3. függelék: Fogalomtár és szakkifejezések gyűjteménye

Adat	Az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas.
Adatfeldolgozás	Az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve, hogy a technikai feladatot az adaton végzik.
Adatkezelés	Az alkalmazott eljárástól függetlenül az adaton végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adat további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése.
Adatgazda	Az adatkezelésért felelős szervezeti egység azon, e feladatkör ellátására kijelölt munkavállalója, aki az adatkezelésért felelős szervezeti egység felelősségi körébe tartozó adatkezelések tekintetében, vagy adatkezeléseknek az adatkezelésért felelős szervezeti egység felelősségi körébe tartozó részében gondoskodik az adatkezelőt terhelő feladatok elvégzéséről.
Adatkör	Az adatkör olyan nagyobb adathalmazt határoz meg, amelyek egy témához, tevékenységhez, feladathoz rendelhetők, és az adatgazda (adatgazdák) működési területéhez tartoznak, 1. az adatkörök kialakításánál olyan egységet szükséges megragadni, amely nagyjából azonosan sorolható be bizalmasság, sértetlenség és rendelkezésre állás (röviden: BSR) szerint, 2. az adatkörbe minden adat beletartozik, azaz: a papír alapú és az elektronikus adat is (amely utóbbi lehet IT rendszerben, de akár SharePointon, Excelben tárolt is), a személyes adatok, valamint az üzleti, gazdasági titkok, továbbá bármilyen a vállalat számára jelentőséggel/ értékkel bíró adat, amely az adott területen keletkezik.
Adattovábbítás (adatátadás)	Az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele.
Adattörlés	Az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása a továbbiakban már nem lehetséges.

Főv.Törv.szék Cégb.Cg.: 01 09 203215

Adatvagyon	A Szervezet folyamatai által kezelt Szervezettitkot-, Értékpapírtitkot-, Közérdekű (valamint közérdekből nyilvános) adatokat-, Különleges-, Személyes- és Üzleti titkot képező adatok összessége. Az adatvagyon részét képezik azok az elektronikusan vezetett nyilvántartások, melyek biztonságos, megbízható és hatékony működése a Szervezet szempontjából kiemelt jelentőséggel bírnak.
Adatvédelem	Az adatvédelem a személyes adatok gyűjtésének, feldolgozásának és felhasználásának korlátozásával, az érintett személyek védelmével foglalkozik. Nevével ellentétben tehát nem elsősorban az adatokat védjük, hanem azokat a személyeket, akikkel az adatok összeköthetők. Az adatvédelem magában foglalja a védelmet nyújtó alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összességét. Az adatvédelem a személyes adatok gyűjtésének, feldolgozásának és felhasználásnak korlátozását jelenti, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összességével együtt. (2011. évi CXII. tv.)
Adatzárolás	Az adatok továbbításának, megismerésének, nyilvánosságra hozatalának, átalakításának, megváltoztatásának, megsemmisítésének, törlésének, összekapcsolásának vagy összehangolásának és felhasználásának véglegesen vagy meghatározott időre lehetetlenné tétele.
Adatmegsemmisítés	Az adatot tartalmazó adathordozó teljes fizikai megsemmisítése.
Adathordozó	Az adatok tárolására szolgáló, beépített vagy cserélhető eszközök összefoglaló neve.
Adminisztratív védelem	A védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések, továbbá a védelemre vonatkozó oktatás.
Akkreditálás	Olyan eljárás, amelynek során egy erre feljogosított testület hivatalos elismerését adja annak, hogy egy szervezet vagy személy felkészült és alkalmas bizonyos tevékenységek elvégzésére.

