmazó saját igényei, céljai érdekében használ, és amely a hardver és az üzemi rendszer funkcióit használja.

Alkalmazásgazda

Az üzemeltetés belső szabályozásában meghatározott értelemben.

Alkalmazói program (alkalmazói szoftver, alkalmazás, felhasználói program)

Olyan program, amelyet az alkalmazó saját speciális céljai érdekében vezet be, és amely a hardver és az üzemi rendszer funkcióit használja.

Állásidő

Az a teljes időtartam, amely alatt egy szolgáltatás, vagy komponens nem működik a megállapodott szolgáltatási időn belül. A szolgáltatás, vagy komponens meghibásodásától a normális működés újraindulásáig mérik.

Archiválás

Inaktív adatoknak eredetitől eltérő – általában egyszer írható – médiára való másolása hosszú távú megőrzés céljából. Gyakran együtt jár az adatok eredeti példányának törlésével.

Archívum

Dokumentációs gyűjtemény, irattár.

Informatikai értelemben: a mindennapi működés során (már) nem használt dokumentumok tárolására szolgáló informatikai rendszer, amelyben a dokumentumokat fizikailag egy példányban, nem módosítható formában, eredeti példányként tárolják, biztosítva későbbi a visszaolvashatóságot.

Back-up rendszer

Az adatbiztosítás során az adatok rendelkezésre állását lehetővé tevő másolatokat őrző rendszer. Rendszerint minimális tartalékkal rendelkező informatikai rendszert is értenek alatta.

Bejelentkezés

A felhasználótól kapcsolatot kezdeményez az informatikai rendszer irányába, amelynek során az informatikai rendszer azon funkcióinak használata lehetővé válik, amelyekhez jogosultsággal rendelkezik.

Belépés

Személyek belépése olyan területekre, például helyiségekbe, amelyekben az informatikai rendszert, illetve egyes elemit tárolják, vagy használják.

Bizalmasság – titkosság

Az információhoz csak azok a természetes és jogi személyek férhetnek hozzá, akiket erre feljogosítottak, és azok is csak az előírt módon. Az adatok biztonsági osztályba sorolása meghatározza azok kezelési módját a bizalmasság – titkosság vonatkozásában is.

Biztonság

Veszélyektől vagy bántódástól mentes (zavartalan) állapot. A rendszerek szabályszerű működésének és a működőképesség fennmaradásának kedvező állapota. Lásd még: Informatikai biztonság.

Biztonsági esemény

A szabályszerű működés sérülése, olyan kedvezőtlen változás, amelynek hatására a biztonság állapota sérül. Fenyegetés a biztonságra nézve, illetőleg figyelmeztető jel a fenyegetésre vagy annak lehetőségére.

Informatika értelemben: az adatok, információk bizalmasságának – titkosságának és / vagy sértetlenségének és / vagy rendelkezésre állásának megsérülése vagy a sérülés lehetősége.

Biztonsági környezet

A szervezet működésének, fejlődésének és fennmaradásának, az erőforrások felhasználásának és a termékek / szolgáltatások létrehozásának keretrendszere, amely a külső jogi és egyéb szabályozások, a szervezet belső szabályai, szokásai, normái, az ott dolgozók szakértelme és tudása, valamint egyéb külső elemek összessége által meghatározott módon működik. Vagyis a tágan értelmezett szervezeti környezet egészére figyelemmel kell lenni a biztonsági kérdé- sek megválaszolásakor.

Biztonsági követelmények

A kockázatelemzés eredményeként meghatározott fenyegető tényezők ellen irányuló biztonsági szükségletek együttese.

Biztonsági tudatosság

A szervezet kultúrájának része, olyan gondolkodás- és magatartásmód, amely biztosítja, hogy a munkatársak személyes elkötelezettségből elismerik a biztonsági intézkedések jogosságát, betartják azokat, és másokkal is megismertetik, illetve betartatják ezeket.

Egyenszilárdságú biztonság

A szervezet valamennyi tevékenységét átfogó, minden ponton (közel) azonos erősségű biztonság.

Elektronikus aláírás

A levelezőrendszer azon szolgáltatása, melynek segítségével a levél címzettje megbizonyosodhat a küldő személyéről, arról, hogy a levelet a továbbítás során senki sem módosította, valamint a küldő sem tagadhatja le a levél elküldésének tényét.

Eseménynaplózás

Tevékenységek időrendi rögzítése, regisztrálása, illetve a készített naplók megőrzése. Annak biztosítása, hogy a megtörtént események, végrehajtott műveletek, lezajlott eljárások utólag rekonstruálhatóak és elemezhetőek legyenek, azért, hogy az

illegális vagy nem megfelelő te- vékenységek feltárásra, jelentésre, illetve bizonyításra kerülhessenek.

Az eseménynaplózáskor rögzíteni kell:

a) a tevékenység azonosítását;
b) amennyiben a tevékenység hozzáféréssel kapcsolatos, akkor a felhasználó és a végberendezés azonosítását;
c) a bejelentkezés és a kijelentkezés dátumát és időpontját;
d) továbbá a sikeres mellett a sikertelen rendszer-, adat- és erőforrás-elérési kísérleteket is.

