Informatikai biztonsági fogalomtár

Kifejezés	Meghatározás
5G vezetéknélküli hálózat	Az ***5G (ötödik generációs) vezeték nélküli hálózat*** alatt a szakirodalom egy vezeték nélküli hálózati architektúrát ért, amely a 802.11ac IEEE vezeték nélküli hálózati szabvány szerint épül fel, és amelynek segítségével az adatkommunikációs sebesség akár háromszorosára növelhető az elődjéhez, a 4G-hez (IEEE 802.11n) képest. Az 5G magában foglalja az IEEE 802.11ac által javasolt architektúra módosításokat, és az 5 GHz-es frekvenciatartományban működik.
Adat	A számítástechnikában adatnak (Angol: D*ata*) nevezzük a számokkal leírható dolgokat, melyek számítástechnikai eszközökkel rögzíthetők, feldolgozhatóak és megjeleníthetők. Az adat nagyon tág fogalom: gyakorlatilag bármilyen jel potenciálisan adatnak tekinthető. Az adat: olyan minta, mely rendelkezik kapcsolattal. Tudjuk azt, hogy az adott bitminta kihez tartozik, minek a jellemzését adja, mit és hogyan ír le. ~ egy leírás, egy passzív elem, egy "tárgy", amit felhasználnak a cselekvésekben (vele, rajta). Ő a művelet bemeneti be- és kimeneti eleme. (forrása, paramétere és eredménye) Rajta, vele végzik a cselekvést. A cselekvés kötelező kelléke, tárgya. Őt változtatják meg (inkrement, hozzáfűzés, elvétel), vele címeznek, segítségével szelektálnak, minta (referencia és cserélt) az összehasonlításnál (változtatásmentes felhasználás). Amennyiben a mintához egy aktív (működési, működtetési) nézet/képesség rendelődik hozzá, akkor már kódnak nevezik, ami egy végrehajtó egységet cselekvésre bír. A mintához rendelt kapcsolatok csoportba szedhetőek. A sok-sok csoportot (értelmezési módokat) típusoknak nevezik. Lásd még: ismeret, információ
Adatalany	Bármely meghatározott személyes adat alapján azonosított vagy egyébként – közvetlenül vagy közvetve – azonosítható természetes személy. A személy különösen akkor tekinthető azonosíthatónak, ha őt – közvetlenül vagy közvetve – név, azonosító jel, illetőleg egy vagy több, fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző tényező alapján azonosítani lehet.
Adatállomány	Az informatikai rendszerben logikailag összetartozó, együtt kezelt adatok.
Adatátvitel	Adatok informatikai rendszerek, rendszerelemek közötti továbbítása.
Adatbiztonság	Az adatok jogosulatlan megszerzése, módosítása és megsemmisítése elleni műszaki és szervezési megoldások rendszere.
Adatfeldolgozás	Az adat informatikai eszközökkel történő feldolgozása. Célja általában a rendelkezésre álló adatok segítségével új információhoz jutás. Tulajdonképpen enyhe túlzással azt is lehetne mondani, hogy az egész informatika célja nem más, mint az adatok feldolgozása. Például: leltárra alkalmazott készletfrissítések, bankszámlaszámlára és ügyfélfájlra alkalmazott banki tranzakciók, foglalás és jegyértékesítés tranzakciók egy légitársaság fenntartási rendszeréhez, számlázás közüzemi szolgáltatásokhoz. Az "elektronikus" vagy "automatikus" módosítót "adatfeldolgozással" (DP), különösen c. 1960-ban, hogy megkülönböztesse az emberi irodalmi adatfeldolgozást a számítógép által elvégzettektől Az adat feldolgozása lehet egyszerű számításokat végző programoktól a táblázatkezelő programokon keresztül a bonyolult (például fizikai mérőeszközökből származó) adatok segítségével végzett új ismeretszerzésre vezető tudományos

Kifejezés	Meghatározás
	programig bármi.
Adatfeldolgozó	Az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel.
Adatgazda	Az, aki, felelős az általa kezelt adatokért, továbbá jogosult minősítés vagy osztályba sorolás elvégzésére.
Adathalászat	Az ***Adathalászat*** (Angol: Phising) fogalma magánjellegű és érzékeny információk, például hitelkártya-adatok, személyes azonosítók, számítógépes fiók felhasználóneveinek és jelszavaink stb. megszerzésére irányuló csalási tevékenységet jelenti. A pszichológiai befolyásolás (Angol: Social Engineering) technikák és a számítógépes programozási ismeretek komplex sorozatának felhasználásával az adathalász web helyek megtévesztéssel e-mail címzetteket és/vagy web felhasználókat vesznek rá arra, hogy azok azt higgyék, hogy a hamis weboldal legitim és valódi. Ennek eredményeként az adathalászat áldozata a személyazonosságával, és egyéb személyes információival kapcsolatos adatokat ad át a csalóknak. Ezekkel az adatokkal később (rossz esetben) a csalók visszaélnek, és direkt, vagy indirekt módon (például az adatok értékesítésével) károkat okozhatnak az adathalászat áldozatainak.
Adathordozható-sághoz való jog	Az adathordozhatósághoz való jog az érintett jogosult az általa az adatkezelő rendelkezésére bocsátott adatait megkapni: • tagolt, széles körben használt, géppel olvasható formátumban • jogosult más adatkezelőhöz továbbítani • kérheti az adatok közvetlen továbbítását a másik adatkezelőhöz – ha ez technikailag megvalósítható • kivéve: közérdekű, vagy közhatalmú jog gyakorlása céljából végzett adatkezelés Az adathordozhatósághoz való jog egy új, a saját adatok feletti rendelkezést erősítő jogintézmény, mely akkor gyakorolható, ha automatizált módon történik az adatkezelés, és az adatkezelő az adatokat az érintett hozzájárulása vagy a szerződéses jogalap alapján kezeli.
Adatkezelés	Az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet, például az adatok gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (ujj- vagy tenyérnyomat, DNS-minta, íriszkép stb.) rögzítése.
Adatkezelés jogalapja	Az adatkezelés jogalapja főszabály szerint az érintett hozzájárulása vagy törvényben elrendelt kötelező adatkezelés.
Adatkezelő	adatkezelő az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza.
Adatminőség	Az adatminőség az adatok, különösen az adattárházban található adatok alkalmazásának hatékonyságát, megbízhatóságát és alkalmasságát jellemző tulajdonság. Az adatminőség meghatározása bonyolult módszerrel történik, az adatok tulajdonságainak mérésére különféle szemszögből. Egy szervezeten belül a megfelelő adatminőség elengedhetetlen a tranzakciós és operatív folyamatokhoz, valamint az Üzleti Intelligencia (Business Intelligence - BI) és

Kifejezés	Meghatározás
	az üzleti elemzés (Business Analysis - BA*)* jelentések megfelelő minőségű kidolgozásához. Az adatok minőségét egyaránt befolyásolja az adatok bevitelének, kezelésének és karbantartásának módja. Az Adatminőséggel kapcsolatos fontos eljárási rend az adatminőség-biztosítás (DQA - Data Quality Assurance) egy olyan eljárás, amelynek célja az adatok hatékonyságának és megbízhatóságának igazolása.
Adatminőség biztosítás	Az Adatminőség biztosítás (Data quality assurance (DQA) eszköze a hatékony adatminőség-karbantartás, amelyhez szükséges az adatok rendszeres figyelése és tisztítása. Az adatminőség fenntartása általában magában foglalja az adatok frissítését, egységesítését, és a rekordok deduplikációját az egyetlen adatnézet létrehozásához. Az adatok minősége a következő okokból létfontosságú: • Pontos és időszerű információkat szolgáltat az elszámoltathatóság és a szolgáltatások kezeléséhez. • Azonnali információkat kínál a szolgáltatás hatékonyságának kezeléséhez. • Segíti az erőforrások prioritásainak meghatározását és garantálását. Az adatminőség fő jellemzői a következők: • Teljesség: A kívánt adat attribútumok megadásának szintje. Az adatoknak nem kell 100 százalékban teljesnek lenniük. • Pontosság: Az adatok valós állapotát képviseli. Különféle listák és leképezések segítségével, automatizált módszerrel számítható ki. • Hitelesség: Annak mértéke, hogy az adatokat hitelesnek és valódnak tekintik-e. • Időszerűség (az adatok kora): az adatokat megfelelő frissítésére vonatkozó jellemző. • Konzisztencia: Annak felmérése, hogy a különféle adatkészletek tényei megfelelnek-e egymásnak. • Integritás: az adatok referenciájának érvényességét és a különböző adatkészletek pontos összekapcsolását jellemzi.
Adatprofilozás	Az Adatprofilozás az adatok különböző felhasználási célokra történő megvizsgálására szolgáló módszer. Ilyen vizsgálatok például a pontosság és a teljesség meghatározása. Az adatprofilozási folyamat egy adatforrást, például adatbázist vizsgál meg, abból a célból, hogy felfedje, meghatározza az adatszervezés hibás, téves területeit. Az adatprofilozás elvégzése, és annak eredménye javítja az adatminőséget. Az adatok profilozására adatfelderítésként is szoktak hivatkozni. Kicsit részletesebben: Az Adatok profilozása az adatforrásban rendelkezésre álló adatok vizsgálata, valamint az adatokra vonatkozó statisztikák és információk gyűjtése. Az ilyen statisztikák segítenek a meta adatok felhasználásának és adatminőségének azonosításában. Ezt a módszert széles körben használják a vállalati adattárolásban. Az adatok profilozásával derítik fel az adatok szerkezetét, kapcsolatát, tartalmát és származtatási szabályait, amelyek elősegítik a meta adatokban szereplő rendellenességek megértését. Az adatok profilozása különféle leíró statisztikákat használ, beleértve az átlag, a minimum, a maximum, a a százalékértékeket, a gyakoriságot valamint az egyéb aggregátumokat, például a számot és az összeget. A profilozás során kapott további meta adat-információk az adattípus, hosszúság, diszkrét értékek, egyediség és absztrakt típusfelismerés.
Adatszivárgás	Adatszivárgásról beszélünk, ha a szervezet vagy a vállalat adatvagyonához tartozó védett információ az információ megszerzésére nem jogosított fél kezébe jut.

Kifejezés	Meghatározás
	Az esemény lehet szándékosan előidézett, vagy akaratlan módon bekövetkezett. • az akaratlanul bekövetkezett adat szivárgás tipikus példája, amikor egy felhasználó véletlenül nem annak a személynek küld el egy e-mailt, akinek akarta, hanem egy olyan személynek, akit a levelezőrendszer automatikusan felajánl a címzett nevének begépelésekor; • szándékosságról beszélünk, ha az adatszivárogtatás hackertámadásra épül, de akkor is, ha adott munkatárs létező jogosultságaival (vissza)élve szerez meg, de munkájához nem tartozó módon használ fel (vagy ad ki) érzékeny adatokat.
Adattal (információval) szembeni követelmények	Minőségi (Angol: *quality*) követelmények: • eredményesség (Angol: *effectiveness*), • hatékonyság (Angol: *efficiency*). Bizalmi (Angol: *fiduciary*) követelmények: • szabályosság (Angol: *compliance*), • megbízhatóság (Angol: *reliability*). Biztonsági (Angol: *security*) követelmények: • bizalmasság (Angol: *confidentiality*), • sértetlenség (Angol: *integrity*), • rendelkezésre állás (Angol: *availability*).
Adattal rendelkezés	• a birtokban tartás, • az adat alapján további adat készítése, • az adat másolása, sokszorosítása, • a betekintés engedélyezése, • a feldolgozás és felhasználás, • a minősítés (biztonsági osztályba sorolás) felülvizsgálata, • a minősítés (biztonsági osztályba sorolás) felül bírálata, • a nyilvánosságra hozatal, • a titoktartási kötelezettség alóli felmentés, • megismerési engedély kiadása.
Adattörlés	Az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk nem lehetséges.
Adattovábbítás	Ha az adatot meghatározott harmadik személy számára hozzáférhetővé teszik.
Adattovábbítás külföldre	Személyes adatok továbbítása az EGT-n (*Európai Gazdasági Térség* az Európai Unió országai, valamint Izland, Norvégia és Liechtenstein) kívüli, harmadik országba adatkezelési tevékenységet folytató adatkezelőhöz.
Adatvédelem	Adatvédelem a személyes adatok jogszerű kezelése, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége.
Adatvédelmi fásultság	Érdektelenség, rutinszerű hozzáállás az adatvédelmi szabályok alkalmazásához.
Adatvédelmi incidens	Adatvédelmi incidens alatt a rendelet értelmében a biztonság olyan sérülését értjük, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.
Adminisztratív védelem	A védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések, továbbá a védelemre vonatkozó oktatás.
AES 256-os titkosítás	Az **AES** (Advanced Encryption Standard) egy módszer elektronikus adatok titkosítására. Az eljárás a legtöbb titkosítással foglalkozó szoftverben elérhető . Az