Főv.Törv.szék Cégb.Cg.: 01 09 203215

Alapfenyegetettségek	A fenyegetések általánosított csoportosítása. Alapfenyegetettségnek minősül az alábbiak kritériumok sérülése vagy elvesztése: • bizalmasság, • hitelesség, • sértetlenség, • rendelkezésre állás, • funkcionalitás
Anonimizálás	Olyan információk, amelyek nem azonosított vagy azonosítható természetes személyre vonatkoznak, valamint az olyan személyes adatokra, amelyeket olyan módon anonimizáltak, amelynek következtében az érintett nem vagy többé nem azonosítható.
BSR	Bizalmasság, Sérthetetlenség, Rendelkezésre állás
Bizalmasság	Az adat tulajdonsága, amely arra vonatkozik, hogy az adat csak az arra jogosultak ismerhessék meg, illetve rendelkezhessenek a felhasználásáról.
Bizalmasság elvesztése	A bizalmas adatok illetéktelenek által történő hozzáférését, illetve megismerését jelenti.
Biztonsági esemény	Az informatikai rendszer biztonságában beállt olyan kedvezőtlen változás, melynek hatására az informatikai rendszerben kezelt adatok bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása megsérült vagy megsérülhet.
Biztonsági osztályba sorolás	Az adatnak az adatkezelés során a kezelés módjára, körülményeire, a védelem eszközeire vonatkozó védelmi szintet meghatározó besorolása, osztályozása.
Biztonsági rendszerdokumentáció (BRD)	A biztonsági rendszertervből, a biztonsági követelmények teljesítését tanúsító táblázatból, valamint – ha értelmezhető – a nemteljesítési űrlapból, felhőszolgáltatás igénybevétele esetén a kitöltött felhőbiztonsági követelmény lista, illetve a fentiek alátámasztására szolgáló, csatolt mellékletekből álló dokumentáció.
Biztonsági tesztelés	Az IT- és információbiztonsági terület által a biztonsági követelmények teljesítésére vonatkozó manuális vizsgálat.

Főv.Törv.szék Cégb.Cg.: 01 09 203215

DAC (Discretionary Access Control)	Hozzáférés jogosultság vezérlés, a Discretionary Access Control (DAC - magyarul: Esetenként meghatározott hozzáférés-vezérlés) elve. Tulajdonosi alapokon nyugvó hozzáférést szabályozó rendszer. Szemléletének megfelelően mindenki szabadon, önkényesen rendelkezhet a saját tulajdonában lévő információkkal, azaz jogosultságait továbbadhatja más felhasználóknak.
DLP (Data Loss Prevention)	A Data Loss Prevention (DLP) szó szerinti fordításban „adatvesztés-megelőzést" jelent, de valójában „adatszivárgás-megelőzés" értelemben használják (gyakori fordítás még: „adatszivárgás elleni védelem"). Az adatszivárgás egy biztonsággal kapcsolatos információs technológiai kifejezés, amelyet olyan esetekben használnak, amikor védett, bizalmas adatok valamilyen módon kijutnak, „kiszivárognak" a védett környezetből.
EIR	Elektronikus Információs Rendszer (vagy más néven informatikai rendszer)
Elektronikus irodai rendszerek	Az irodai munkát, illetve az ügyviteli folyamatokat támogató egyedi vagy összekapcsolt, hálózatban üzemelő informatikai és kommunikációs rendszerek.
Ellenőri szerepkör	Olyan speciális szerepkör, amely az adott rendszerben teljes betekintési jog mellett semmilyen végrehajtási joggal nem rendelkezik.
Esemény	A körülmények egy adott összességének bekövetkezése.
Érdekelt felek	Személy vagy csoport, amelynek érdeke fűződik egy szervezet teljesítményéhez vagy sikeréhez.
Érzékeny rendszer	Érzékeny információkat kezelő és feldolgozó rendszer. Az információ akkor tekinthető érzékenynek, ha az információhoz való jogosulatlan hozzáférés súlyos következményekkel járhat az érdekelt felek (pl. tulajdonos, üzemeltető, felhasználó) számára.
Felhasználó	Az a személy, szervezet vagy csoport, aki (amely) egy vagy több informatikai rendszert igénybe vesz feladatai megoldásához.
Fenyegetés	Támadás vagy a biztonság megsértésének lehetősége, a fenyegetés tárgyát képező erőforrással szemben.
Folytonos védelem	Olyan védelmi megoldás, amely az időben változó körülmények és viszonyok ellenére is megszakítás nélkül megvalósul.