Eszkaláció

Egy incidensről, problémáról, vagy változtatásról szóló információ továbbadása és/vagy intézkedés kérése a rangidős személyzettől (hierarchikus eszkaláció), vagy más szakértőtől (funkcionális eszkaláció). Az eszkalációs szabályokat a prioritási célokhoz kapcsolják.

Eszköz

Szó szerinti jelentése tulajdonolt értékes személy, vagy tárgy; az eszközök gyakran megjelennek a mérlegben, mint a szervezet kötelezettségeivel szembeállított tételek.

Az informatika-szolgáltatás folytonosságának biztosításában, a biztonsági átvizsgálásban és menedzsmentben az eszköz olyan tétel, amellyel kapcsolatban fenyegetések és sebezhetőségek azonosíthatók, számolhatók, a kockázatelemzés elkészítésének céljából. Ebben az érte- lemben a szolgáltatások vizsgálatában az eszköz fontossága számít és nem annak a költsége.

Észlelés

Az incidens életciklusának második állomása az előfordulás után, amikor a szolgáltatás hibája ismertté válik az informatikai szervezet számára.

Feladatkör

Valamely természetes vagy jogi személyre háruló, összetartozó feladatok (vagyis kötelességszerűen elvégzendő dolgok) összessége.

Feladatmegosztás

Az informatikai rendszereket használó és üzemeltető személyek feladatköreit úgy kell meghatározni, hogy azzal minimalizáljuk a mulasztások és szándékos visszaélések kockázatát, ugyanakkor biztosítsuk a minél teljesebb körű helyettesítés vagy kiváltás lehetőségét. Célja, hogy minden folyamat lefutásába beleépüljön a kontroll – vagyis egyetlen személy se tudja (szándékosan vagy gondatlanságból) megakadályozni valamely folyamat lefutását, illetve a szervezet számára károsan eltéríteni azt eredeti rendeltetésétől. A feladatmegosztás kialakítása biztonsági vezetői feladat.

Feladatelhatárolás

Az informatikai biztonság szempontjából összeférhetetlen munkakörök szétválasztása a szükséges tudás elve alapján, vagyis: a kiemelt biztonsági osztályba tartozó vagyon tulajdonosa meghatározza a felhasználók számára munkahelyi kötelezettségeik függvényében

jogosultságaikat (az adatkezelésre, információkezelésre, rendszerek esetében ezek használatára vonatkozóan). A feladatelhatárolások kialakítása biztonsági vezetői feladat.

Felelős

A rábízott dolgokról, személyekről, feladatokról számot adni, a velük kapcsolatos anyagi, jogi stb. következményeket viselni köteles természetes vagy jogi személy.

Felhasználó

Az a személy, vagy szervezet, aki, amely egy, vagy több informatikai rendszert használ feladatai ellátásához.

Felhasználói azonosítás és hitelesítés

A felhasználói azonosítás és hitelesítés jelenti a rendszerekhez, adatokhoz, adatkezelési formákhoz történő hozzáférés alapját.

Felhasználói azonosítás: az informatikai rendszer minden felhasználóját egyedi azonosítóval kell ellátni az eseménynaplózás céljainak érdekében. Egyes kivételes esetekben kiadható osztott azonosító is egy használói csoport számára.

Felhasználói hitelesítés: folyamat, melynek során megtörténik az azonosított felhasználó hitelességének ellenőrzése, annak igazolása, hogy ténylegesen az-e, akinek állítja magát, s ha tényleg az, akkor megtörténik jogainak érvényesítése.

Fizikai biztonság

A fizikai erőforrások szabályszerű működésének és a működőképesség fennmaradásának kedvező állapota.

Informatikai értelemben: az információ bizalmasságának – titkosságának, sértetlenségének – integritásának és rendelkezésre állásának megőrzése – fizikai oldalról. Pl. belépési engedélyek és korlátozások, zárrendszerek, tűzvédelmi rendszerek, robbanás- és földrengésvédett kialakí- tás, lopás és rongálás elleni védelem révén.

Funkcionalitás

Mindazon tevékenység, rendeltetés és feladat, amit egy adott rendszer, program vagy eszköz képes nyújtani, illetve elvégezni a felhasználó számára. Az informatikai rendszerek esetében a különböző adatok kezelésének, az eljárások végrehajtásának biztosítása a működési folyamatok támogatására – melyet a rendszer megfelelő tervezése és hatékony működtetése tesz lehe tővé.

Gépterem

Szervert, vagy az IT-infrastruktúra szempontjából kiemelkedő fontosságú berendezést (pl. switchet) is tartalmazó, de nem kizárólag ezek tárolására használt terem. Ilyen pl. az olyan rendszergazdai szoba, melyben szerver működik.