Kifejezés	Meghatározás
	AES a *Rijndael* kódolás olyan változata, ahol a blokkméret szigorúan 128 bit, a kulcs pedig 128, 192 vagy 256 bit. Összehasonlításként a Rijndael kódolásban a blokkméret és a kulcsméret is lehet 32 bit tetszőleges többszöröse azzal a kikötéssel, hogy mind a kulcs, mind a blokkméret minimum 128 és maximum 256 bit lehet.
Akkreditálás	Olyan eljárás, amelynek során egy erre feljogosított testület hivatalos elismerését adja annak, hogy egy szervezet vagy személy felkészült és alkalmas bizonyos tevékenységek elvégzésére.
Aláírás-létrehozó eszköz	Olyan hardver, illetve szoftver eszköz, melynek segítségével az aláíró az aláírás-létrehozó adatok felhasználásával az elektronikus aláírást létrehozza.
Alap fenye-getettségek	A fenyegetések általánosított csoportosítása. Alapfenyegetettségek: • a bizalmasság, • a sértetlenség, • a rendelkezésre állás • sérülése vagy elvesztése.
Alkalmazás, alkalmazói program	Olyan program, amelyet az alkalmazó saját igényei, céljai érdekében használ, és amely a hardver és az üzemi rendszer funkcióit használja.
Államtitok	A "szigorúan titkos" minősítésű adat régi megnevezése. Lásd: Minősített adat."
Auditálás	Az előírások, elvárások teljesítésére vonatkozó megfelelőségi vizsgálat, ellenőrzés.
Authentication	a.) az authentikáció a görög αυθεντικός: 'valódi', 'eredeti' jelentésű szóból származik, és az informatikában olyan eljárást jelent, amelynek során meggyőződünk arról, hogy valamely információ (legtöbbször egy felhasználó azonosságára vonatkozó állítás) megfelel a valóságnak. Legjobb magyar megfelelője a "hitelesítés" szó lehet. Az informatikai rendszerek különböző fokú (megbízhatóságú) hitelesítési eljárás után adnak jogosultságot erőforrásaikhoz. b.) a számítógépes biztonság témakörében ismert AAA (Authentication, Authorization, Accounting) funkció együttes biztonságos azonosításért felelős komponense. A hitelesítés azt az azonosítási folyamatot jelenti, melynek során egy személy, számítógép vagy hálózati eszközök bizonyítja, hogy rendelkezik megfelelő hitelesítő adatokkal. Többféle hitelesítő módszer létezik, melyek közül a legegyszerűbb a felhasználónevek és jelszavak alkalmazása, de ide tartozik a digitális aláírás és a biometriai azonosítás is. Kritikus biztonságú rendszerek esetén legalább két módszer egyidejű alkalmazása javasolt.
Authorizáció	általánosságban az authorizáció (engedélyezés) olyan biztonsági mechanizmusok gyűjteményét jelenti, mely meghatározza, hogy a felhasználók mit tehetnek egy rendszerben, azaz milyen erőforrásokhoz férhetnek hozzá és milyen műveleteket hajthatnak végre. A számítástechnikában olyan eljárást jelent, amely megadott erőforrásokhoz (adatállományokhoz, valamilyen rendszer meghatározott szolgáltatásaihoz) való hozzáférést csak jogosultság esetén tesz lehetővé
Az adatkezelés elvei	A célhoz kötött adatkezelés követelménye (lásd alább), valamint az adatminőség követelménye. Ez utóbbi magában foglalja a pontos, teljes és naprakész adatok igényét, valamint az adatfelvétel és az adatkezelés tisztességes, törvényes mivoltát.
Banktitok	Minden olyan, az egyes ügyfelekről a pénzügyi intézmény rendelkezésére álló tény, információ, megoldás vagy adat, amely ügyfél személyére, adataira, vagyoni helyzetére, üzleti tevékenységére, gazdálkodására, tulajdonosi, üzleti kapcsolataira, valamint a pénzügyi intézmény által vezetett számlájának egyenlegére, forgalmára,

Kifejezés	Meghatározás
	továbbá a pénzügyi intézménnyel kötött szerződéseire vonatkozik.
Beépített intelligencia	A Beépített intelligencia (Angol: *Onboard Intelligence*) kifejezést arra a megoldásra használjuk, amikor a mesterséges intelligenciát egyedi eszközökbe építik be az eszköz tervezésének során, az elosztott rendszerek analógiája szerint. A beépített intelligencia nagyon sok előnyt, de egyben hátrányt is jelenthet azokkal a kihívásokkal és problémákkal kapcsolatban, amelyekkel a tervezők és a mérnökök a mesterséges intelligencia területén találkozhatnak. A beépített intelligencia alkalmazásának egyértelmű hatékonysága abban rejlik, hogy az eszköznek nem kell külső helyen telepített mesterséges intelligenciát használnia. A mesterséges intelligencia motorok energia- és számítási kapacitásigényei azonban a beépített intelligencia alkalmazását gyakran lehetetlenné teszik.
Behatolási teszt	Az informatikai rendszer, vagy annak egy elemének olyan ellenőrzése, melynek során megállapíthatók, hogy vannak-e a gyakorlatban kiaknázható, ismert gyenge pontok. (Angol: *Penetration Testing*)
Bejelentkezés	A felhasználó között általi logikai kapcsolat kezdeményezése, amelynek eredményeképpen az informatikai rendszer funkcióinak használata lehetővé válik.
Betörés detektáló eszköz	Olyan rendszer, amely minden észlelt aktivitást valós időben megvizsgálva, egyenként eldönti, hogy az adott aktivitás legális-e, vagy sem.Fajtái • a minta alapú betörés detektáló eszközök (Angol: *signature-based IDS*) és • a viselkedést vizsgáló betörés detektáló eszközök (Angol: *behavior-based IDS*). Intrusion Detecting Systems (rövidítve: IDS).
Bevált gyakorlat	A Bevált gyakorlat vagy Jó gyakorlat (Angol: *Best Practice*) a vállalati menedzsment és minőségbiztosítás területén olyan, rutinszerűen végzett tevékenységre utal, ami széles körű tapasztalatokon alapul, és több szervezetben is sikeresnek bizonyult. Gyakran nevezik az angol kifejezés tükörfordításaként félrevezetően „legjobb gyakorlatnak”. Ez azonban nem helytálló, hiszen semmilyen (adott körben vagy időszakban bevált) gyakorlat nem garantálja, hogy nem létezik nála jobb gyakorlat.
Biometrikus azonosítás	Az informatikában a biometrikus azonosítás/hitelesítés fogalma azokat a technológiákat öleli fel, amelyek segítségével, alkalmazásával rögzítik és/vagy mérik az azonosítandó személy egyedi biológiai, fizikai jellemzőit, és az ezekből nyert adatokkal kísérlik meg a személy azonosítását/hitelesítését. Mára már számtalan formáját alkalmazzák a biometrikus azonosításnak/hitelesítésnek: alak és mozgás, arc, ujj és tenyérlenyomatfelismerés, íriszelemzés, vénaszkenner stb. Attól függően, hogy milyen erősen védett rendszerről van szó, egyszerre akár több azonosítási módszert is alkalmazhatnak egy-egy rendszerben. Magyarországon a biometrikus azonosítás erős törvényi szabályozás mellett lehetséges.
Bizalmasság	Az adat azon tulajdonsága, amely arra vonatkozik, hogy az adatot csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról.
Biztonság	A rendszer olyan – az érintett számára kielégítő mértékű – állapota, amelyben zárt, teljes körű, folytonos és a kockázatokkal arányos védelem valósul meg.
Biztonság megsértése	Biztonság megsértése alatt az olyan eseményeket értjük, amelyek adatok, alkalmazások, szolgáltatások, hálózatok és / vagy eszközök jogosulatlan hozzáférését eredményezik, az azok alapjául szolgáló biztonsági mechanizmusok megkerülésével. Biztonsági sérülések akkor fordulnak elő, amikor egy személy vagy egy alkalmazás jogellenesen fér hozzá egy privát, bizalmas vagy más logikai IT tartományhoz.

Kifejezés	Meghatározás
	Azokat a hardver vagy szoftver vagy szolgáltatási hiányosságokat, problémákat, amelyek lehetővé teszik a biztonság megsértését, biztonsági résnek is nevezik.
Biztonsági esemény	Olyan nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül.
Biztonsági események kezelése	A Biztonsági események kezelése (az eredeti angol kifejezésből, a *Security Event Management*-ből a rövidítő betűszóval SEM) a biztonsággal kapcsolatos események azonosításának, összegyűjtésének, megfigyelésének és jelentésének folyamata egy szoftver és/vagy rendszer és/vagy informatikai környezetben. A SEM lehetővé teszi az események rögzítését és értékelését, és segít a biztonsági vagy rendszergazdáknak az információbiztonsági architektúra, az irányelvek és az eljárások elemzésében, beállításában és kezelésében.
Biztonsági incidensek és események kezelése	A Biztonsági incidensek és események kezelése (az angol kifejezés *Security Incident and Event Management* rövidítésével, a SIEM betűszóval használjuk) alatt a biztonsági incidensek vagy események azonosítását, megfigyelését, rögzítését és elemzését értjük, valós idejű IT-környezetben. A SIEM rendszer segítségével a rendszer tulajdonosa átfogó és központosított képet kaphat az informatikai infrastruktúra biztonsági eseményeiről. A Biztonsági incidensek és események kezelése Biztonsági információs eseménykezelésként is ismert. A SIEM szoftvereken, rendszereken, készülékeken vagy ezen elemek valamilyen kombinációján keresztül valósul meg. Egy SIEM rendszer lényegét tekintve olyan központi naplóelemző rendszer, mely különböző eszközök/felügyeleti rendszerek/szoftverek központosított naplóadataira épülve szolgáltatásokat nyújt a cég biztonsági/ellenőrzési/audit felügyeletének/központjának. Általában véve egy SIEM rendszer hat fő tulajdonságán keresztül jellemezhető: • Megőrzés: Az adatok hosszú ideig történő tárolása, hogy a teljesebb adatkészletek alapján döntéseket lehessen hozni. • Irányítópultok: Adatok elemzésére (és megjelenítésére), minták megismerése céljából, célzott tevékenység vagy olyan adatok, amelyek nem felelnek meg a normál mintának. • Összefüggések keresése: (Korreláció): Az adatokat olyan csomagokba rendezi, amelyek értelmezhetőek, hasonlóak és közös vonásokkal rendelkeznek. A korrelációs műveletek célja, hogy az adatokat hasznos információkká alakítsák. • Riasztás: Ha olyan adatokat gyűjt vagy azonosít, amelyek bizonyos válaszokat kiváltanak - például riasztások vagy potenciális biztonsági problémák -, a SIEM eszközök olyan protokollokat aktiválhatnak a felhasználók figyelmeztetésére, mint például az irányítópultra küldött értesítések, automatizált e-mail vagy szöveges üzenet. • Adatok összesítése: Az adatok a SIEM bevezetése után tetszőleges számú helyről gyűjthetők, beleértve a kiszolgálókat, hálózatokat, adatbázisokat, szoftvereket és e-mail rendszereket. Az aggregátor összevont erőforrásként is szolgál, mielőtt az adatokat korreláció vagy megőrzés céljából elküldenék. • Megfelelés vizsgálat: A SIEM-ben protokollokat lehet létrehozni, amelyek automatikusan összegyűjtik a vállalati, szervezeti vagy kormányzati politikákkal kapcsolatos, azok betartásának ellenőrzéséhez szükséges adatokat.