Forrásazonosítás	A kockázati források megtalálása, összegyűjtése és jellemzése.
Funkcionalitás	Az informatikai rendszerelem (ideértve az adatot is) tulajdonsága, amely arra vonatkozik, hogy az informatikai rendszerelem a kezelési céloknak megfelel és használható.
Harmadik fél	Olyan személy vagy testület, akit, vagy amelyet az adott kérdésben függetlennek ismernek el a résztvevő felek.
Harmadik ország	Minden olyan ország, amely nem tagja az Európai Uniónak vagy az Európai Gazdasági Térségnek.
Harmadik személy	Olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, amely, vagy aki nem azonos az érintettel, az adatkezelővel vagy az adatfeldolgozóval.
Hálózat	Számítógépek, informatikai rendszerek olyan összekapcsolása, amely az összekapcsolt rendszerek legkülönbözőbb komponensei közötti adatcserét teszik lehetővé.
Háromgenerációs elv	Az informatikai rendszer megvalósításához, és az adatok rendelkezésre állásának biztosításához szükséges olyan megoldás, amely a legutolsó három mentésből állítja vissza az informatikai rendszer működőképességét.
Helyreállítás	A katasztrófa következtében megsérült erőforrások eredeti állapotának biztosítása, eredeti helyen.
Hitelesség	Az adat olyan tulajdonsága, amely arra vonatkozik, hogy az adatot bizonyítottan vagy bizonyíthatóan az elvárt forrásból származik.
IBF	Információbiztonsági Felelős vagy Felügyelő
Illetéktelen személy	Olyan személy, aki az adat megismerésére nem jogosult.
Informatika	A számítógépes információrendszerek tudománya, amely elméletet, szemléletet és módszertant ad a számítógépes információrendszerek tervezéséhez, fejlesztéséhez, szervezéséhez és működtetéséhez.

Informatikai biztonság	Olyan jogszabályok, előírások, szabványok betartásának eredménye, amelyek az információk elérhetőségét, sérthetetlenségét és megbízhatóságát, valamint az informatikai rendszer és elemeinek sértetlenségét és rendelkezésre állását érintik, és amelyeket az informatikai rendszerekben vagy komponenseikben, valamint az informatikai rendszerek vagy komponenseik alkalmazása során megelőző biztonsági intézkedésekkel lehet elérni. Informatikai biztonság alatt valamely informatikai rendszer azon állapota értendő, amelyben a kockázatok és fenyegető tényezők az informatikai rendszerben alkalmazott elfogadható intézkedések hatására az adott kockázati tényezővel arányos védelmet kapnak.
Informatikai rendszer	Információs, ügyviteli, üzletviteli vagy folyamatot, szolgáltatás működését támogató elektronikus adatfeldolgozó eszközök és eljárások, valamint az ezeket kiszolgáló emberi erőforrások és a kapcsolódó folyamatok összessége.
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 felhasználó számára koherens és önálló entitásként érzékelhető. Informatikai szolgáltatás lehet valamely egyszerű alkalmazás, de lehet egy komplex, számos alkalmazást tömörítő csomag.
Információ	Jelentéssel bíró szimbólumok összessége, amelyek jelentést hordozó adatokat tartalmaznak és olyan új ismeretet szolgáltatnak a megismerő számára, hogy ezáltal annak valamilyen bizonytalanságát megszüntetik és célirányos cselekvését kiváltják. Az információ általános értelemben a valóság folyamatairól és dologi viszonyairól szóló felvilágosítás. Ebből következően értelmezése kapcsolatfüggő. Informatikai értelemben, azaz az informatikai rendszereken belül az információk kódolva, adatok formájában fordulnak elő. Ahhoz, hogy az informatikai rendszerben tárolt adatokat ember számára érthetővé tegyük, át kell alakítani, vagy interpretálni, magyarázni kell azokat.
Információ feldolgozó eszközök	Bármely információ feldolgozó rendszer, szolgáltatás, infrastruktúra vagy a fizikai helyek, amelyek befogadják azokat.
Információ biztonsági esemény	Valamely rendszer, szolgáltatás, illetve hálózat meghatározott állapotának előfordulása, amely az információbiztonsági szabályzat lehetséges megsértésére, vagy a biztonsági ellenintézkedések hiányára, vagy a biztonsággal esetleg összefüggő, korábban nem ismert helyzetre utal.