Harmadik fél

Az adatkezelés kapcsán harmadik félnek minősül az a szervezet állományába nem tartozó, külső természetes vagy jogi személy:

a) akire a szervezet birtokában lévő adatok vonatkoznak;
b) akik valamilyen szerződéses vagy egyéb jogilag szabályozott kapcsolat keretében

a szervezet valamely adataival kapcsolatban adatkezelést végeznek.

Hardver

Az informatikai rendszer eszközeit, fizikai elemeit alkotó részei.

Hatáskör

Intézkedési jog köre, érvényességi határa. A munkakör betöltőjének a feladatai ellátása érdekében szükséges cselekvési jogosultságai. Fajtái:

a) döntési,
b) véleményezési,
c) javaslattételi,
d) információadásravonatkozó,
e) valamint információ megkapásáravonatkozó.

Hálózat

Két vagy több számítógép, vagy általánosabban informatikai rendszerek összekapcsolása, amely informatikai rendszerek legkülönbözőbb komponensei között adatcserét tesz lehetővé.

Hálózatmenedzser

Az üzemeltetés belső szabályozásában meghatározott értelemben.

Helyi rendszer

Használata, üzemeltetése egy intézetre korlátozódik.

Helyreállítási idő

Valamely informatikai szolgáltatás vagy információtechnológiai komponens hibája esetén a normál működés állapotába történő visszaállításhoz szükséges időtartam.

Hiba

Az a körülmény, amely előidézi, hogy egy funkcionális egység képtelen lesz a tőle megkívánt funkció ellátására.

Hitelesség

Az adatnak az a tulajdonsága, amely megmutatja, hogy bizonyítottan vagy bizonyíthatóan az elvárt forrásból származik-e.

Hozzáférés

Olyan eljárás, amelynek révén az arra jogosult személy számára elérhetővé válik, amire szüksége van. A hozzáférés jog, mely felelősséggel jár.

Informatikai értelemben: a hozzáférés eljárásán keresztül az informatikai rendszer jogosult használója számára – jogosultságainak megfelelően – elérhetővé válnak a rendszerben tárolt adatok, valamint az ezeken történő adatkezelés. Az adatokhoz, információkhoz és rendszerekhez való hozzáférést az üzemeltetési és a biztonsági követelmények alapján ajánlatos kialakítani, ellenőrzés alatt tartani és menedzselni.

A hozzáférés két fajtája:

1) fizikai hozzáférés: olyan eljárás, amelynek révén az arra jogosult személy számára elérhetővé válnak az informatikai rendszer meghatározott hardver elemei;
2) logikai hozzáférés: olyan eljárás, amelynek révén az arra jogosult személy számára elérhe-

tővé válnak az informatikai rendszer meghatározott szoftver elemei.

Humán biztonság

A humán erőforrásokkal kapcsolatban álló rendszerek szabályszerű működésének és a működőképesség fennmaradásának kedvező állapota.

Informatikai értelemben: az információ bizalmasságának – titkosságának, sértetlenségének – integritásának és rendelkezésre állásának megőrzése – humán oldalról. Pl. az alkalmazotti és egyéb szerződések előtti informálódás, a szerződés létrejöttekor titoktartási megállapodás megkötése, a munkaköröknél a biztonsági feladatok, hatáskörök és felelősségek rögzítése révén.

Informatika

A számítógépes információrendszerek tudománya, amely elméletet, szemléletet és módszertant ad a számítógépes információrendszerek tervezéséhez, fejlesztéséhez, szervezéséhez és működtetéséhez.

Informatikai biztonság

Olyan állapot, amelyben az informatikai rendszer védelme – a rendszer által kezelt adatok bizalmassága, sértetlensége, hitelessége, illetve rendelkezésre állása és működőképessége szempontjából – zárt, teljes körű, folyamatos és a kockázatokkal arányos.

A védelem zárt, ha az összes releváns tényezőt figyelembe veszi. Teljes körű a védelem, ha a védelmi intézkedések az összes rendszerelemre kiterjednek. A folyamatos védelem jellemzője, hogy az időben változó körülmények ellenére megszakítás nélkül, állandóan megfelelő mértékű védelmet nyújt. Ha a védelem a kockázattal arányos, akkor hosszú távon a védelem költségei arányosak a potenciális kárértékkel. Ezt az arányt a Biztonsági Politika határozza meg.

Informatikai infrastruktúra

Az információ áramoltatását és feldolgozását lehetővé tevő, a számítógépek és felhasználók összekapcsolására szolgáló fizikai hardver és szoftver. Tartalmazza az adatátviteli közeget, pl. telefonvonalakat, kábeltelevíziós vonalakat, műholdakat és antennákat, továbbá routereket, és más számítógép-hálózati aktív elemeket és egyéb, az adatátvitelt vezérlő berendezéseket. Tartalmazza továbbá a továbbított jelek küldéséhez, fogadásához és kezeléséhez szükséges szoftvereket.

Informatikai rendszer

A hardverek és szoftverek olyan kombinációjából álló rendszer, amit az adat- illetve információkezelés különböző feladatainak elvégzésére alkalmazunk, ezáltal támogatva a szervezet működési folyamatait.