Kifejezés	Meghatározás
	A Seacon Europe Sealog rendszere a fentieknek megfelelő SIEM rendszer. A SeaLog a különböző rendszerek eseményeit összegyűjti, majd az összegyűjtött adatokat automatikus, informatikai módszerekkel együttesen elemzi, és a felhasználók számára érthető formában képes megjeleníteni.
Biztonsági mechanizmus	A biztonsági mechanizmusok (Angol: *security mechanism),* műszaki eszközök és technikák, amelyeket a biztonsági szolgáltatások megvalósításához használnak. Egy mechanizmus önmagában vagy másokkal működhet egy adott szolgáltatás nyújtása érdekében.
Biztonsági mentés	A biztonsági mentést pontosan leíró fogalom az adatmentés. Adatmentésen, a számítógépen tárolt információkról történő biztonsági másolat készítését értjük, a mentés célja pedig az eredeti forrásadatokat tartalmazó tároló esetleges sérülésének elhárítása. A biztonsági mentés folyamata üzleti alapú döntéseket, szoftveres és hardveres megoldásokat foglal magában. Nagyvállalati környezetben gyakori az egymástól földrajzilag távol lévő tároló rendszerekre történő adatmentés. Fontos, hogy a mentési (és helyreállítási) rendszerek hardverfüggetlenek legyenek. A mentési folyamat többféle rendszer (és ezek kombinációja) szerint történhet: • Nincs mentés • Teljes mentés minden alkalommal • Növekményes mentés • Differenciális mentés Folyamatos védelem
Biztonsági osztály	Az elektronikus információs rendszer védelmének elvárt erőssége.
Biztonsági osztályba sorolás	A kockázatok alapján az elektronikus információs rendszer védelme elvárt erősségének meghatározása.
Biztonsági szint	A szervezet felkészültsége a törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére.
Biztonsági szintbe sorolás	A szervezet felkészültsége (érettsége) a biztonsági feladatok kezelésére.
Bűnügyi személyes adat	a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat.
BYOD	A BYOD betűszó a "*Bring your own device*!" angol mondat rövidítése, ami magyarul annyit tesz, hogy „Hozd a saját eszközödet!”. Magyarán: hozd be a céghez, és használd a saját eszközeidet a munkád során! Ez a "módi", ez az "engedékenység" a folyamatos technikai újítások miatt alakult ki. Míg egy magánszemély, amennyiben érdeklődő típus – legyen szó számítógépről, hordozható eszközökről vagy okos telefonról – szívesen cseréli le eszközeit a legújabbakra, addig egy nagyobb cég szerverparkját, eszköztárát csak ütemezetten újítja meg (un. avultatással). A gyorsan elavuló eszközökkel a dolgozó számára nehézkes lehet a munka, míg a saját (és elég gyakran frissített) eszközeit használva a munkavégzése hatékonyabb lehet, de mindenképpen megtakarítást eredményezhet a munkáltatója számára…
Célhoz kötött	Személyes adat kizárólag meghatározott célból, jog gyakorlása és kötelezettség

Kifejezés	Meghatározás
adatkezelés	teljesítése érdekében kezelhető. Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának, az adatok felvételének és kezelésének tisztességesnek és törvényesnek kell lennie. Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas. A személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető. Az adatkezelés során biztosítani kell, hogy az adatok pontosak, teljesek és – ha az adatkezelés céljára tekintettel szükséges – naprakészek legyenek, valamint azt, hogy az érintettet csak az adatkezelés céljához szükséges ideig lehessen azonosítani.
CIA	Az elektronikus információs rendszer védelmének alapvető céljának, a bizalmasság (Angol; C*onfidentiality*), a sértetlenség (Angol: ***I**ntegrity*) és a rendelkezésre állás (Angol: ***A**vailability*) védelmi hármasának jelölése.
Crack	A programok védelmének "feltörése"
Cracker	Az informatikai rendszerbe informatikai eszközöket használva, direkt rombolási céllal betörő személy. Lásd: még Hacker.
CRAMM	Az Egyesült Királyság Central Computer and Telecommunication Agency szervezete által kidolgozott kockázatelemzési és kezelési módszertan. (CCTA Risk Analysis and Management Method).
Crosssec Backup	A Crosssec Backup egy biztonsági mentési megoldás.
Cryptolocker	A CryptoLocker egy trójai zsarolóprogram, amely a futó Microsoft Windows rendszert veszi célba. Az interneten először 2013. szeptember 5.-én jelent meg. A CryptoLocker egy fertőzött e-mail mellékleteken keresztül, egy már létező botnet közreműködésével terjed. Miután aktiválódik, egy RSA nyilvános kulcsú titkosítással titkosít bizonyos típusú, *a* megtámadott eszközön tárolt fájlokat a helyi és a csatlakoztatott hálózati meghajtókon, a tárolt magánkulcsot pedig csak a malware vezérlő szerverein tárolja. A malware ezután egy üzenetet jelenít meg a felhasználó gépén. Amennyiben a megtámadott kifizeti a megadott határidőig a megadott összeget (a fizetés általában Bitcoin-ban, vagy készpénzátutalással lehetséges), felkínálja az adatok titkosításának megszüntetését. Az üzenet egyben azzal fenyegeti meg a felhasználót, hogy törli a titkosítás feloldásához szükséges privát kulcsot, amennyiben letelik a megadott határidő.
CryptoWall	A CryptoWall fájlok titkosításával, használhatatlanná tételével okoz komoly károkat, majd pénzt követel a felhasználótól a dekódoláshoz, helyreállításhoz szükséges információkért cserébe. A CrypoWall ransomware program nem vírus (pontosabban az is), hanem weboldalakon vagy elektronikus levelek mellékletében terjesztett állományok, illetve egyéb számítógépes károkozók (pl. botnetek) révén kerülhet fel a rendszerekre. Egyebek mellett az Onkods és az Upatre trójai programok ***is*** terjesztik. A CryptoWall nem végez jelentősebb módosításokat a Windows beállításaiban, mindössze arról gondoskodik, hogy a rendszer újraindítása után is életképes maradjon. A kiszemelt számítógépre néhány fájlt másol fel, amelyek egyrészt a titkosítást végzik, másrészt különféle formátumban tartalmazzák a követelésekkel kapcsolatos üzenteket. A CryptoWall nem kizárólag a helyi adattárolókon lévő állományokra jelent veszélyt, hanem minden, a számára hozzáférhető, és írási/módosítási joggal rendelkező meghajtón tárolt fájlra. Így a cserélhető és hálózati meghajtókon is képes pusztítani titkosítást végezni.
DDoS	Lásd: Terjesztett szolgáltatásmegtagadás.

Kifejezés	Meghatározás
(Distributed Denial of Service)	
Demilitarizált zóna	Az informatikai biztonság területén a katonai használatra utaló nevű demilitarizált zóna (DMZ*)*, más néven demarkációs zóna vagy határhálózat egy olyan fizikai vagy logikai alhálózat, ami egy szervezet belső szolgáltatásait tartalmazza és tárja fel egy nagyobb, nem megbízható hálózatnak, általában az internetnek. A DMZ célja, hogy egy plusz biztonsági réteget biztosítson a szervezet helyi hálózatának (LAN). Így egy külső támadónak csak a DMZ-ben található berendezésekhez lehet hozzáférése, nem az egész hálózathoz. Egy hálózatban azok a hostok a legsebezhetőbbek, amelyek a LAN-on kívüli felhasználóknak nyújtanak szolgáltatásokat, úgy mint az e-mail-, web- és DNS szerverek. Ezeket a hostokat a megnövekedett fenyegetettség miatt egy saját alhálózatba helyezik. Ezzel védik a hálózat többi részét abban az esetben, ha valakinek sikerülne behatolnia. A DMZ-ben lévő hostoknak csak jól szabályozott, korlátozott kapcsolatban szabad lenniük a belső hálózatba tartozó gépekkel. A kommunikáció másik hostokkal a DMZ-n belül és a külső hálózatba viszont engedélyezett. Ez teszi lehetővé, hogy a DMZ-n belüli hostok szolgáltatást nyújthassanak mind a belső, mind a külső hálózatba. A forgalmat pedig egy közbenső tűzfal irányítja a DMZ-ben levő szerverek és a belső hálózat kliensei közt. A DMZ szolgáltatásai: alapjában minden szolgáltatást, ami a külső hálózat felhasználóit látja el, a DMZ-n belülre kellene helyezni. A leggyakoribbak ezek közül a web-, mail-, ftp- és DNS-szerverek. Néhány helyzetben további lépéseket kell alkalmazni, hogy biztonságos szolgáltatásokat nyújthassunk.
Digitális aláírás	A digitális aláírás egy matematikai eljárás a digitális üzenetek vagy dokumentumok hitelességének igazolására. A digitális aláírás folyamatában egy informatikai rendszerben egy kezelt adathoz rejtjelezéssel előállított jelsorozatot csatolnak, amely a hozzá tartozó adat hitelességének és sértetlenségének bizonyítására használható. Az érvényes digitális aláírás, amennyiben az előfeltételek teljesülnek, nagyon erős bizonyítékot nyújt a címzett számára arra, hogy feltételezhesse azt, hogy az érkezett üzenetet egy ismert küldő készítette (hitelesítés), és hogy az üzenetet nem változtatta meg az átvitel során (integritás). Fontos észrevenni, hogy a digitális aláírás és az elektronikus aláírás csak hasonló fogalmak, de míg a digitális aláírás elsősorban a technológiát, az elektronikus aláírás a technológia mellett a jogi fogalmat is jelenti. Ez egyben azt is jelenti, hogy *a* digitális aláírás és az elektronikus aláírás nem szinonimái egymásnak.
Digitális bizonyíték	Digitális bizonyíték (vagy elektronikus bizonyíték, Angolul: *The digital evidence*) lehet minden olyan adat, amelyet számítógéppel tárolnak vagy továbbítanak, és amely alátámasztja vagy megcáfolja egy cselekmény bekövetkezésének elméletét, vagy amely az adott cselekmény kritikus elemeire, például a cselekmény elkövetésének szándékára vagy az alibire irányul. Az ebben a meghatározásban említett adatok lényegében számok kombinációi, amelyek különféle információk alapjait képezik, mint például a szövegek, képek, hangok, videók. Más megfogalmazás szerint: Digitális bizonyíték bármilyen digitális formában tárolt vagy továbbított bizonyító erejű információ lehet, amelyet a bírósági eljárásban részt vevő valamelyik fél a tárgyalás során felhasznál(hat). A digitális bizonyítékok elfogadása előtt a bíróság megvizsgálhatja, hogy a bizonyítékok relevánsak-e, hitelesek-e, és elfogadhatók-e, és

Kifejezés	Meghatározás
	ha a vizsgált bizonyíték másolat, akkor szükség van-e az eredeti példányra.
Digitális nyomelemzés	A Digitális nyomelemzés (Angol: *Digital trace analysis)* egy összetett folyamat, amely adatgyűjtésből (on-line – logok, és off-line – egyéb naplóadatok, valamint operatív rendszerek adatainak gyűjtése), logelemzésből, az eredmény értelmezéséből és felhasználói riportkészítésből áll. A Sealog Digitális Nyomelemző Rendszer • összegyűjti a szervezet/cég működése szempontjából kritikus folyamatokban alkalmazott különböző informatikai rendszerek által rögzített digitális nyomokat; • felügyeli és ellenőrzi a nyomgyűjtést; • a forrásadatok feldolgozásával feltárja a rendellenességeket, felderíti a működési anomáliákat, az esetleges fenyegetéseket, és a rendszerek használata során felderíthető rejtett összefüggések elemzésével támogatja az ilyen típusú események megelőzését.
Digitális vízjel	A Digitális vízjel **(**Angolul*: Digital Watermark)* egy, a digitális multimédiás tartalomba beágyazott adat. A digitális vízjelet a tartalom hitelességének igazolására vagy a digitális tartalom tulajdonosának azonosítására használják, például: • szerzői jogi védelem • forráskövetés • közzétételkövetés, mint például vízjelekkel ellátott videók • rejtett kommunikáció
Dirty COW	A Dirty COW (*Dirty Copy-On-Write*-ból kialakult név*),* egy számítógép Linux kernelének biztonsági sérülékenysége, amelyen keresztül minden Linux alapú operációs rendszer (beleértve az Androidot is) megfertőzhető.
Dolgok mesterséges Intelligenciája	A Mesterséges Intelligenciája (Angol*: Artificial Intelligence of Things, AIoT*) egy általános kifejezés a mesterséges intelligenciának a tárgyak internetére (IoT) történő alkalmazására – ez egy új megközelítés, amely a sok egyszerű digitális kapcsolat leírására szolgál egy IoT rendszer hardver elemei között. A Tárgyak Internete milliárdnyi összekapcsolt eszközből állhat, beleértve a hagyományos, és az egymással hálózatba kapcsolt, internetes protokollokon keresztül kommunikáló eszközöket is. A Mesterséges Intelligenciával kiegészítve az IoT rendszerek új kérdéseket és újabb lehetséges megoldásokat vetnek fel, illetve mutathatnak. Amikor a Dolgok Internetjén az elemzéseket, műveleteket automatizált módon hajtják végre, a dolgok mesterséges intelligenciájáról beszélünk. A vállalatok és szervezetek ezzel szemben a dolgok mesterséges intelligenciájáról akkor beszélnek, amikor azoknak a lehetséges műveleteknek bővítéséről, kiterjesztéséről, fejlesztéséről beszélnek, amiket az egyes felhasználók a dolgok internetjén keresztül megtehetnek, vagy amikor arról, hogy a technológiák hogyan használhatják a dolgok internetét a saját működésükhöz.
Doxing v. Doxxing	Doxing – (angol kifejezés*, a dox a documents* rövidítése) Egy személy, vagy szervezet magán, vagy azonosításra alkalmas adatainak (különösen személyazonosításra alkalmas információinak) internet-alapú kutatási és közzétételi gyakorlata. Ezen információk megszerzésére alkalmazott módszerek tartalmazzák a nyilvánosan hozzáférhető adatbázisok és a közösségi média (Social Networks) oldalak (mint pl. a Facebook, Linkedln, Twitter) kereséseit, a hekkelést, és a pszichológiai befolyásolást (Social Networking) is. A doxing szorosan kapcsolódik az internetes bosszúálláshoz és hacktivizmushoz. A "doxing"-ot különböző okok miatt alkalmazzák,