Főv.Törv.szék Cégb.Cg.: 01 09 203215

Információ biztonsági incidens	Nem kívánt vagy nem várt egyedi, vagy sorozatos információbiztonsági események, amelyek nagy valószínűséggel veszélyeztetik az üzleti tevékenységet és fenyegetik az információbiztonságot.
Információs vagyon	Az információs vagyon jelenti mind a védendő információkat, mind azokat az adathordozókat és eszközöket, ahol azok előfordulnak, illetve amelyeken keresztül azok hozzáférhetők. Információs vagyontárgyak lehetnek: - információk: adatbázisok és adatállományok, rendszerdokumentációk, használói/kezelői kézikönyvek, oktatási anyagok, folyamatossági tervek stb. - szoftver vagyontárgyak: alkalmazói szoftverek, rendszerszoftverek, fejlesztési eszközök és szolgáltatások, - fizikai vagyontárgyak: számítógépek (és azok tartozékai, perifériás elemei), hálózati eszközök, adathordozók, egyéb, információkezelő rendszerekhez kapcsolódó műszaki berendezések (légkondicionálók stb.), fizikai hozzáférés ellenőrző eszközök (zárak, beléptető rendszerek).
Információs vagyontárgyak gazdái	Azon személyek, melyek felelősséggel tartoznak a leltár alapján rájuk ruházott eszközökért, szoftverekért, a Szervezet által megvásárolt dokumentumokért, dokumentációkért, és minden egyéb olyan eszközért melyekért a személyi leltár alapján felelősséggel tartozik.
Információvédelem	Az informatikai rendszerek által kezelt adatok által hordozott információk bizalmasságának, hitelességének és sértetlenségének védelme.
Intézkedés	Az IB kockázatkezelés eszközei, beleértve a szabályzatokat, eljárásokat, irányelveket, gyakorlatot vagy szervezeti felépítést, amelyek lehetnek adminisztratív, műszaki, irányítási vagy jogi természetűek.
Irányelv	Leírás, amely megmagyarázza, hogy mit és hogyan kell tenni a szabályzatokban kitűzött célok elérése érdekben
ITSEC	Information Technology Security Evaluation Criteria (Információtechnológia Biztonsági Értékelési Kritériumok) az Európai Közösség ajánlása az IT rendszerek biztonságának funkcionális és minősítési követelményeire.
Kár	A bekövetkezett esemény gazdasági következménye. A kockázatelemzés tekintetében kárnak minősül minden olyan kockázati incidenssel kapcsolatos következmény, ami gazdasági, információs vagy reputációs veszteséggel jár.

IB Kockázatkezelés	Az elektronikus információs rendszerre ható kockázatok csökkentésére irányuló intézkedésrendszer kidolgozása és végrehajtása. A kockázatkezelés a kockázatpotenciál csökkentését jelenti kármegelőzéssel, vagyis a várható negatív esemény bekövetkezési valószínűségének csökkentésével, illetve kárcsökkentéssel, a kárhatás horderejének ellensúlyozásával.
IB Kockázat	A kockázat annak a lehetőségnek a valószínűsége, hogy egy fenyegetés támadás útján kárkövetkezményeket okoz. Más szóval, a *kockázat* az üzleti folyamatokat fenyegető veszélyek (fenyegetettségek) bekövetkezésének valószínűségi értéke.
IB Kockázatelemzés	A kockázatelemzés olyan szakértők által elvégzett, elemző és értékelő jellegű vizsgálat, amely az informatikai rendszerben kezelt adatok és alkalmazások értékelése, gyenge pontjainak és fenyegetettségeinek elemzése útján meghatározza a lehetséges kárértékeket és azok bekövetkezési gyakoriságát.
IB Kockázatelemzésen alapuló vizsgálat (kockázati analízis)	Olyan elemző és értékelő jellegű szakértői vizsgálat, amelynek során a védelmi célok, a rendszer biztonsága feltérképezésre kerül és kockázatelemzés után a nem elviselhető kockázatot jelentő fenyegetéseket kimutatja. A kockázatok felmérése alapján meghatározza a nem elviselhető kockázatokat, amelyek alapján védelmi intézkedési terv készül. A vizsgálat során kockázat-kezelés, intézkedési javaslatok készülnek.
IB Kockázattal arányos védelem	A kockázatokkal arányos a védelem, ha egy kellően nagy időintervallumban a védelem költségei arányosak a potenciális kárértékkel.
IB Kockázatértékelés	A becsült kockázat és az adott kockázati kritériumok összehasonlításának folyamata a kockázat jelentőségének meghatározása céljából.
Katasztrófa elhárítási terv (DRP)	A DRP magába foglalja az üzletmenet (működés) szempontjából kritikus adatok, hardver és szoftver működésének visszaállításához szükséges lépéseket.
Kockázatbecslés	Folyamat, amelynek segítségével értékeket rendelnek a kockázat valószínűségéhez és következményeihez.
Kockázatfelmérés	A kockázatelemzés és a kockázatértékelés átfogó folyamata.
Kockázatcsökkentés	Intézkedések, amelyeket egy kockázattal kapcsolatos valószínűség vagy a negatív következmények (vagy mindkettő) enyhítésére hoztak.