Az informatikai rendszer elemei, melyek részt vesznek a biztonságos működés megvalósításában és fenntartásában, illetve amelyek a veszélyek által érintettek lehetnek.

Ezek:

a) az informatikai infrastruktúra:

b) a szervezet,

c) a számítógépek (célszámítógépek, illetve általános célú számítógépek),
d) a hálózat,
e) a hardver elemek,
f) a szoftver elemek,
g) illetve a szoftverrel kapcsolatos telekommunikáció,
h) az egyéb (pl. telekommunikáció),
i) a dokumentációk,
j) valamint a humán elemek: az informatikai rendszerrel – az informatikai szervezet állományán kívül – kapcsolatba kerülő természetes és jogi személyek, valamint jogi személyiség nélküli gazdasági társaságok.

Az informatikai rendszerek különleges tulajdonsága a szabad programozhatóság.

Informatikai szervezet

Ide értendő minden informatikával foglalkozó szervezet, függetlenül nagyságától, hatásköreitől, intézetben elfoglalt helyétől. (pl.: informatikai csoport, osztály, informatikai központ).

Informatika-szolgáltatás

Létező informatikai rendszerek működtetésének és hozzáférhetőségük biztosításának tevékenységköre. Szűkebb, mint az informatikai szolgáltatások tevékenységköre.

Integritás

Teljesség és épség. Ezek fenntartása megkívánja az adatok védelmét a nem engedélyezett változtatástól és rongálódástól.

Informatikai szolgáltatás

Szolgáltatási tevékenység az informatika területén. Információtechnológián alapuló rendszerek által működtetett kapcsolódó funkciók rendszere, amely egy vagy több szervezeti tevékenységet támogat. Bár számos hardver, szoftver, telekommunikációs elem alkotja, a felhasz- náló számára koherens és önálló entitásként érzékelhető.

Informatikai szolgáltatás lehet valamely egyszerű alkalmazás, (pl. egy főkönyvi rendszer elérése, de lehet egy komplex, számos alkalmazást tömörítő csomag, pl. iroda- automatizáció).

Tágabb tevékenységkör, mint az informatikaszolgáltatás, mert ezen túlmenően tartalmazza az új informatikai rendszerek létrehozására irányuló szolgáltatásokat (pl. rendszerintegráció, alkalmazásfejlesztés és –integráció), valamint az informatikai tanácsadás és oktatás tevékenységeit is.

Az informatikai szolgáltatási egység vezetője felel a szolgáltatás minőségéért. Egyenrangú az alkalmazásfejlesztési vezetővel, valamint a pénzügyi és adminisztrációs vezetővel.

Informatikai védelmi intézkedés

Mindazon fizikai, logikai, valamint humán alapú óvintézkedések (technológiai, belső szabályozási, jogi stb. megoldások révén)

a) amelyek csökkentik az informatikai biztonság sérülésének lehetőségét;

b) illetőleg amelyek a sérülés bekövetkeztekor csökkentik a felmerülő károkat.

Információ

Bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságot csökkent vagy szüntet meg.

Információkezelés

Az adatkezelés definíciójából levezethető.

Internet

TCP/IP protokollon alapuló, nyilvános, világméretű számítógépes hálózat.

Az egész világot behálózó kommunikációs közeg, melyben hálózatok és számítógépek csatlakoznak egymáshoz (hálózatok hálózata) és amelyen emberek és alkalmazások információt cserélnek egymással.

Az Internetnek talán legismertebb része a Web (WWW), további részei: Usenet, Arpanet, Bulettin Boards, különböző on-line szolgáltatások és egyéb hálózatok.

Ismert hiba

Egy konfigurációs elem hibája, amelyet egy probléma sikeres diagnózisa felismert, és amelyhez egy ideiglenes megkerülő megoldást, vagy egy végleges megoldást találtak. Az ismert hiba és a konfigurációs elem kapcsolata eredhet egy probléma helyi diagnózisából, de származhat külső forrásból is. Fontos, hogy minden lényeges ismert hibát rögzítsünk a konfigurációkezelés adatbázisába (CMDB), bár az nyilván nem az ismert hibák adatainak egyetlen forrása. Mivel sok problémának több kiváltó oka lehet, az egyes problémák és az egyes ismert hibák közötti kapcsolat esetenként igen komplex. (Jó példa egy ismert hibára, amikor a hibát az adott szoftver következő kiadásában fogják csak kijavítani, addig együtt kell élni vele.)

IT

Informatika

ITIL (Mozaikszó: Information Technology Infrastructure Library)

Az informatikai szolgáltatás menedzsment módszertana.

Jogosultság

Valamire jogosító jogi helyzet, állapot. A lehetőség megléte valamely tevékenység végrehajtására.

Informatikai értelemben: a jogosultság jog az adatkezelésre, információkezelésre, illetve a különböző rendszerek, programok, eszközök használatára.

Jogosultsági rendszer

A szervezethez tartozó belső és külső felek jogosultságainak rendszere (felhasználói csoportok, illetve az általuk végezhető műveletek rendszere), illetve az e rendszer menedzseléséhez kapcsolódó feladatok összessége.