Kifejezés	Meghatározás
	beleértve (a társadalmilag pozitív értelmű) a bűnüldözés támogatását, az üzleti elemzést, de a rosszindulatú (adott esetben törvényellenes) cselekvést is, vagyis pl. a zsarolást, a kényszerítést, a zaklatást, az online megszégyenítést és a bosszúállást egyaránt.
Durva hamisítvány	A Durva hamisítvány (Angol: *Deepfake*) kifejezést olyan videók, prezentációk esetén használjuk, amelyeket a mesterséges intelligencia, és más modern technológiák segítségével hoztak létre, hazug, valótlan és hamis események, eredmények bemutatására. A Durva hamisítványra az egyik legjobb példa a képfeldolgozás felhasználása, abból a célból, hogy videókat készítsenek hírességekről, politikusokról vagy más személyekről úgy, hogy olyat mondatnak, vagy csináltatnak a célszeméllyel, amelyet az soha nem is mondott vagy nem is tett. Jordan Peele, a kortárs kreatív médiaikon a YouTube-on bemutatta a viszonylag széles körben elérhető technológiák alkalmazását hamis videók készítésére (például Barack Obamaról). Nyugodtan mondhatjuk azt, hogy hamis videókat készíteni viszonylag nagyon könnyű. Ez rövid távon minden országban nemzetbiztonsági kérdéssé válhat, vagy különféle fogyasztói csalásokhoz vagy egyéb problémákhoz vezethet. Ennek szem előtt tartásával az informatikai értelemben fejlett országokban a vállalatvezetések, állami és civil szervezetek vezetései arról tárgyalnak, hogyan lehetnek megközelíteni az AI-t etikai szemszögből annak érdekében, hogy korlátozzák a durva hamisításokat és a hasonló csalásokat, valamint az ezeket lehetővé tevő technológiák által okozott károk megelőzését.
Egyszer használható jelszó	Az Egyszer használható jelszó (Angol: *One-time password* - OTP) olyan típusú jelszó, amely csak egy felhasználásra érvényes. Ez egy biztonságos módja annak, hogy hozzáférést biztosítson egy alkalmazáshoz, vagy egyszer és csak egyszer végezzen el egy tranzakciót. A jelszó használat után érvénytelenné válik, és ismételten már nem használható. Az egyszer használható jelszó egy olyan (olcsó) biztonsági technikát képvisel, amely védelmet nyújt különféle jelszó alapú támadásokkal, különösképpen a jelszó megszerzésével és újra felhasználásával járó támadásokkal szemben. Sokkal hatékonyabb védelmet nyújt, mint csupán a statikus jelszavak alkalmazása, amelyek több bejelentkezési munkamenetnél is változatlanok maradnak. Az egyszer használható jelszó olyan véletlen alapú algoritmusokon keresztül működik, amelyek minden alkalommal új jelszót generálnak. Az algoritmus mindig véletlenszerű karaktereket és szimbólumokat használ a jelszó létrehozásához, hogy a hackerek ne tudják kitalálni a jövőbeli jelszavakat. Az egyszer használható jelszó számos technikát használ a jelszó létrehozásához, például: – idő-szinkronizálás – a jelszó csak rövid ideig érvényes – matematikai algoritmus – a jelszót az algoritmuson belül képzett véletlen számok felhasználásával állítják elő
Elektronikai hadviselés	Katonai tevékenység, amely az elektromágneses energiát felhasználva meghatározza, felderíti, csökkenti vagy megakadályozza az elektromágneses spektrum ellenfél részéről történő használatát és biztosítja annak a saját oldali hatékony alkalmazását.
Elektronikus aláírás	Az elektronikus aláírás olyan kriptográfiai és (hozzá kapcsolódóan jogi) eljárás, amelynek segítségével joghatás kiváltására alkalmas, akár a kézzel írott aláírással vagy a közjegyző előtt tett aláírással egyenértékű bizonyító erejű dokumentum hozható létre. Az elektronikus aláírás a digitális aláíráshoz csak hasonló fogalom, de míg a digitális

Kifejezés	Meghatározás
	aláírás elsősorban a technológiát, az elektronikus aláírás a technológia mellett a jogi fogalmat is jelenti. Az elektronikus aláírás a következő jogi alapokon nyugszik: • a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról szóló 910/2014/EU európai parlamenti és tanácsi rendelet • Az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény az elektronikus ügyintézési szolgáltatások nyújtására felhasználható elektronikus aláíráshoz és bélyegzőhöz kapcsolódó követelményekről szóló 137/2016. (VI. 13.) Korm. rendelet
Elektronikus dokumentum	Olyan elektronikus eszköz útján értelmezhető adat, mely elektronikus aláírással van ellátva.
Elektronikus információs rendszer	Az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese. (Informatikai rendszer)Az elektronikus információs rendszerekhez tartoznak: • a számítástechnikai rendszerek és hálózatok, ide értve az internet szolgáltatást is; • helyhez kötött, mobil és egyéb rádiófrekvenciás, valamint műholdas elektronikus hírközlési hálózatok, szolgáltatások; • a vezetékes, a rádiófrekvenciás és műholdas műsorszórás; • a rádiós vagy műholdas navigáció; • az automatizálási, vezérlési és ellenőrzési rendszerek (SCADA, távmérő, távérzékelő és telemetriai rendszerek, stb.); • valamint a fentiek felderítéséhez, lehallgatásához vagy zavarásához használható rendszerek
Elektronikus információs rendszer biztonsága	Az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos. (Informatikai biztonság)
Elektronikus információs rendszer elemei	Lásd: Rendszerelemek.
Elektronikus információs rendszer védelme	Az elektronikus információs rendszerben kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának védelme, továbbá a rendszer elemei sértetlenségének és rendelkezésre állásának védelme. (Informatikai védelem)
Elektronikus irat	Olyan elektronikus dokumentum, melynek funkciója szöveg betűkkel való közlése és a szövegen kívül az olvasó számára érzékelhetően kizárólag olyan egyéb adatokat foglal magában, melyek a szöveggel szorosan összefüggenek, annak azonosítását (pl. fejléc), illetve könnyebb megértését (pl. ábra) szolgálják.
Elektronikus kereskedelmi szolgáltatás	Olyan információs társadalommal összefüggő szolgáltatás, amelynek célja áruk, illetőleg szolgáltatások üzletszerű értékesítése, beszerzése, cseréje.
Elektronikus okirat	Olyan elektronikus irat, mely nyilatkozattételt, illetőleg nyilatkozat elfogadását, vagy

Kifejezés	Meghatározás
	nyilatkozat kötelezőnek elismerését foglalja magában.
Életciklus	Az elektronikus információs rendszer tervezését, fejlesztését, üzemeltetését és megszüntetését magába foglaló időtartam.
Érintett	Bármely meghatározott személyes adat alapján azonosított vagy egyébként – közvetlenül vagy közvetve – azonosítható természetes személy. A személy különösen akkor tekinthető azonosíthatónak, ha őt – közvetlenül vagy közvetve – név, azonosító jel, illetőleg egy vagy több, fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző tényező alapján azonosítani lehet.
Észlelés	A biztonsági esemény bekövetkezésének felismerése.
Fejlesztési környezet	A fejlesztés tárgyának előállítása során érvényesített szervezeti intézkedések, eljárások és szabványok.(Angol: *Development Environment*)
Fejlesztői biztonság	A fejlesztőnek a fejlesztési környezetére gyakorolt fizikai, eljárási és személyi védelmi szabályozói, biztonsági intézkedései.(Angol: *Developer Security*)
Felelősségre vonhatóság	Olyan tulajdonság, amely lehetővé teszi, hogy az adott entitás tevékenységei egyértelműen az adott entitásra legyenek visszavezethetők.
Felhasználó	Egy adott elektronikus információs rendszert igénybe vevők köre.
Felhasználói dokumentáció	A fejlesztő által a végfelhasználó részére, a fejlesztés tárgyáról készített információ.(Angol: *User Documentation*)
Felhasználói program	Lásd: Alkalmazás.
Fenyegetés	Olyan lehetséges művelet vagy esemény, amely sértheti az elektronikus információs rendszer vagy az elektronikus információs rendszer elemei védettségét, biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer védettségét, biztonságát.(Angol: *Threat*)
Féreg	Olyan program, amely a számítógép hálózaton keresztül, a hálózati funkciók kihasználásával terjed számítógéptől számítógépig és károkozó hatását önmaga – a számítógép összeomlásáig tartó reprodukálásával, továbbításával éri el.(Angol: *Worm*)
Fizikai védelem	A fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai jelzőrendszer, az élőerős védelem, a beléptető-rendszer, a megfigyelő rendszer, a tápáramellátás, a sugárzott és vezetett zavarvédelem, klimatizálás és a tűzvédelem.
Fokozott biztonságú elektronikus aláírás	Olyan elektronikus aláírás, amely: • alkalmas az aláíró azonosítására és egyedülállóan hozzá köthető, • olyan eszközzel hozták létre, mely kizárólag az aláíró befolyása alatt áll, • a dokumentum tartalmához olyan módon kapcsolódik, hogy minden – az aláírás elhelyezését követően az iraton, illetve dokumentumon tett – módosítás érzékelhető.
Folytonos védelem	Az az időben változó körülmények és viszonyok között isis megszakítás nélkül megvalósuló védelem.
Futtatható melléklet nélküli malware	Futtatható melléklet nélküli malware (Angol: *Fileless Malware*) alatt, olyan rosszindulatú programokat értünk, amelyek hagyományos futtatható fájl használata nélkül működnek. Egy csatolmány, illetve egy hagyományos futtatható fájl helyett az

Kifejezés	Meghatározás
	ilyen típusú rosszindulatú programok a támadási vektor létrehozásához sérülékenységeket, makrókat vagy más eszközöket használnak fel anélkül, hogy a felhasználó letölthetne és telepítene egy valódi futtatható fájlt.
Galois / számláló mód	A Galois/számláló mód (Angol: *Galois/Counter Mode,* rövidítve GCM) a kriptográfiában a hatékonyságának, teljesítményének köszönhetően széles körben alkalmazott szimmetrikus kulcsú kriptográfiai blokkok rejtjeleinek működési módja . A korszerű, nagy sebességű kommunikációs csatornák GCM átviteli sebessége olcsó hardver erőforrásokkal is elérhető. A művelet egy hitelesített titkosítási algoritmus, amely az adatok hitelességének, integritásának és bizalmasságnak egyaránt megfelel. A GCM 128 bites blokkmérettel került meghatározásra. A Galois üzenet hitelesítési kód (GMAC) a GCM-nek a csak hitelesítésére szolgáló változata, amely növekményes üzenet-hitelesítési kódot képezhet. Mind a GCM, mind a GMAC tetszőleges hosszúságú inicializációs vektorokat képes elfogadni. A különböző blokk rejtjel működési módok egymáshoz képest jelentősen eltérő teljesítmény- és hatékonysági jellemzőkkel rendelkeznek, még akkor is, ha ugyanazt a blokk rejtjelet használják. A GCM teljes mértékben kihasználhatja a párhuzamos feldolgozás előnyeit, és a GCM végrehajtása hatékonyan működhet szoftver vagy hardver megoldásokban egyaránt.
GDPR	General Data Protection Regulation (GDPR) – Általános Adatvédelmi Rendelet Az Európai Parlament és a Tanács által elfogadott, a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló 2016/679 rendelet.
Gyakoriság	0 és 1 közötti érték, amely azt mutatja, hogy valamilyen esemény a kísérletek mekkora hányadában következik be. Pontosan: relatív gyakoriság.
Gyenge pont	Az informatikai rendszerelem olyan része vagy tulajdonsága, amelyen keresztül valamely fenyegetés megvalósulhat.
Hacker	Az informatikai rendszerbe informatikai eszközöket használva, kifejezett ártó szándék nélküli betörő személy. A tömegkommunikációban helytelenül minden számítógépes bűnözőre használják. Eredeti jelentése szerint a hacker olyan mesterember, aki fából tárgyakat farag. Lásd még: Cracker.
Hálózat	Informatikai eszközök közötti adatátvitelt megvalósító logikai és fizikai eszközök összessége.
Hash-függvény	Olyan transzformáció, amely egy tetszőleges hosszú szöveg egyedi, az adott szövegre jellemző fix hosszúságú digitális sűrítményét készíti el.
Hitelesítés szolgáltató	Olyan mindenki által megbízhatónak tartott, szakosodott szervezet, amely tanúsítványokat adhat ki kliensek és szerverek számára. Elektronikus vagy digitális közjegyzőnek is nevezik.
Hitelesség	Az adat tulajdonsága, amely arra vonatkozik, hogy az adatot bizonyítottan vagy bizonyíthatóan az elvárt forrásból származik.
Hoax	Olyan e-mail, ami valamilyen új – általában fiktív – vírus terjedésére figyelmeztet, és a fertőzés megakadályozása érdekében egy vagy több fájl törlésére ösztönöz (ezek azonban a rendszer működéséhez szükséges, de kevésbé ismert állományok). Az e-mail