Főv.Törv.szék Cégb.Cg.: 01 09 203215

Kvalitatív (minőségi) kockázatelemzés	A Szervezetet veszélyeztető kockázatok feltárása, a velük kapcsolatba hozható veszélyforrásokkal, hibákkal, kiváltott következményekkel és szabályozásokkal. Az elemzés valószínűségeket, biztonsági mérőszámokat nem állít elő, csupán súlyossági és kockázati szinteket ad meg.
Kvantitatív (mennyiségi) kockázatelemzés	A kockázatot jelentő események bekövetkezési valószínűségének vagy gyakoriságának számszerű meghatározása, a gyenge pontok azonosítása, valamint a bizonytalansági mérőszámok meghatározása és a kapott adatok statisztikai elemzése. Ezeket az eredményeket a modellezési technikák alkalmazásával kapjuk meg.
Legjobb gyakorlat (Best practice)	Olyan rutin szerűén végzett tevékenység, amely széles körű tapasztalatokon alapul, és több, különböző szervezetben is eredményesnek bizonyult.
Legkisebb jogosultság elve	Csak annyi adatot érhessen el és olyan funkciókat végezhessen a munkavállaló, ami a munkavégzéshez, a kijelölt belső folyamatok és tevékenységek ellátásához feltétlenül szükséges.
Letagadhatatlanság	A letagadhatatlanság azon követelmény, amely meghatározza az üzleti életben, hogy a felhasználók egy későbbi időpontban ne tudják, valamilyen okból önkényesen megtagadni az előzőekben általuk végrehajtott tranzakciót.
Maradványkockázat	Az a kockázat, amely alapvetően – kis mértékben – annak ellenére fennmarad, hogy a fenyegető tényezők ellen intézkedéseket tettünk.
Megbízható működés	Olyan működés, amelyet helyesnek érzékelünk bizonyos (pl. a biztonsági politika által előírt) követelmények értelmében.
Mentés	Informatikai folyamat, amelynek során az informatikai, telekommunikációs rendszerben digitálisan tárolt, vagy használatban lévő fontos adathalmazokról egy speciális eszközzel egy speciális adathordozóra (mentési médium) másolatokat készítenek.
Minősítés	Az a döntés, melynek meghozatala során az arra felhatalmazott személy megállapítja, hogy egy adat a tartalmánál fogva a nyilvánosságát korlátozó titokkörbe tartozik.
Mobil eszköz	A mobil eszköz olyan számítástechnikai eszköz, ami fizikailag könnyedén és szabadon mozgatható, és számítási képességei használhatóak mozgatás közben is *(mint pl. mobiltelefonok, tabletek, net- és notebookok, GPS készülékek stb.)*.