A jogosultsági rendszer értelmezhető egy-egy alkalmazás szintjén is (pl. egy levelezési rendszerre).

Kapacitásmenedzsment

Az a szolgáltatásirányítási folyamat, amelynek feladata az informatikai kapacitásra vonatkozó üzleti igények meghatározása, mind technikai, mind üzleti értelemben, valamint annak megértése és bemutatása, hogy e tevékenységmennyiségeknek az informatikai infrastruktúrán a megfelelő időben és optimális költséggel történő megtermelése milyen következményekkel jár.

Katasztrófa

Informatikai rendszer, rendelkezésre állásának megszűnése, vagy nagymértékű csökkenése.

Katasztrófa-elhárítási terv

A katasztrófa elhárítási terv – informatikai vonatkozásban – tartalmazza mindazokat az információkat, melyek szükségesek egy esetleges katasztrófa bekövetkezte után az informatikai szolgáltatások ellenőrzött, egy előre megállapított szinten történő helyreállításához. A terv világos útmutatást ad érvényes a személyi felelősségekre, illetve az elvégzendő tevékenységekre vonatkozóan, illetve arra is, hogy hogyan, és mikor kell használni.

Kijelentkezés

A felhasználótól kezdeményezésére az informatikai rendszer irányába, amelynek során az informatikai rendszer számára biztosított funkcióinak használata lehetővé válik.

Kockázat

Valamely cselekvéssel járó veszély, veszteség lehetősége. A fenyegetettség mértéke, amely valamely fenyegető tényezőből ered, és amelyet a kockázatelemzés során a fenyegető tényezők értékelése révén tárunk fel. A kockázat a kárnagyság és a bekövetkezési valószínűség (gyakoriság) szorzata.

Kockázatértékelés

Az információ és az informatikai eszközök fenyegetettségének, sérülékenységének és befolyásolhatóságának, valamint ezek előfordulása valószínűségének felbecslése, vagyis:

a) a kockázati tényezők feltárása;
b) a feltárt tényezők kvalitatív értékelése;
c) a kritikus tényezők kiválasztása;
d) szükség esetén a kritikus tényezők mélyebb értékelése.

Kockázatkezelés

Az informatikai rendszerre hatással bíró biztonsági kockázatok kezelése, minimalizálása, megszüntetése érdekben elfogadható költségen kockázatmenedzsment rendszer működtetése, ennek keretében:

a) az informatikai kockázatkezelési stratégia meghatározása;
b) az informatikai kockázatkezelés kereteinek kijelölése;
c) az informatikai kockázatkezelési kontroll működtetése:

- a kockázatok azonosítása;
- a kockázatok elemzése;
- az eredmények értékelése – a kockázatok „irányítása";
- a kockázatok monitorozása, megfigyelése;

d) valamint e rendszer felülvizsgálata, fejlesztése, megismertetése a szervezettel,

e) illetve a közreműködők képzése.

Konfigurációkezelés

A konfigurációs elem azonosításának, felügyeletének és ellenőrzésének folyamata egy szolgáltatáson belül, állapotának feljegyzése, jelentése, a változáskezelés támogatására annak felmérése, hogy az elemek megváltoztatásának milyen potenciális informatikai hatása van.

Konfigurációs állomány

A konfigurációs elemek adatait tartalmazó, eszköz funkciónként különböző állomány. Ezeket a konfigurációkezelési könyvtárban kell elhelyezni.

Konfigurációs elem

A konfigurációs elem egy informatikai infrastruktúra bármely komponense lehet, beleértve a dokumentációs elemeket is, mint például egy szolgáltatási megállapodás, vagy egy változtatási kérelem, amely a konfigurációkezelés felügyelete alatt áll (vagy kell állnia), és így a változásfelügyelet hatáskörébe tartozik. Legalacsonyabb szintű konfigurációs elem rendszerint az a legkisebb egység, amely a többi összetevőtől függetlenül megváltoztatható. A konfigurációs elemek bonyolultságban, méretben és típusban széleskörűen eltérhetnek, egy teljes szolgáltatástól (beleértve az összes hardvert, szoftvert, dokumentációt, stb.) egy programmodulon át egy kisebb hardverösszetevőig. Az összes meglévő vagy potenciális szolgáltatási probléma kapcsolható kell, hogy legyen egy, vagy több konfigurációs elemhez.

Központi rendszer

Azon rendszer, amelyik kilép egy Intézet keretei közül.

LAN (Local Area Network):

Helyi hálózat.

Logikai biztonság

Logikai (szoftver) erőforrások szabályszerű működésének és a működőképesség fennmaradásának kedvező állapota.

Informatikai értelemben: az információ bizalmasságának – titkosságának, sértetlenségének – integritásának és rendelkezésre állásának megőrzése – logikai oldalról. Pl. azonosítók, jelszavak, hozzáférési jogok és jogosultsági szintek révén.

Meghibásodás

Meghibásodás akkor történik, amikor a funkcionális egység már nem felel meg a céljának.