Kifejezés	Meghatározás
	továbbküldésre is buzdít, hogy a levéláradat – lánc-levél – szűk keresztmetszetet generáljon a hálózaton.
Időbélyegző	Olyan, az elektronikus irathoz, illetve dokumentumhoz végérvényesen hozzárendelt, illetőleg az irattal vagy dokumentummal logikailag összekapcsolt igazolás, amely tartalmazza a bélyegzés időpontját, és amely a dokumentum tartalmához technikailag olyan módon kapcsolódik, hogy minden – az igazolás kiadását követő – módosítás érzékelhető.
Illetéktelen személy	Valamely legális tevékenység végzésére nem jogosult személy. Az informatikai biztonság esetében tipikusan az objektumba, az informatikai rendszerbe történő belépésre, adatkezelésre nem jogosult személy.
Industrial Cybersecurity	Industrial Cybersecurity (ICS) - Ipari kiber biztonság
Információ	Az Információ latin eredetű szó, amely értesülést, hírt, üzenetet, tájékoztatást jelent. Egyben az informatika alapfogalma. Számos jelentése, kifejtése ismert, különböző tudományágak különböző módon közelítik meg, írják le. Egyértelműen elfogadott definíciója nem ismert. Általánosságban információnak azt az adatot, hírt tekintjük, amely számunkra releváns és ismerethiányt csökkent. Egyik legleegyszerűsítettebb megfogalmazás szerint az információ nem más, mint a valóság (vagy egy részének) visszatükröződése.
Információ biztonsági incidens	Olyan nem kívánt vagy nem várt egyedi vagy sorozatos információbiztonsági esemény(ek), amely(ek) nagy valószínűséggel veszélyezteti(k) az üzleti tevékenységet és fenyegeti(k) az üzleti rendszer információbiztonságát. Nem minden információbiztonsági esemény minősíthető incidensként. az ITIL informatikai szolgáltatás módszertan szerint egy Incidens (Angol: *Incident*) olyan esemény, amely nem része az informatikai szolgáltatások normális működésének és szolgáltatás(ok) kiesését vagy minőségének romlását eredményezi. Az Incidens kiváltó oka egy probléma. Az ITIL meghatározása szerint a probléma az incidens(ek) valódi, még fel nem tárt oka. Ez az ok akár egy meghibásodott konfigurációs elem is lehet, de akár egy ismeretlen hiba is.
Információs műveletek (információs hadviselés)	Hadban álló felek között az információs fölény elérése érdekében végrehajtott, a szemben álló fél információi, információalapú folyamatai, információs rendszerei és számítógépes hálózatai befolyásolására, illetve a saját információk, információalapú folyamatok, információs rendszerek és számítógépes hálózatok védelmére irányuló tevékenységek összessége. (Nem azonos a kiberműveletekkel) (Angol: *Information Operation* (*Information Warfare*, röviden: INFOWAR))
Információs önrendelkezési jog	Az egyén joga arra, hogy ellenőrizze vagy befolyásolja azt, hogy ki és milyen vele kapcsolatos adatot kezelhet.
Információs társadalommal összefüggő szolgáltatás	Olyan elektronikus úton, távollevők részére, ellenszolgáltatás fejében nyújtott szolgáltatás, amelynek igénybevételét a szolgáltatás igénybe vevője egyedileg kezdeményezi, továbbá mindazon ellenszolgáltatás nélkül, elektronikus úton, távollevők részére, az igénybe vevő egyedi kezdeményezésére nyújtott szolgáltatások, amelyek a szolgáltató, illetve az igénybe vevő részéről nem az Alkotmány által biztosított véleményszabadság gyakorlásának körébe tartoznak.
Információ védelem	Az információk bizalmasságának, sértetlenségének és rendelkezésre állásának védelme.

Kifejezés	Meghatározás
Informatikai biztonság	Lásd: Elektronikus információs rendszer biztonsága.
Informatikai biztonsági stratégia	Az informatikai biztonságpolitikában kitűzött célok megvalósításának útja, módszere.
Informatikai biztonságpolitika	A biztonsági célok, alapelvek és a szervezet vezetői elkötelezettségének bemutatása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok irányítására és támogatására.
Informatikai rendszer	Lásd: Elektronikus információs rendszer.
Informatikai rendszer elemei	Lásd: Rendszerelemek.
Informatikai védelem	Lásd: Elektronikus információs rendszer védelme.
Information Technology	Information Technology (IT) – információtechnológia, informatika
Internet	A TCP/IP protokollon alapuló, nyilvános, világméretű számítógépes hálózat. Az Internet a szolgáltatások széles skáláját nyújtja felhasználóinak (FTP, Gopher, IRC, e-mail, telnet, UUCP, WWW stb.).
Internet of Things (IoT)	Lásd: Tárgyak Internete
Intrusion Detecting System	Lásd: Betörés detektáló eszköz.
Ismeret	Ismeretnek nevezzük a valóságra vagy annak valamely részére, témájára vonatkozó tapasztalatokat, általánosításokat, fogalmakat. Aki ismer valamit, az tájékozott (informált), tapasztalt a "valamiben", míg aki nem, annak hiányosak az ismeretei vagy nincs fogalma a dologról. Az ismeretek tartalmi megkülönböztetésének egyik módja a kategorizálás, másik módja lehet a hordozó, műfaj, vagy az ismeret egyéb minősége (frissesség, érthetőség, hozzáférhetőség, ár stb.) szerint való.
Jelszó	A jelszó (Angol: *password*), vagy más néven kulcsszó, kódszó, kód-, vagy jelmondat, egy jelből vagy jelsorból álló kifejezés, melyet azonosításnál, illetve hitelesítéshez használunk. Ebből a célból egy információt használunk igazolvány gyanánt, amely arra szolgál, hogy egy egyedi azonosító segítségével felcserélhetetlenül megerősíthessük kilétünket. A hitelesség legfeljebb csak addig tartható fenn, amíg a jelszó titokban (azaz illetéktelenek számára ismeretlen) marad.
Katasztrófa elhárítás-tervezés	Az informatikai rendszer, rendelkezésre állásának megszűnése, nagymértékű csökkenése utáni visszaállításra vonatkozó tervezés
Kiber zsarolás	A kiber zsarolás a fenyegetések egy olyan formája, mely esetén az informatikai támadás áldozatait a károk elkerülése érdekében, váltságdíj fizetésre kényszerítik.

Kifejezés	Meghatározás
Kiber-rugalmasság	A Kiber-rugalmasság (Angol: *Cyber resilience*) vagy másképpen Kiber-ellenállóképesség arra utal, hogy az entitás folyamatosan képes elérni egy kívánt eredményt a kedvezőtlen kibernetikus események ellenére is. A kiber-rugalmasság egy olyan változó nézőpontot eredményez, amely segítségével egy állapot kedvezőtlen helyzete gyorsan felismerésre kerülhet. A kiber-rugalmasság koncepciója lényegében egyesíti az információbiztonság, az üzletmenet folytonosság és a (szervezeti) ellenálló képesség területét. Azok a szervezetek, amelyeknek potenciálisan kiber-rugalmasságra van szükségük, többek között az IT rendszerek, a kritikus infrastruktúra, az üzleti folyamatok, (de a szervezetek, a társadalmak és a nemzetállamok is). A kedvezőtlen számítógépes események negatívan befolyásolják a hálózatba kapcsolt IT rendszerek, valamint a hozzájuk kapcsolódó információs rendszerek és szolgáltatások elérhetőségét, integritását vagy bizalmas jellegét. Ezek az események szándékos (pl. számítógépes támadás) vagy nem szándékos (pl. sikertelen szoftverfrissítés) történések eredményei, amelyeket emberek vagy a természet, vagy ezek kombinációja okozhat. A kiber-rugalmasság kialakításának célja, hogy segítségével fenntartsák az entitás azon képességét, hogy mindenkor folyamatosan elérje a kívánt eredményt. Ez tehát akkor is megtörténik egy kiber-rugalmas rendszerben, ha a rendszeres kézbesítési mechanizmusok kudarcot vallanak – például válság idején vagy egy biztonsági esemény megtörténte után. A kiber-rugalmasság koncepciója magában foglalja a rendszeres kézbesítési mechanizmusok helyreállításának képességét az ilyen események után, valamint azt a képességet is, hogy ezeket a kézbesítési mechanizmusokat folyamatosan meg tudjuk változtatni, vagy módosítani tudjuk, amennyiben ez szükséges, a felmerülő új kockázatokkal szemben. A biztonsági mentések és a katasztrófa utáni helyreállítási műveletek is a kézbesítési mechanizmusok helyreállítási folyamatának részét képezik.
Kiberműveletek	A kibertér képességek alkalmazása, ahol az elsődleges cél katonai eredmények vagy hatások elérése a kibertérben vagy azon keresztül. (A kiberműveletek nem egyenlőek az információs műveletekkel. Az információs műveleteket el lehet végezni a kibertérben, és más területeken egyaránt. A kiberműveletek közvetlenül támogatják az információs műveleteket és a nem internetes alapú információs műveletek hatással lehetnek a kiberműveletekre.)(Angol.: *Cyberspace operations, Cyberoperations*)
Kibertér	Egy globális tartomány az informatikai környezeten belül, amely tartalmazza az egymással összefüggő informatikai hálózatok infrastruktúráit, beleértve az internetet, a távközlési hálózatokat, a számítógépes rendszerek és beágyazott processzorokat és vezérlőket. (Megjegyzés: Eredetileg W. Gibson regényéből átvett science-fiction kifejezés, mely a számítógép-kommunikáció birodalmát, annak virtuális világát kívánja megnevezni. Eszerint a kibertér nem más mint a hálózatba kötött számítógépek által létrehozott virtuális valóság világa, annak összes objektumával egyetemben.) (Angol: *Cyberspace*)
Kockázat	A fenyegetettség mértéke, amely valamely fenyegető tényezőből ered, és amelyet a kockázatelemzés során a fenyegető tényezők értékelése révén tárunk fel. A kockázatot egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye.