Mobil kód	Olyan szoftver vagy kód, mely általában egy távoli számítógépről, hálózaton keresztül letöltve, határozott telepítési vagy indítási procedúra nélkül fut vagy futtatható a kliens gépen. Ilyenek például a scriptek (JavaScript, VBScript), Flash animációk, Java kisalkalmazások, MS Office dokumentumok makrói, ActiveX vezérlők.
Működőképesség	A rendszernek és elemeinek az elvárt és igényelt üzemelési állapotban való fennmaradása. A működőképesség fogalom sok esetben azonos az üzembiztonság fogalommal. Ezen állapot fenntartásának alapfeladatait a rendszeradminisztrátor (rendszer menedzser) látja el.
Nem-megfelelőség	Az elfogadott vagy előírt követelmények ki nem elégítése, illetve hiányos teljesítése.
Nyilvánosságra hozatal	Az adatnak meghatározhatatlan körben, mindenki részére biztosított megismerhetővé, hozzáférhetővé tétele.
Papíralapú információhordozó	Az információk valamennyi olyan megjelenítési változatának meghatározására szolgál, amelyek papíron állnak rendelkezésre, és amelyek az informatikai rendszer használatával, illetve üzemeltetésével összefüggésben vannak.
PKI	A PKI (Public Key Infrastructure) nemzetközileg elismert, szabványos eljárásokon alapuló adatbiztonsági rendszer elnevezése, amely elektronikus dokumentumok magas biztonságú védelmére (módosítás elleni védelem, titkosítás), elektronikus aláírás generálására, a felhasználók és számítástechnikai eszközök – közjegyzői szintű – azonosítására alkalmazható.
Project	A projekt meghatározott cél elérésére irányuló határidő-, költség-, erőforrás- és minőségkorlátokkal rendelkező, adott szervezeti környezetben megtervezett és végrehajtott tevékenységsorozat, amely konkrét célokat valósít meg, és a célok eléréséhez erőforrásokat rendel. Időben és térben jól körül határolt összetett feladat, amely a kijelölt világos céloknak megfelelő tevékenységek és a rendelkezésre álló erőforrások összehangolt ésszerű felhasználásával valósítható meg.
Politika	A vezetőség által hivatalosan kifejezett átfogó szándék és irányvonal.

Főv.Törv.szék Cégb.Cg.: 01 09 203215

RBAC	Szerep-alapú hozzáférés-vezérlés (Role Based Access Control – RBAC) A rendszergazdai feladatok szabályozott feldarabolására alkalmas. Az operációs rendszerben kialakítható szerepek korlátozott root jogosultságot élveznek: csak és kizárólag az előre specifikált parancsok esetében adnak rendszergazdai jogkört. A definiált szerepekbe, mint account-okba nem lehet belépni, csak a hagyományos felhasználói azonosítóval rendelkező felhasználók tudnak szerepeket felvenni, ha jogosultak és ismerik az adott szerep jelszavát.
Rendelkezésre állás	A rendszer olyan állapota, amelyben eredeti rendeltetésének megfelelő szolgáltatásokat tud nyújtani (funkcionalitás) meghatározott helyen és időben (elérhetőség), továbbá annak biztosítása, hogy a felhatalmazott felhasználók mindig hozzáférjenek az információkhoz és a kapcsolódó értékekhez, amikor szükséges.
Rendszerelemek	Az elektronikus információs rendszer (informatikai rendszer) részét képző elemek. A rendszerelemek főbb csoportjai: eszközök, eljárások, emberek.
Rendszerelem csoportok:	• az informatikai rendszer környezetét alkotó infrastruktúra, • az informatikai rendszer hardver elemei, • az informatikai rendszer szoftver elemei, • az informatikai rendszer kommunikációs elemei, • adathordozók, • input és output dokumentumok, az informatikai rendszerre vonatkozó dokumentációk, • az informatika rendszerben résztvevő emberi erőforrások.
Rendszergazda (adminisztrátor)	A rendszergazda a kis- és közepes vállalat, intézmény, szervezet informatikáért felelős vezetőjének közvetlen munkatársa, vagy kihelyezett informatikai szolgáltatásokat végző cégben első szintű támogatói feladatokat lát el. Megfelelő mélységű (elméleti és gyakorlati) informatikai, hálózati ismeretei birtokában részt vesz a munkahely infokommunikációs hálózatának kialakításában és működtetésében. Koncepcionális kérdésekben feladata elsősorban a döntések előkészítése, míg megvalósításban a koordináló feladatok ellátása. Együttműködik a rendszerszervezőkkel, szoftverfejlesztőkkel.