Megbízhatóság

Egy informatikai összetevő azon képessége, hogy ellásson egy tőle jogosan elvárt funkciót meghatározott körülmények között, egy meghatározott időtartamra.

Megkerülő megoldás

Eljárás egy incidens, vagy probléma elkerülésére, egy ideiglenes javítással, vagy egy olyan technikával, amely azt eredményezi, hogy az ügyfél nem függ attól a konfigurációs elemtől, amely ismerten hibát okoz.

Megoldás

Az a tevékenység, amely elhárít egy incidenst, vagyis lehetővé teszi a felhasználók számára munkájuk folytatását. Lehet ideiglenes megkerülő megoldás, vagy a hibás konfigurációs elem végleges megjavítása vagy cseréje.

Mentés

Aktív adatoknak az eredetitől eltérő adathordozóra másolása, biztonsági megőrzés, valamint meghibásodás, vagy katasztrófa bekövetkezése után az eredeti állapot visszaállításának megvalósíthatósága céljából.

Munkakörökhöz tartozó érzékenységi szint

A feladatmegosztás és feladatelhatárolás elveiből levezethető az egyes munkakörök érzékenységi szintje – a munkakörhöz kapcsolódó adatok, információk és rendszerek biztonsági osztályokhoz való tartozása alapján. Az IT biztonsági vezető jóváhagyja, véglegesíti a kategóriákat és besorolásokat.

Probléma

Megoldásra váró elméleti, gyakorlati kérdés. Egy, vagy több létező, vagy potenciális incidens ismeretlen eredeti oka. Nehezen megoldható kérdés, felmerült gond.

Vagy egy egyedi, jelentős hatású esemény, amelynek hatása nagymértékben rontja a felhasználók számára nyújtott szolgáltatás minőségét; vagy megegyező tüneteket mutató események sorozata, amelyek valamilyen közös, de ismeretlen eredetű okra vezethetők vissza.

Problémakezelés

Az a folyamat, amely a tényleges és potenciális meghibásodások eredeti okát felismeri. Elsődleges célja annak biztosítása, hogy a szolgáltatások biztosak, pontosak legyenek és a problémák bekövetkezésének, illetve ismétlődésének esélye csekély legyen. A folyamat fejlettségét a probléma megelőzésre való képessége mutatja.

Program

Egy számítógép műveleteinek típusát és sorrendjét meghatározó utasítások sorozata. Eljárási leírás, amely valamely informatikai rendszer által közvetlenül vagy átalakítást követően végrehajtható.

Rendelkezés

Utasítás, intézkedés. Az a lehetőség, hogy valaki rendelkezhet valakivel, valamivel, utasítást adhat, munkát irányíthat, dönthet valamiben.

Rendelkezésre állás

Az a tényleges állapot, amikor is egy informatikai rendszer szolgáltatásai – amely szolgáltatások különbözők lehetnek – állandóan, illetve egy meghatározott időben

rendelkezésre állnak és a rendszer működőképessége sem átmenetileg, sem pedig tartósan nincs akadályozva.

Ebben az összefüggésben jelentősége van az információ vagy adatok rendelkezésre állásának, elérhetőségének is.

Rendelkezésre-állási arány

Annak az időnek az aránya, amely alatt a szolgáltatás ténylegesen elérhető a felhasználó számára az elfogadott szolgáltatási időn belül.

Az elfogadott szolgáltatási időszakot a Szolgáltatási Szint Megállapodás tartalmazza).

Rendelkezésre állás (%) = rendelkezésre állási idő / elfogadott szolgáltatási időszak. (Pl. ha egy szolgáltatás a 40 órás szolgáltatási periódusban 39 órán keresztül áll rendelkezésre, akkor a rendelkezésre állás ez esetben 97.5%).

Rendszer

A rendszer egynemű vagy összetartozó dolgoknak, jelenségeknek, cselekvéseknek, tevékenységeknek bizonyos törvényszerűségeket mutató, bizonyos elvekhez igazodó rendezett egésze.

Rendszergazda

Az üzemeltetés belső szabályozásában meghatározott értelemben.

Rendszerelemek

Az informatikai rendszer részét képező elemek.

Rendszerelem csoportok:

a) az informatikai rendszer környezetét alkotó infrastruktúra,
b) az informatikai rendszer hardverelemei,
c) az informatikai rendszer szoftverelemei,
d) az informatikai rendszer kommunikációs elemei,
e) adathordozók,
f) az informatikai rendszerre vonatkozó dokumentációk,
g) az informatikai rendszerben részt vevő emberi erőforrások.

Rendszer-monitorozó eszközök

Az egész rendszerről gyűjtenek információt, illetve valamilyen csoportosító szempont alapján.

Rendszerprogram (rendszer szoftver)

Olyan alapszoftver, amelyre szükség van, hogy valamely informatikai rendszer hardvereit használhassuk, és az alkalmazói programokat működtessük. A rendszerprogramok legnagyobb részét az operációs rendszerek alkotják.