Kifejezés	Meghatározás
Kockázatelemzés	Az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése.
Kockázatkezelés	Az elektronikus információs rendszerre ható kockázatok csökkentésére irányuló intézkedésrendszer kidolgozása és végre hajtása. Kockázatmenedzsment (Angol: *Risk Management)*
Kockázattal arányos védelem	Az elektronikus információs rendszer olyan védelme, amelynek során - egy kellően nagy időintervallumban - a védelem költségei arányosak a fenyegetések által okozható károk értékével.
Korai figyelmeztetés	Valamely fenyegetés várható bekövetkezésének jelzése a fenyegetés bekövetkezése előtt annyi idővel, hogy hatékony védelmi intézkedéseket lehessen hozni.
Korrelációs logelemzés	A korrelációs logelemzés egy olyan technológia, amely a különböző rendszerekről gyűjthető logokat (üzeneteket) „veti” össze úgy, hogy miközben az elemzési adatok között egyetlen eseményhez tartozó összes üzenet megtalálható (pl. a különböző rendszerekben – hálózati eszközök, tűzfalak, szerverek, programok – egy hibás, vagy rosszindulatú tevékenység által generált üzenetek), korrelációs vizsgálatot végeznek annak érdekében, hogy megállapítsák, a történés típusát (hiba, rosszindulatú beavatkozás stb.). (A statisztikában a korreláció jelzi két tetszőleges érték közötti lineáris kapcsolat nagyságát és irányát [avagy ezek egymáshoz való viszonyát]. Az általános statisztikai használat során a korreláció jelzi azt, hogy két tetszőleges érték nem független egymástól. A korreláció csak a lineáris kapcsolatot jelzi. Ha a korreláció értéke 1, akkor a két változó kapcsolata tökéletes egyenes arányosság. 0, akkor nincs kapcsolat a két változó között, függetlenek.)
Követelmények	A fejlesztési folyamatnak azon szakasza, melyben a fejlesztés tárgyának védelmi célját határozzák meg.(Angol: *Requirements)*
Közérdekű adat	Olyan – nem személyes – adatok, amelyek az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében vannak.
Kriptoanalízis (kriptográfiai bevizsgálás)	A rejtjeles üzenet illetéktelenek általi, azaz eljárás ismerete nélkül, vagy annak részleges ismeretében az eredeti üzenetet visszaállításának kísérlete.
Kriptográfia	Mindazoknak az eljárásoknak, algoritmusoknak, biztonsági rendszabályoknak kutatását, alkalmazását jelenti, amelyek információnak illetéktelenek előli elrejtését hivatottak megvalósítani. Lásd még: Rejtjelezés
Kriptológia	A kriptoanalízis és a kriptográfia elméletének és gyakorlatának együttese.
Kritikus információs infrastruktúrák	Azon az infokommunikációs létesítmények, eszközök vagy szolgáltatások, amelyek önmagukban is kritikus infrastruktúra elemek, továbbá a kritikus infrastruktúra elemeinek azon infokommunikációs létesítményei, eszközei vagy szolgáltatásai, amelyek működésképtelenné válása, vagy megsemmisülése a kritikus infrastruktúrákat, vagy azok részeit elérhetetlenné tenné, vagy működőképességüket jelentősen

Kifejezés	Meghatározás
	csökkentené. A mai magyar jogalkotásban: létfontosságú információs rendszerelem
Kritikus infrastruktúrák	Azon létesítmények, eszközök vagy szolgáltatások, amelyek működésképtelenné válása, vagy megsemmisülése a nemzet biztonságát, a nemzetgazdaságot, a közbiztonságot, a közegészségügyet vagy a kormány hatékony működését gyengítené, továbbá azon létesítmények, eszközök és szolgáltatások, amelyek megsemmisülése a nemzeti morált vagy a nemzet biztonságába, a nemzetgazdaságba, vagy a közbiztonságba vetett bizalmat jelentősen csökkentené. A mai magyar jogalkotásban: létfontosságú rendszerek, rendszerelemek
Kulcs	A kriptológiában a rejtjelezés és a megfejtés műveleteihez használt szimbólumok sorozata. Az adatbázis-kezelésben egy rekord vagy rekordcsoport azonosítója. A mechanikai védelemben a zárak nyitásához és zárásához használt eszköz.(Angol: *Key*)
Kulcs menedzsment	A kriptográfiában a rejtjelzés és a megfejtés műveleteihez használt kulcsok előállítása, tárolása, szétosztása, törlése, archiválása és alkalmazása, illetve ezek szabályrendszere.(Angol: *Key management*)
Különleges adat	A faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre, az egészségi állapotra, valamint a kóros szenvedélyre vonatkozó és a bűnügyi személyes adat.
Különleges adat	A faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre, az egészségi állapotra, genetikai vagy biometrikus jellemzőkre, valamint a kóros szenvedélyre vonatkozó és a bűnügyi személyes adat.
Letagadhatat-lanság	Valamilyen esemény, tipikusan a kommunikáció során a származás, vagy a kézbesítés megtörténtének garantálása.(Angol: *Non-repudiation*)
Locky	A Locky egy zsarolóprogramot tartalmazó malware (fenyegetés), amely 2016-ban jelent meg. A terjesztése e-mailben történik, egy csatolt Microsoft Word dokumentumban (ami például egy teljesített díjfizetés számlájának látszik), és amely rosszindulatú makrókat tartalmaz. Amikor a felhasználó megnyitja a dokumentumot, úgy tűnik számára, hogy az tele van szeméttel, de a dokumentum szövege tartalmazza az "Enable macro if data encoding is incorrect!" megtévesztő üzenetet is. Ha a felhasználó a felszólításnak eleget téve engedélyezi makrók futtatását, a makrók elmentenek és futtatnak egy bináris fájl, amely letölti az aktuális titkosítást végző trójai programot, amely végül titkosítja az összes olyan fájlt, amely bizonyos kiterjesztéssel rendelkezik. A fájlneveket egy egyedi 16 betűből és számból valamint a .locky fájl-kiterjesztésből álló fájlnévvé alakítja.
Log elemzés	Az informatikai rendszerek főbb alkotóelemei – az operációs rendszerek, az alkalmazások, a különféle szoftver és hardver elemek – működésük során naplófájlokban rögzítik a különböző folyamatok, események részleteit, rengeteg naplóbejegyzésben, vagy más néven logban. A logok a működés szempontjából kifogástalan naplóbejegyzések mellett a rendellenes működéseket – (vagyis az incidenseket) – jelző naplóbejegyzéseket is tartalmaznak. Az incidenseket mindig megelőzi a rendszerekben bekövetkező viselkedésbeli változás. A rendszerek működése során esetleg előforduló incidensek felderítését, a hiba/probléma meghatározását a logok (naplóbejegyzések) elemzésével derítik fel. A log elemzés az összegyűjtött, központosított, aggreált (vagyis feldolgozható formába

Kifejezés	Meghatározás
	átalakított) naplóbejegyzéseken kerül végrehajtásra. Egy naplóelemző rendszer az informatikai rendszerek naplóállományait összegyűjteni és tárolni képes, és igény szerinti vizsgálatokat végrehajtani tudó megoldás. A naplóelemzés célja sokféle lehet, például az üzemeltetés támogatása vagy a biztonság növelése. Az elemzési feladatokat külső és belső szabályzók, illetve igények határozhatják meg. *(*Angol: *Log analysis)*
Logikai bomba	Olyan program vagy programrészlet, amely logikailag (funkcionálisan) nem várt hatást fejt ki. Jelentkezése váratlan, hatása pusztító – innen a bomba kifejezés. (Angol: *Logic bomb*)
Logikai védelem	Az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem, amelynek fontosabb részei az azonosítás és a hitelesítés, a hozzáférés-védelmi rendszer, a bizonyítékok rendszere.
Makrovírus	Olyan dokumentumhoz csatolt (abban tárolt) makrónyelven írt vírus, amely a dokumentumot kezelő és a makrót használni képes alkalmazáshoz kötődik. Hatását a dokumentum használata során fejti ki.
Malware	Az angol malware kifejezés az angol malicious software (rosszindulatú szoftver, káros szoftver, kártékony szoftver) összevonásából kialakított mozaikszó. Mint ilyen, a rosszindulatú számítógépes programok összefoglaló neve. Ide tartoznak a vírusok, férgek (worm), kémprogramok (spyware), agresszív reklámprogramok (adware), a rendszerben láthatatlanul megbúvó, egy támadónak emelt jogokat biztosító eszközök (rootkit).
Megelőzés	A fenyegetés hatása bekövetkezésének elkerülése.
Megfelelő tájékoztatás	Az érintettel az adatkezelés megkezdése előtt közölni kell, hogy az adatkezelés a hozzájárulásán alapul-e vagy kötelező, továbbá egyértelműen és részletesen tájékoztatni kell az adatai kezelésével kapcsolatos minden tényről, így különösen az adatkezelés céljáról és jogalapjáról, az adatkezelésre és az adatfeldolgozásra jogosult személyéről, az adatkezelés időtartamáról, illetve arról, hogy kik ismerhetik meg az adatokat. A tájékoztatásnak ki kell terjednie az érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire is.
Megoldás (desifrírozás)	A rejtjeles üzenet legális címzettje által, az eljárás ismeretében az eredeti üzenetet visszaállítása.
Megszemélyesítés	1. A megszemélyesítés, idegen szóval perszonifikáció (a latin personificatio szóból) vagy antropomorfizáció olyan reprezentáció, amely elvont dolgokat, élettelen tárgyakat vagy természeti jelenségeket, illetve növényeket vagy állatokat az emberekre jellemző érzésekkel és tulajdonságokkal ruház fel. 2. Egy entitás (személy, program, folyamat stb.) magát más entitásnak tünteti fel
Minősítés	Az a döntés, melynek meghozatala során az arra felhatalmazott személy megállapítja, hogy egy adat a tartalmánál fogva a nyilvánosságát korlátozó titokkörbe tartozik.

Kifejezés	Meghatározás
Minősített adat	Nemzeti minősített adat: a minősítéssel védhető közérdekek körébe tartozó, a minősítési jelölést törvényben, valamint a törvény felhatalmazása alapján kiadott jogszabályokban meghatározott formai követelményeknek megfelelően tartalmazó olyan adat, amelyről - a megjelenési formájától függetlenül - a minősítő a minősítési eljárás során megállapította, hogy az érvényességi időn belüli nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, továbbá illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele a minősítéssel védhető közérdekek közül bármelyiket közvetlenül sérti vagy veszélyezteti (a továbbiakban együtt: károsítja), és tartalmára tekintettel annak nyilvánosságát és megismerhetőségét a minősítés keretében korlátozza, Külföldi minősített adat: az Európai Unió valamennyi intézménye és szerve, továbbá az Európai Unió képviseletében eljáró tagállam, a külföldi részes fél vagy nemzetközi szervezet által készített és törvényben kihirdetett nemzetközi szerződés vagy megállapodás alapján átadott olyan adat, amelyhez történő hozzáférést az Európai Unió intézményei és szervei, az Európai Unió képviseletében eljáró tagállam, más állam vagy külföldi részes fél, illetve nemzetközi szervezet minősítés keretében korlátozza.
Minősített elektronikus aláírás	Olyan – fokozott biztonságú – elektronikus aláírás, amely biztonságos aláírás létrehozó eszközzel készült, és amelynek hitelesítése céljából minősített tanúsítványt bocsátottak ki.
Naplóelemzés	Lásd: Logelemzés Angol: *Log analysis*
Naplókezelés	Az informatikában/információtechnológiában nagyszámú, számítógép(ek)kel előállított naplóüzenet (más módon: naplózási nyilvántartás, naplózási idősor rekord, eseménynaplók stb.) kezelését jelenti. A Naplókezelés során általában a következő feladatokkal kell foglalkozni: • Helyi (lokális) loggyűjtés (rendszerek kiválasztása és konfigurálása) • Központosított loggyűjtés • A naplók hosszú távú tárolása, megőrzése • A logok folyamatos frissítése • Naplóelemzés v. log elemzés (valós időben és tömegesen a tárolást követően) • Jelentések készítése és keresés a mentett naplóállományok között Angol*: Log managemen*)
NAS	A NAS angol betűszó a Network Attached Storage, azaz a hálózatra kapcsolt tároló rövidítése. Magyar megfelelője: hálózati adattároló. A NAS fájl szintű adattároló eszköz, amely egy számítógépes hálózatba csatlakoztatva biztosítja az adatok megfelelő tárolását és menedzselését, biztosítja a tárolt adatok elérését a feljogosított helyi és távoli felhasználók számára, legyenek azok akár egy másik földrészen is. A tárolt adatok megoszthatók, internetkapcsolat segítségével bárhonnan elérhetőek, védelmük a felhasználói engedélyek megfelelő beállításával oldható meg. A NAS egy speciális hardvert és szoftvert is tartalmazó eszköz, amely többplatformos hozzáféréssel (OS, Linux, Unix, Windows) rendelkezik, illetve különböző célprogramokat (is) tartalmazhat (pl. Plex, Netflix, Skype stb.)