Reputációs kár	A reputációs veszteség a likviditást, a tőkét vagy a jövedelmezőséget közvetve érintő olyan veszteség, amely az intézményről kialakult kedvezőtlen fogyasztói, üzletpartneri, részvényesi, befektetői vagy hatósági véleményből származik, és az intézmény külső megítélésének a kívánatos szinttől való elmaradásában nyilvánul meg.
Sebezhetőség (vulnerability)	A veszélyforrás képezte sikeres támadás bekövetkezése esetén az erőforrások sérülésének lehetősége.
Sértetlenség	Az adat azon tulajdonsága, amely arra vonatkozik, hogy az adat fizikailag és logikailag teljes. A sértetlenséget általában az információkra, adatokra, illetve a programokra értelmezik. Az információk sértetlensége alatt azt a fogalmat értjük, hogy az információkat csak az arra jogosultak változtathatják meg és azok véletlenül sem módosulnak. 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 sérthetetlenségen túli teljességet, továbbá az ellentmondás mentességet és a korrektséget, együttesen: 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.
Sérülékenység	Az IT biztonságban a „sérülékenység” vagy „biztonsági rés” olyan gyengeség, amelyet egy támadó (hacker, támadó program vagy robot) kihasználhat azért, hogy számítógépes rendszeren belül jogosulatlan lépéseket hajthasson végre. A sérülékenységek és biztonsági rések kihasználásához a támadónak valamilyen eszköz, felület kell, amellyel kapcsolódhat a rendszer gyenge pontjához (exploit). A sérülékenységet szokták még támadási felületnek is nevezni.
Sérülékenység vizsgálat	A Szervezet informatikai sérülékenység vizsgáló eszköze által folyamatosan végzett automatizált vizsgálat (szkennelés).
SLA	Service Level Agreement (Szolgáltatási szint megállapodás)
Szabály alapú biztonsági politika (rule-based security policy)	Valamennyi felhasználó számára kötelező, általános szabályokon alapuló biztonsági politika. Ezen szabályok rendszerint az elérendő erőforrások érzékenységének összehasonlítására, a felhasználók vagy a felhasználói csoportok nevében tevékenykedő entitások megfelelő jellemzőinek ismeretére épülnek.

Főv.Törv.szék Cégb.Cg.: 01 09 203215

Szerepkör	Az informatikai rendszer adataihoz, erőforrásaihoz való hozzáférési jogosultságot meghatározó csoport. A szerepkörök tartalmát a Szervezet Szervezeti és Működési Szabályzatában (a továbbiakban: SZMSZ) és más utasításokban meghatározott munkakörök, valamint a szervezeti hierarchiában elfoglalt hely határozzák meg.
Szolgáltatás megtagadás	Valamely informatikai rendszer, illetve szolgáltatás hibás működésből fakadó elérhetetlensége. Szolgáltatás megtagadásos támadásnak nevezzük továbbá egy kiszolgáló gép, vagy például egy szervezet kiszolgálói által kezelt honlapok csoportjának a célzott leterhelését, gyakran zombi hálózatok segítségével. DoS támadás esetén rövid időn belül olyan sok információkérés érkezik a szolgáltatást kiszolgáló szerverhez, hogy fizikailag nem képes rá válaszolni. Ez a rendszerek túlterheléséhez és a szolgáltatások átmeneti elérhetetlenségéhez vagy leállásához vezet.
Támadás	Minden olyan tevékenység, amelynek célja valamely informatikai rendszer veszélyeztetése és az abban történő kártokozás.
Távmunka	A távmunka egy munkaszervezési mód, melynek lényege, hogy a távmunkás számára biztosított a vállalati központtól eltérő helyen is egy olyan munkakörnyezet, ahol infokommunikációs eszközök segítségével egyes munkafeladatait teljes értékűen el tudja végezni.
Teljes körű védelem	Teljes körű a védelem, ha az az informatikai rendszer összes elemére kiterjed.
Trójai faló	Olyan programtörzs, amelyeket készítője illegálisan épített be az általa tervezett programba és a felhasználó szándéka ellenére és tudta nélkül hajt végre illegális feladatokat (adattörlés, illegális lemezművelet, program-megsemmisítés stb.).
Ügyfél	Olyan külső szervezet vagy személy, amely, vagy aki a Szervezet egy adott szolgáltatását igénybe veszi.
Üzletmenetfolytonosság tervezés	Az üzletmenet folytonossági tervezés egy olyan keretrendszer, amely képessé teszi a szervezetet arra, hogy hatékonyan reagáljon a működésének folyamatosságát veszélyeztető fenyegetésekre. Az üzleti hatáselemzés alapján kiválasztott kritikus folyamatokra üzletmenetfolytonossági terveket kell készíteni, melyek tesztelésre kerülnek.