Rendszerszoftver

A számítógépek működéséhez szükséges, elengedhetetlen, alapvető programok. (pl.: operációs rendszer, víruskereső, e-mail kliens, webböngésző, stb.)

Riasztás

Egy küszöbérték eléréséről (amely hiba megtörténtét vagy valószínű bekövetkezését jelzi) vagy más eseményről (betörési kísérlet, kommunikációs kapcsolat lebontása, stb.) történő jelzés.

Sebezhetőség

Valamilyen támadás esetén az erőforrások sérülésének lehetősége.

Sértetlenség – Integritás

Eredeti teljesség, épség, sértetlenség. Az adat / információ / rendszer hitelességének, pontosságának, teljességének állapota.

A sértetlenséget általában az információkra, adatokra illetve a programokra értelmezik. Az információk sértetlensége alatt azt értjük, hogy az információkat csak az arra jogosultak változtathatják meg, illetve, hogy azok véletlenül nem módosulhatnak. Ez az alap veszélyforrás a programokat is érinti, mivel az adatok sértetlenségét csak rendeltetésszerű feldolgozás és átvitel esetén lehet biztosítani.

A sértetlenség fogalma alatt gyakran értik a sértetlenségen túl a teljességet, továbbá az ellentmondás-mentességet és a korrektséget – együttesen: az integritást. Az integritás ebben az összefüggésben azt jelenti, hogy az információ valamennyi része rendelkezésre áll, elérhető. Korrektek azok az információk, amelyek a valós dologi vagy – pl. modellezésnél – feltételezett állapotot helyesen írják le.

Sürgősség

Olyan incidens, probléma vagy változtatás üzleti kritikusságának mértéke, amelynek hatása van az üzleti határidőkre. A sürgősség tükrözi a javításra vagy megkerülésre rendelkezésre álló időt, amelyből való kicsúszás hatását az üzlet megérzi. A hatással és talán a műszaki súlyossággal együtt ez a legfőbb eszköz az incidensek, problémák vagy változtatások prioritásának meghatározására.

Számonkérhetőség

Az eseménynaplózás, valamint tágabb értelemben a különböző kontroll-mechanizmusok révén annak biztosítása, hogy a megtörtént események, végrehajtott műveletek, lezajlott eljárások utólag rekonstruálhatóak és elemezhetőek legyenek, azért, hogy az illegális vagy nem megfelelő tevékenységek feltárásra, jelentésre, illetve bizonyításra kerülhessenek.

Szerep

Foglalkozással, feladatkörrel kapcsolatos, illetve az egyéniségből folyó szokásos magatartás. Valamely folyamatban betöltött működési kör, megvalósított feladat, valaminek jutó rész.

Szoftver

Valamely informatikai rendszer olyan logikai része, amely a működtetés vezérléséhez szükséges.

Szerverterem

Szervert és/vagy az IT infrastruktúra szempontjából kiemelkedő fontosságú berendezést (pl. switchet) tartalmazó, és kizárólag ezek tárolásra használt terem.

Szoftverzavar

Nyilvánvalóan hibás szoftverműködés. Pl. „kék-halál", értelmezhetetlen hibaüzenet.

Szolgáltatási időszak

Azok az időszakok, melyekben egy meghatározott informatikai rendszer vagy szolgáltatás elérhető a felhasználó számára.

Szolgáltatási megállapodás (SLA: Service Level Agreement.)

Részletesen tartalmazza az IT-szolgáltató és ügyfele közötti megállapodásokat az egyes szolgáltatások minőségére (szintjére) vonatkozóan.

Szolgáltatási szint megállapodás (SLA)

Írott megállapodás (szerződés) a felhasználói közösség és az informatikai szolgáltató egység között, amely dokumentálja az elfogadott szolgáltatási szintet valamely informatikai szolgáltatás kapcsán.

Jellemzően kiterjed:

a) a szolgáltatási időszakra;
b) a szolgáltatás rendelkezésre-állására;
c) a felhasználói támogatás szintjére;
d) a terminál válaszidőkre;
e) a különféle korlátozásokra;
f) a funkcionalitásra
g) és a katasztrófa szituáció esetén nyújtandó szolgáltatási szintre

Tartalmazhatja továbbá:

a) a biztonsági
b) és az esetleges számlázási elveket is.

Szolgáltatási szint menedzsment

Az ügyfeleknek nyújtott szolgáltatási szintek menedzselésének és az elvárt és megvalósított szolgáltatási szintek összevetésének folyamata.

Szolgáltatáskatalógus

Az adott szervezet által másoknak nyújtott szolgáltatások definiálása, dokumentálása, pl. ki az adott szolgáltatás menedzsere, mely munkacsoport felelős érte.

Szolgáltatásmenedzsment

Az üzlet-informatika összehangolás egyik eleme. Az a magas szintű folyamat, amely irányítja az informatikai szolgáltatást az ügyfelek nevében. Jogköre van döntéseket hozni az informatikai szolgáltatás teljes portfoliójának nyújtásáról. Az ITIL úgy tekinti a szolgáltatásmenedzsmentet, mint egy átfogó filozófiát, amely áthatja az egyedi ITIL folyamatok működtetését.