Kifejezés	Meghatározás
Négy szem elv	Olyan biztonságot megkövetelő tevékenység, amelyet két személy, egymást ellenőrizve végezhet.
Nulladik napi támadás	A nulladik napi támadás (zero-day vagy zero-hour támadás) egy biztonsági rés (valamely számítógépes alkalmazásnak a támadásig még nem nem ismert sebezhetősége) felhasználásával végrehajtott kibertámadás. A biztonsági rés ebben az esteben olyan, amely még nem került publikálásra, a szoftver fejlesztője nem tud róla, vagy nem érhető még el sérülékenységet megszüntető biztonsági javítás. Zero-day exploitnak pedig azt a tényleges kódot nevezik , amelyet a támadók felhasználnak a sérülékenység kiaknázására, mielőtt a szoftver fejlesztője tudomást szerezhetne a sérülékenységről.
Nyilvános kulcsú infrastruktúra	Az elektronikus aláírás létrehozására, ellenőrzésére, kezelésére, illetve titkos vagy hiteles kommunikációra szolgáló, aszimmetrikus kulcspárokat alkalmazó infrastruktúra, beleértve a mögöttes intézményrendszert, a különböző szolgáltatókat és eszközöket is.
Nyilvános kulcsú rendszer	Olyan kriptográfiai rendszer, amelyben a résztvevők két – a használattól függő – kulcsot egy közös algoritmussal használnak rejtjelezésre és a rejtjelezett adatok megoldására, vagy az adatok hitelesítésére (digitális aláírás) és annak ellenőrzésére. A kulcsok egyikét nevükkel együtt nyilvánosságra hozzák (nyilvános kulcs), a másikat titokban tartják (magánkulcs). Az üzenetet küldő a címzett nyilvános kulcsával rejtjelezi, a saját magánkulcsával hitelesíti az adatot (üzenetet), a címzett csak a saját magánkulcsával tudja megoldani a rejtjelezett üzenetet, illetve az aláírt üzenet sértetlenségét (és hitelességét) a küldő nyilvános kulcsával ellenőrizheti.
Nyilvánosságra hozatal	Az adatnak meghatározhatatlan körben, mindenki részére biztosított megismerhetővé, hozzáférhetővé tétele;
Onboard Intelligence	Lásd: Beépített intelligencia
One-time password	Lásd: Egyszer használható jelszó
Operational Technology	Operational Technology (OT) – működési technológia
Panda Security	A Panda Security egy spanyol multinacionális vállalat, amely informatikai biztonsági megoldások fejlesztésére szakosodott. A cég kezdetben antivírus szoftver fejlesztésére fókuszált, de azóta kibővítette üzleti tevékenységét a kiberbűnözés megakadályozását célozva, fejlett számítógépes biztonsági szolgáltatások technológiáinak kidolgozásán keresztül. A Panda Security szabadalmaztatott technológiája a TruPrevent, amely egy sor proaktív képesség birtokában képes blokkolni az ismeretlen vírusokat, felhasználva a Collective Intelligence (Kollektív Intelligencia) modelljét, az első olyan rendszert, amely valós időben automatikusan képes észlelni, elemzni és osztályozni a malware-eket, és az új Adaptive Defense (adaptív védelmi) biztonsági modellje képes előre jelezni azokat..

Kifejezés	Meghatározás
PGP (Pretty Good Privacy)	Philipp Zimmermenn által kifejlesztett, az Interneten gyakran használt nyilvános kulcsú kriptográfiai program elektronikus levelek rejtjelezésére és elektronikus aláírásra.
PKI – Public Key Infrastructure.	Lásd: Nyilvános Kulcsú Infrastruktúra.
Program	A számítógépes utasítások logikailag és funkcionálisan összetartozó sorozata.
Programhiba	A program leírástól (specifikációtól) eltérő működése.
Pszichológiai befolyásolás	A pszichológiai befolyásolás (Angol: *Social Engineering*) az informatikai rendszerekhez (is) kötődő fogalom, annak a fajta támadásnak a meghatározását sűríti egy kifejezésbe, amikor a támadó nem technológiai sebezhetőségeket használ ki, hanem arra törekszik, hogy megtévesszen egy felhasználót. A megtévesztés eredményeként a jogosultsággal rendelkező felhasználó a jogosulatlan személy számára bizalmas adatokat ad át, vagy lehetőséget biztosít számára a saját, vagy szervezete egy vagy több rendszerébe történő belépésre, kimondottan a pszichológiai befolyásolást végző személy megtévesztő viselkedése miatt. Akik pszichológiai manipuláció útján akarnak hozzájutni információkhoz, általában az emberi természet két aspektusát igyekeznek kihasználni. • Az első: a legtöbb ember segítőkész és igyekszik segíteni azoknak, akik segítséget kérnek. • A második pedig az, hogy az emberek általában konfliktuskerülők, és inkább együttműködnek, mint nem.
Public Key Cryptosystem	Lásd: Nyilvános kulcsú rendszer.
Ransomvare	A ransomware olyan malware, azaz rosszindulatú számítógépes program, amely valamilyen fenyegetéssel próbál pénzt kicsikarni a felhasználóból. Ez rendszerint azt jelenti, hogy használhatatlanná teszi a számítógépet vagy elérhetetlenné a rajta lévő adatokat, és csak pénzért vásárolható meg az a kód, aminek a hatására visszaállítja az eredeti állapotot.
Reagálás	A bekövetkezett biztonsági esemény terjedésének megakadályozására vagy késleltetésére, a további károk mérséklésére tett intézkedés.
Rejtett ajtó	Olyan programszegmens, amely a tartalmazó program futtatása során nem dokumentált műveleteket végez illegális, többnyire károkozási célból.(Lásd még: Hátsó ajtó (Angol: *Backdoor*), Csapóajtó (Angol: *Trap door*)
Rejtjelezés	Nyílt üzenetet kódolása kriptográfiai eljárással, eszközzel vagy módszerrel. A rejtjelezés eredménye a rejtjeles üzenet.

Kifejezés	Meghatározás
Rendelkezésre állás	Az az elektronikus információs rendszer vagy annak elemének tulajdonsága, amely arra vonatkozik, hogy az (ideértve az abban vagy az által kezelt adatot is) a szükséges időben és időtartamban használható.
Rendszer	Adott rendeltetésű, egymással kapcsolatban álló eszközök, eljárások, valamint az ezeket kezelő, kiszolgáló és a felhasználó személyek együttese.(Angol: *System*)
Rendszerelemek	Az elektronikus információs rendszer (informatikai rendszer) részét képző elemek. A rendszerelemek csoportjai: • eszközök: • az informatikai rendszer fizikai környezete és a működéséhez szükséges infrastruktúra; • hardver; • kommunikáció és hálózat; • adathordozók; • eljárások: • szoftver; • szabályozás; • emberek: • személyek.
Rendszerprogram (rendszerszoftver)	Az operációs rendszer részeként futó programok.
Rendszerterv	A fejlesztési folyamatnak az a szakasza, melyben a fejlesztés tárgyának felső szintű definíciója és terve kerül meghatározásra.(Angol: *Architectural Design*)
RSA rejtjelezés	Ronald Rivest, Adi Shamir és Leonard Adleman 1978-ban szabadalmazott nyilvános kulcsú kriptográfiai algoritmus.(Angol: *RSA encrytion*)
Scareware	A Scareware alatt olyan rosszindulatú számítógépes programokat értünk, amelyek abból a célból készültek, hogy becsapják a felhasználót, és rávegyék olyan felesleges és potenciálisan veszélyes szoftverek vásárlására és letöltésére, mint például a hamis vírusvédelemi programok. "… a jelentés újabb aggasztó megállapítása az ijesztő eszközök óriási növekedése…" A Scareware általános társadalmi fogalomként is ismert, létezik, és tömegek ijesztgetéssel, félelemkeltéssel történő manipulációját értik alatta. Ennek megfelelő a Scarevare módszer a kiberbűnözésben is, ijesztgetéssel, félelemkeltéssel manipulál a scareware program.
Sebezhetőség	A Sebezhetőség (Angol: *Vulnerability),* egy kiberbiztonsági kifejezés, amely egy rendszer olyan hibájára utal, amelyet biztonsági résként értelmezünk, és amelyen keresztül egy rossz szándékú személy, vagy egy rosszindulatú célból készített eszköz támadást indíthat a szóban forgó rendszer ellen. A sebezhetőség bármilyen típusú gyengeségre utalhat magában a számítógépes rendszerben, vagy az eljáráskészletben vagy bármi olyanban, amely az információbiztonságot fenyegetésnek teszi ki.

Kifejezés	Meghatározás
Sebezhetőség értékelése	A sebezhetőség értékelése egy olyan kockázatkezelési folyamat, amelyet egy adott rendszer fenyegetéseivel kapcsolatos esetleges sebezhetőségek azonosítására, számszerűsítésére és rangsorolására használnak. A sebezhetőség értékelése, mint folyamat vagy eljárás nem csak egyetlen területre értelmezhető, hanem különféle iparágakban is alkalmazható, ilyenek például: • az IT rendszerek, • az energia és egyéb közművek, • a szállítás, valamint • a kommunikációs rendszerek. A sebezhetőség értékelésének kulcsfontosságú alapeleme a *hatásvesztés-értékelés* eredményének pontos meghatározása. A hatásvesztés értéke arányos a szóban forgó rendszernek az adott fenyegetéssel szembeni sebezhetőségével. A hatásvesztés rendszerenként eltérő mértékű. Például egy légiforgalmi irányítótorony irányítási rendszerének néhány perces leállása súlyos ütközésveszélyt eredményezhet, ugyanakkor egy önkormányzati hivatal számára az ügyintézési rendszerének egy hasonló, néhány perces megakadása elhanyagolható lehet.
Sértetlenség	Az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanság) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható.
Sérülékenység	Lásd: Sebezhetőség
Sérülékenység vizsgálat	Az elektronikus információs rendszerek gyenge pontjainak (biztonsági rések) és az ezeken keresztül fenyegető biztonsági eseményeknek a feltárása.
SET (Secure Electronic Transaction) protokoll	Az e üzlet biztonságos elektronikus tranzakciói céljára, kártyakibocsátó és informatikai vállalkozások által közösen kifejlesztett kommunikációs protokoll, amelynek használata a felek közötti rejtett adatátvitelt és a felek biztonságos hitelesítését szolgálja.
Social Engineering	Social Engineering (magyarul: pszichológiai befolyásolás) az informatikai rendszerekhez (is) kötődő fogalom, annak a fajta támadásnak a meghatározását sűríti egy kifejezésbe, amikor a támadó nem technológiai sebezhetőségeket használ ki, hanem arra törekszik, hogy megtévesszen egy felhasználót. A megtévesztés eredményeként a jogosultsággal rendelkező felhasználó a jogosulatlan személy számára bizalmas adatokat ad át, vagy lehetőséget biztosít számára a saját, vagy szervezete egy vagy több rendszerébe történő belépésre, kimondottan a pszichológiai befolyásolást végző személy megtévesztő viselkedése miatt. Akik pszichológiai manipuláció útján akarnak hozzájutni információkhoz, általában az emberi természet két aspektusát igyekeznek kihasználni. • Az első: a legtöbb ember segítőkész és igyekszik segíteni azoknak, akik segítséget kérnek. • A második pedig az, hogy az emberek általában konfliktuskerülők, és inkább együttműködnek, mint nem.

Kifejezés	Meghatározás
SSL (Secure Socket Layer)	A Netscape által kifejlesztett nyílt ajánlás (szabvány) biztonságos kommunikációs csatorna létrehozására.
Számítógép biztonság	A számítógépes biztonság, másképpen a kiberbiztonság vagy még másképpen az informatikai technológia biztonsága (IT biztonság) alatt a számítógépes rendszerek védelmét értjük, a hardverek, a szoftverek vagy az elektronikusan tárolt adatok ellopásától vagy megsérülésétől, valamint az ezek által nyújtott szolgáltatások megzavarásától vagy rosszindulatú irányításától. A számítógép biztonság egyre fontosabbá válik, a felhasználók által a számítógépes rendszerek, az internet és a vezeték nélküli hálózatok (például a Bluetooth és a Wi-Fi) egyre fokozottabb használata, valamint az "intelligens" eszközök számának növekedése miatt (ebbe beleértve az okostelefonokat, a televíziókat és azon eszközöket, amelyek a Tárgyak Internetét (*IoT*) alkotják). A számítógép biztonság bonyolultsága miatt a technológiák és a politika szempontjából a számítógép biztonság (a kiberbiztonság) a mai világ egyik legnagyobb kihívása. *(*Angol: *Computer security, cybersecurity, information technology security IT security)*
Számítógépes bűnözés	Haszonszerzés vagy károkozás céljából, az informatikai rendszerekben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, illetve a rendszerelemek sértetlensége és rendelkezésre állása elleni bűncselekmények összefoglaló megnevezése. (Az informatikai eszközök felhasználásával elkövetett bűncselekményekre is szokták alkalmazni.)
Személyes adat	A személyes adat minden olyan információ, amely valamely azonosított vagy azonosítható élő személlyel kapcsolatos. Mindazon információk, amelyek összegyűjtése egy bizonyos személy azonosításához vezethet, ugyancsak személyes adatnak minősülnek. Azok az azonosításra alkalmatlanná tett, titkosított vagy álnevesített személyes adatok, amelyek felhasználhatóak egy személy újraazonosítására, személyes adatnak minősülnek, és az általános adatvédelmi rendelet hatálya alá tartoznak. Az olyan személyes adatok, amelyeket olyan módon anonimizáltak, amelynek következtében az érintett nem vagy többé nem azonosítható, nem tekinthetők többé személyes adatnak. Az adatok valódi anonimizálásához az anonimizálásnak visszafordíthatatlannak kell lennie. Példák személyes adatra • vezetéknév és utónév; • lakcím; • a vezetéknév.utónév@vállalkozás.com típusú e-mail-címek; • személyazonosító igazolvány száma; • helymeghatározó adatok (pl. mobiltelefon helymeghatározási funkciója); • IP-cím; • süti (cookie)-azonosító; • a telefon hirdetési azonosítója; • a személy egyedi azonosítását lehetővé tevő, kórház vagy orvos által tárolt adatok. Példák nem személyes adatnak minősülő adatra • cégjegyzékszám; • az info@vállalkozás.com típusú e-mail-címek; • anonimizált adatok.