Főv.Törv.szék Cégb.Cg.: 01 09 203215

Üzleti tervezés	Az üzleti tervezés egy olyan (irányítási) folyamat, amely a vállalat jövőbeli működésének pályáját vázolja fel. A terv tartalmazza ezen pálya jellemző állapotait, valamint azt az akcióprogramot, amelynek végrehajtásával a kívánt állapot(ok) elérhető(k).
Vagyonleltár	A vagyonleltár célja, hogy a szervezet naprakész nyilvántartással rendelkezzen a védendő információs, szoftver és fizikai vagyonáról, azok tulajdonosáról és az egyes vagyonelemek értékéről. A vagyonleltár meglétével/segítségével tudunk hatékony és megfelelő szintű védelmet kialakítani, mivel pontosan ismerjük, hogy mit is kell megvédeni. A Szervezet vagyonleltárának az alábbiakat kell tartalmaznia: • Információ-vagyon: az adatok, adatbázisok, szoftver-kezelési kézikönyvek, oktatási, üzemviteli, üzemeltetési, biztonsági segédletek és nyilvántartások. • Szoftver-vagyon: rendszerszoftverek, alkalmazói szoftverek, fejlesztő-eszközök és szolgáltatások. • Fizikai-vagyon: hardver (számítógépek, perifériák, mobil számítástechnikai eszközök), kommunikációs eszközök (telefonok, faxok, modemek, hálózati csatoló eszközök, telefon-alközpontok), adathordozók és egyéb műszaki berendezések (szünetmentes tápegység, légkondicionáló berendezés, villámhárító stb.).
Vagyontárgy	A szervezet tulajdonában lévő, meghatározható értékkel rendelkező fizikai dolog, illetve eszköz.
Valószínűség	Annak a mértéke, hogy egy esemény milyen eséllyel következik be.
Változásfelügyelet	Azok az eljárások, amelyek biztosítják, hogy minden változtatás ellenőrzött legyen, beleértve annak kérelmezését, rögzítését, elemzését, a vonatkozó döntés meghozását, jóváhagyását, kivitelezését és a változtatás megvalósítás utáni áttekintését is.
Változásmenedzsment	Az informatikai termék vagy rendszer fejlesztési, előállítási vagy karbantartási folyamatai alatt megvalósuló változásokat kezelő rendszer.
Vészhelyzet	Az informatikai rendszerekben bekövetkezett olyan esemény, amely a rendszerben nem tervezett leállást, biztonsági eseményt vált ki. A vészhelyzetekre adandó válaszintézkedéseket és folyamatokat az érintett rendszer katasztrófa-elhárítási terve tartalmazza.

Főv.Törv.szék Cégb.Cg.: 01 09 203215

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. Némely vírus késleltetve fejti csak ki hatását, például csak egy bizonyos számú gazdaprogram megfertőzése után. A vírusok domináns kártékony hatása az ellenőrizetlen reprodukciójuk, mely túlterhelheti a számítógépes erőforrásokat.
Zárt védelem	Zártnak nevezik az informatikai rendszer védelmét, ha az összes releváns fenyegetést figyelembe veszi.

Főv.Törv.szék Cégb.Cg.: 01 09 203215