Szolgáltató

Egy szervezet, amely szolgáltatásokat vagy termékeket nyújt vevőknek. A szolgáltató lehet belső vagy külső is.

Teszt-környezet

Itt történnek az éles kiadás terítése előtti tesztelések – az éles környezethez hasonló körülmények között.

Titkosítás

Adatok megváltozatása (lefordítás titkos, nem érthető formába, tárolás ebben a formában, valamint visszaalakítás érhető formába) abból a célból, hogy csak a jogosultak ismerhessék meg az adat tartalmát. (Nem tévesztendő össze a titkos adatkezeléssel.)

Jelen szabályzatban nem teszünk különbséget a rejtjelezés (encipherment) és titkosítás (encryption), illetve a rejtjelmegfejtés (decipherment) és a titkosítás visszafejtése (decryption) között.

Tulajdonos

Rendelkezési joggal (adott esetben: kizárólagos rendelkezési joggal) bíró természetes vagy jogi személy.

Informatikai értelemben: egy meghatározott informatikai vagyonelem (hardver, szoftver, információ) felett rendelkezési joggal bíró természetes vagy jogi személy.

Tűzfal

Olyan kapcsolódó programok összessége, amelyek egy hálózati átjáró szerveren működve védik a saját (védeni kívánt) hálózat erőforrásait a külső hálózatoktól, illetve ezek felhasználóitól. A tűzfal célja, hogy a rajta keresztül haladó forgalom engedélyezésén, megtagadásán vagy visszairányításán keresztül naplózza, ellenőrizze és kontrollálja a hálózatokhoz kapcsolódó tevékenységeket.

Ügyfélszolgálat - Help Desk

A kapcsolat az informatika és felhasználói között. Alapfolyamatai az incidenskezelés és a felhasználói igények kezelése, biztosítva, hogy egy hívás (bejelentés) vagy incidens sem marad feldolgozatlanul (nem felejtik el vagy hagyják figyelmen kívül), és hogy a szolgáltatást visszaállítják, amilyen gyorsan csak lehet. Az ITIL új kiadása a segélyszolgálatot kettéosztotta ügyfélszolgálati funkcióra és incidenskezelési folyamatra.

Üzemeltetés-vezető

Az üzemeltetés belső szabályozásában meghatározott értelemben.

Üzemeltetés felügyeleti szoftver

Az informatikai rendszer működésének ellenőrzésére, felügyeletére szolgáló szoftver.

Változás

A menedzselt infrastruktúrában, vagy egy adott szolgáltatás nyújtásához szükséges bármilyen funkcionális egységben bekövetkezett változtatások (több kisebb lépésből álló folyamat) részletes leírása.

Változás-felügyelet

Azok az eljárások, amelyek biztosítják, hogy minden változtatás felügyelt legyen, beleértve a változtatáskérelem benyújtását, naplózását, elemzését, a döntéshozást, jóváhagyást, megvalósítást és a megvalósítás utáni áttekintést is.

Változtatás-kérelem

Az informatikai infrastruktúra bármely összetevőjének vagy az informatikai szolgáltatás bármely jellegének megváltoztatására tett javaslat. Lehet egy dokumentum vagy egy feljegyzés, amelyben szerepel a javasolt változtatás természete, részletei, indoklása és engedélyezése.

Változáskezelés

A változási folyamatok kezeléséhez és dokumentáláshoz nyújt segítséget. Végigkíséri a változásokat azok bejelentésétől a lezárásukig. Több változás projektbe szervezhető és együtt menedzselhető.

Veszélyforrás

Veszélyforrásnak tekintendő mindaz, amelynek hatására, illetve bekövetkeztekor az informatika biztonság sérül: egy vagy több informatikai rendszerelem működésében nem kívánt változás áll be.

A támadás az informatika biztonság valamely pillére ellen ható, valamely veszélyforrásból kiinduló folyamat.

Vírus

Olyan programtörzs, amely illegálisan készült egy felhasználói program részeként. A felhasználói program alkalmazása során átterjedhet, "megfertőzhet" más, az informatikai rendszerben lévő rendszer-, illetve felhasználói programot, sokszorozva önmagát (ami lehet mutáns is) és a logikai bomba hatás révén egy beépített feltételhez kötötten (pl. konkrét időpont, szabad lemezterületi helyek száma stb.) trójai faló hatást indít el.

VPN (Virtual Private Network)

Virtuális magánhálózat. Magánhálózatok összekapcsolása (Site-to-Site VPN), vagy távoli dolgozóknak cégük hálózatához történő kapcsolódása (Remote Access VPN) olyan módon, hogy ennek megvalósításához nyilvános hálózatot (pl. internetet) vesznek igénybe és adataik sértetlenségének, hitelességének és bizalmasságának megteremtésére titkosítást és egyéb védelmet alkalmaznak.

WAN

Wide Area Network. Egy régióra kiterjedő, de gyakran földrészre kiterjedő számítógépes hálózat (pl. Debreceni Egyetem informatikai hálózata).