Kifejezés	Meghatározás
Szimmetrikus rejtjelező eljárás	A rejtjelezésre és megoldásra egyetlen kulcsot használó rejtjelező eljárás. A megoldó algoritmus nem feltétlenül egy fordított sorrendben végrehajtott rejtjelezés!
Szoftver	Lásd: Program.
Szolgálati titok	A "titkos" minősítésű adat régi megnevezése. Lásd: Minősített adat.
Támadás	Valamilyen védett érték megszerzése, megsemmisítésére, károkozásra irányuló cselekmény. Támadás alatt nem csak a személyek, szervezetek által elkövetett támadásokat, de áttételesen a gondatlanságból, nem szándékosan kiváltott veszélyeztetéseket és a környezeti, természeti fenyegetéseket is értjük. A támadás legtöbbször nem közvetlenül éri a védett értéket, hanem a körülményektől függő támadási útvonalon zajlik le.
Tanúsítás	Egy informatikai biztonsági vizsgálat (értékelés) eredményeit igazoló formális nyilatkozat kibocsátása, melyből kiderül, hogy az értékelési követelményeket, kritériumokat megfelelően alkalmazták.(Angol: *Certification*)
Tárgyak internete	A Tárgyak (vagy Dolgok) Internete fogalom (Angol: *Internet of Things, IoT)*) azt a gondolatot írja le, hogy a mindennapi fizikai tárgyak képesek az internethez kapcsolódni, és képesek azonosítani is magukat a más eszközökkel történő kommunikáció során. A kifejezést szorosan együtt szokták emlegetni az RFID-vel mint kommunikációs módszerrel, bár a Tárgyak Internete más érzékelő, vagy vezeték nélküli technológiákat, vagy QR-kódot is tartalmazhat. A Tárgyak Internete, mint fogalom azért fontos, mert az olyan objektumokkal kapcsolatos, amely objektumok képesek digitálisan azonosítani magukat, és ez mindenképpen többet jelent, mint önmagukban az objektumok. Tehát az objektumok már nemcsak a felhasználóval képesek kommunikálni, hanem a környező objektumokhoz és adatbázis-adatokhoz is kapcsolódhatnak. Ha sok Tárgyak Internete képességgel rendelkező objektum egymással összhangban működik, akkor együttesen "Környezeti Intelligenciának" (*Ambient Intelligence*) hívják.
Teljes körű védelem	Az elektronikus információs rendszer valamennyi elemére kiterjedő védelem.
Terjesztett szolgáltatásmegtagadás	Olyan logikai támadás, amely az informatikai rendszer egy (vagy több) kiszolgálóját tömeges szolgáltatás igénnyel túlterheli, ami a felhasználók hozzáférését nehezíti, vagy akár a kiszolgáló teljes leállásához is vezethet.(Angol: *Distributed Denial of Service,* rövidítve: DDoS))
Termék	Egy informatikai hardver és/vagy szoftver, melyet funkcionálisan úgy terveztek meg, hogy alkalmas legyen a használatra, vagy rendszerbe történő beépítésre is.(Angol: *Product*)

Kifejezés	Meghatározás
Tiltakozás	Az érintett nyilatkozata, amellyel személyes adatainak kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adatok törlését kéri.
Titkosítás	A titkosítás (Angol: *encryption*) a kriptográfiának az az eljárása, amellyel az információt (nyílt szöveg) egy algoritmus (titkosító eljárás) segítségével olyan szöveggé alakítjuk, ami olvashatatlan olyan ember számára, aki nem rendelkezik az olvasáshoz szükséges speciális tudással. Ez a speciális tudás az, amit általában kulcsnak nevezünk. Az eredmény a titkosított információ (titkosított szöveg). Sok titkosító eljárás egy az egyben (vagy egyszerű átalakítással) használható a titkosított üzenet megfejtésre is, azaz, hogy a titkosított szöveget újra olvashatóvá alakítsa. A titkosítást napjainkban már a polgári rendszerekben is sokféle területen használják. Ilyen területek a különböző kommunikációs rendszerek, mint például a számítógép-hálózatok, az Internet, a mobiltelefonok stb… Bár a titkosítás meg tudja védeni az üzenet bizalmasságát, ahhoz viszont, hogy biztosítani tudjuk az üzenet sérthetetlenségét és hitelességét más technológiákra is szükség van.
Trójai faló	Olyan kártékony program, amelyet alkalmazásnak, játéknak, szolgáltatásnak, vagy más egyéb tevékenység mögé rejtenek, álcáznak. Futtatásakor fejti ki károkozó hatását.(Angol: *Trojan Horse*)
Üzemeltető	Az a természetes személy, jogi személy, jogi személyiséggel nem rendelkező szervezet, aki vagy amely az elektronikus információs rendszer vagy annak részei működtetését végzi és a működésért felelős.
Üzleti titok	A gazdasági tevékenységhez kapcsolódó minden olyan tény, információ, megoldás vagy adat, amelynek titokban maradásához a jogosultnak méltányolható érdeke fűződik, és amelynek titokban tartása érdekében a jogosult a szükséges intézkedéseket megtette.
Üzletmenet-folytonosság	Az üzletmenet-folytonosság ideális esetben azt jelenti, hogy a szervezet kritikus folyamatai zavartalanul működnek, az azokhoz szükséges erőforrások kellő mértékben rendelkezésre állnak. Ez az állapot azonban csak elméletileg létezik. A mindennapi működés során bekövetkezhetnek olyan váratlan események, amelyek veszélyeztetik a kritikus folyamatok zavartalan működését. A hardver és/vagy rendszerhibák az esetek ~ 40-55%-ában, az emberi hibák ~25-36%-ában, szoftverhibák ~10-20%-ában fordulnak elő. Ugyan a legnagyobb károkat a természeti katasztrófák okozhatják, de ezek csak az esetek 2-3%-t teszik ki. Az üzletmenet-folytonosság biztosítása a megfelelő felkészülés hiányában azt eredményezheti, hogy a felmerült problémákra adott válaszok tervezetlenek, összehangolatlanok, lassúak lehetnek, így az üzleti szolgáltatások kiesése, és ezzel együtt a bekövetkező károk mértéke is sokkal nagyobb lehet, mint amikor a szervezet felkészülése megfelelő egy bekövetkező káresemény elhárítására.
Üzletmenet-folytonosság tervezés	Az informatikai rendszer rendelkezésre állásának olyan szinten történő fenntartása, hogy a kiesésből származó károk a szervezet számára még elviselhetőek legyenek.(Angol: *Business Continuity Planning* (rövidítve: BCP))

Kifejezés	Meghatározás
Validáció	A Validáció biztosíték arra, hogy egy termék, szolgáltatás vagy rendszer megfelel az ügyfél és más azonosított érdekelt felek igényeinek. A validáció gyakran magában foglalja a külső ügyfelekkel való elfogadtatást és az általuk történő alkalmasság-igazolást. *(*Angol: *Validation), IEEE, PMBOK*
Változásmenedzsment	Az informatikai termék vagy rendszer fejlesztési, előállítási vagy karbantartási folyamatai alatt megvalósuló változásokat kezelő rendszer.(Angol: *Change management*)
Védelmi cél	Az informatikai terméktől vagy rendszertől megkövetelt védettség specifikációja, mely alapul szolgál a biztonsági vizsgálatokhoz. A védelmi cél fogja meghatározni a védelemerősítő funkciókat. Ez fogja továbbá meghatározni a védelmi célkitűzéseket, az ezen célkitűzéseket fenyegető veszélyeket, valamint bármely alkalmazásra kerülő védelmi mechanizmust.(Angol: *Security Target*)
Védelmi feladatok	• megelőzés (Angol: *prevention*) és korai figyelmeztetés (Angol: *early warning*); • észlelés (Angol: *detection*); • reagálás (Angol: *reaction*); • esemény- (Angol: *incident management*) vagy válságkezelés (Angol: *crisis management*).
Védelmi mechanizmus	Olyan logikai felépítés vagy algoritmus, amely a termékben egy adott védelemerősítő, vagy a védelem szempontjából fontosnak minősülő funkciót alkalmaz. (Angol: *Security Mechanism*)
Verifikáció	A verifikáció fogalma azt az ellenőrzést takarja, amely során ellenőrzik, hogy egy termék, egy szolgáltatás vagy egy rendszer megfelel-e a vonatkozó szabályozásoknak, követelményeknek, specifikációknak vagy előírt feltételeknek. *(*Angol*: Verification)*
Veszély	Lásd: Fenyegetés.
Virtuális magánhálózat	Olyan logikai hálózat, amelyben a nyilvános hálózat egyes végpontjai biztonságos átviteli csatornán keresztül vannak összekapcsolva, és így a nyilvános hálózaton belül védett kommunikációt valósít meg.(Angol: *Virtual Private Network* (rövidítve: VPN))
Vírus	Olyan programtörzs, amely a megfertőzött program alkalmazása során másolja, esetleg kis mértékben változtatja (mutálja) önmagát. Valamilyen beépített feltétel bekövetkezésekor többnyire romboló, néha csak figyelmeztető vagy "tréfás" hatású kódja is elindul. Többnyire komoly károkat okoznak.

Kifejezés	Meghatározás
Viselkedésalapú vírusfelismerés	Az antivírus szoftverek különböző technikákat használnak a számítógépvírusok kimutatására. Ezek egyike a viselkedésalapú malware (kártékony szoftver) felismerés. A viselkedésalapú vírusfelismerés során a védelmi szoftver nem pusztán emulálja a vizsgált programrész végrehajtását, hanem ténylegesen meg is figyeli azt, hogy a program hogyan hajtódik végre. Az ilyen típusú megközelítés megkísérli azonosítani az olyan gyanús jellegű viselkedéseket, mint például a veszélyes kódokat tartalmazó hosts fájl kicsomagolása. Vegyük észre, hogy az ilyen vizsgálatok lehetővé teszik, hogy a vírusellenőrző program korábban nem látott malware-ek jelenlétét is képes kimutatni a védett rendszerben. Mivel ez az eljárás heurisztikus, ez az eljárás önmagában nem elegendő ahhoz, hogy osztályozza a kártékony szoftvert. Azonban képes lesz jelezni egy rosszindulatú programot, amelyet aztán a védelmi szoftver gyártója vizsgálhat. A vizsgált program a vizsgálat idejére karanténba kerül, nem hajtódik végre.
Viselkedésalapú vírusvédelem	Az antivírus szoftverek különböző technikákat használnak a számítógépvírusok kimutatására. Ezek egyike a viselkedésalapú malware (kártékony szoftver) felismerés. A viselkedésalapú vírusfelismerés során a védelmi szoftver nem pusztán emulálja a vizsgált programrész végrehajtását, hanem ténylegesen meg is figyeli azt, hogy a program hogyan hajtódik végre. Az ilyen típusú megközelítésben a védelmi szoftver megkísérli azonosítani az olyan gyanús jellegű viselkedéseket, mint például a veszélyes kódokat tartalmazó hosts fájl kicsomagolása stb. Vegyük észre, hogy az ilyen vizsgálatok lehetővé teszik, hogy a vírusellenőrző program korábban nem látott malware-ek jelenlétét is képes kimutatni a védett rendszerben. Mivel ez az eljárás heurisztikus, önmagában nem elegendő ahhoz, hogy megfelelően osztályozza a kártékony szoftvert. Azonban képes lesz jelezni egy rosszindulatú programot, amelyet aztán a védelmi szoftver gyártója vizsgálhat. A vizsgált program a vizsgálat idejére karanténba kerül, nem hajtódik végre.
Warez-oldal	Olyan internetes oldal, ahonnan illegális szoftvermásolatok – az eredeti másolásvédelmet vagy regisztrációt feltörve, semlegesítve – bárki számára ingyenesen letölthetők.(Angol: *Warez-site*)
Zárt célú elektronikus információs rendszer	Jogszabályban meghatározott elkülönült nemzetbiztonsági, honvédelmi, rendészeti, igazságszolgáltatási, külügyi feladatokat ellátó elektronikus információs, informatikai vagy hírközlési rendszer.
Zsarolóvírus	A zsarolóvírus vagy zsarolóprogram a következő dolgokat hajthatja végre (ezek közül akár az összeset is): • blokkolja a számítógép működését; • megtiltja a felhasználói hozzáférést; • titkosítja a fájlokat; • és váltságdíjat követel a rendszer és az adatok visszaállításért.