

NEM OSZTÁLYOZOTT



**Budapesti Műszaki és Gazdaságtudományi Egyetem
Gazdaság- és Társadalomtudományi Kar
Információ- és Tudásmenedzsment Tanszék**

BIZTONSÁG MENEDZSMENT CSOPORT

***AZ INFORMATIKAI BIZTONSÁG FOGALMAINAK
GYŰJTEMÉNYE***

AJÁNLÁS

1.0 változat

Készítette: a Csoport

2003

A BIZTONSÁG MENEDZSMENT CSOPORT TAGJAI:

Csík Balázs	Ph.D hallgató
Dr. Danyi Pál CISA,	egyetemi docens
Egerszegi Krisztián	Ph. D. hallgató
Erdősi Péter CISA,	Ph. D. hallgató
Dr. Székely Iván	egyetemi docens
Vasvári György	tiszteleti egyetemi docens (a csoport vezetője)

LEKTORÁLTA :

Mazgon Sándor	távközlési és adatátviteli szakértő (HÍF)
---------------	---

Ez az anyag, korlátozás nélkül felhasználható, a forrás megjelölése mellett!

1. BEVEZETÉS

A meghatározások (esetleg a fordítások), amelyek első sorban az informatikai biztonságra vonatkoznak, más biztonsági környezetben (pl. vagyon-, és üzembiztonság) eltérőek is lehetnek. A szakkifejezések e gyűjteménye adatvédelmi szakkifejezéseket is tartalmaz, mivel az adatvédelem a kiinduló pontja az informatikai biztonsági követelmények meghatározásának. Munkánkat nehezítette, hogy sem a külföldi, sem a hazai szakmai gyakorlatban nem egységes a szakkifejezések értelmezése. Ennek megfelelően kérjük az Olvasót, tekintse kezdeményezésnek munkánkat. Természetesen várjuk a tanszék honlapján megtalálható (www.itm.bme.hu) Biztonság Menedzsment Csoport portálon javaslataikat, észrevételeiket, illetve esetleges ellen véleményüket is.

Biztonságmenedzsment Csoport

2. A

ADAT (data)

- Az adat tények, elképzelések, utasítások emberi vagy technikai eszközökkel történő formalizált ábrázolása ismertetés, feldolgozás, illetve távközlés céljára.

ADAT MEGHAJTOTTA TÁMADÁS (data driven attack)

- Támadás, amely rejtett vagy tömörített adatokat tűzfalon felfedés nélkül juttat keresztül,

ADATVÉDELEM (data protection)

- A személyes adatok gyűjtésének, feldolgozásának és felhasználásának korlátozása, beleértve a védelmet nyújtó alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összességét. (ugyanaz vonatkozik, a hatályos jogszabályok szerint az üzleti titkot, banktitkot, értékpapírtitkot, biztosítási titkot képező, illetve minden személyre vonatkozó, vonatkoztatható adatra is).

ADATBIZTONSÁG (data security)

- Az adatbiztonság az adatok védelme a jogosulatlan hozzáférés, a módosítás, és a törlés, illetve a megsemmisítés ellen. Azaz az adatok bizalmasságának, rendelkezésre állásának, és sértetlenségének védelme/védettsége.

ALKALMAZÁSI KAPÚ (application gateway)

- Átjáró, amely a külső világ, és a belső hálózat között megszüri az információ folyamatot.

ALKALMAZÓI RENDSZER (application system)

- Programok, és manuális folyamatok összessége, amelyek üzleti funkciót hajtanak végre.

ALTERNATÍV FORGALOMIRÁNYÍTÁS (alternate routing)

- Több útvonal használata ugyanazon két pont között.

ÁTVILÁGÍTHATÓSÁG (auditability)

- Annak megállapíthatósága, hogy a rendszernek megvannak a kívánt funkciói és azok rendeltetésszerűen használhatók.

AZONOSÍTÁS (identification, ID)

- Egy személy (vagy más entitás) állított azonosságának megállapítása (pl. belépésekor).

ÁTJÁRÓ (gateway)

- Egy hálózati processzor, amely adat csomagokat irányít két, vagy több kapcsolt hálózat között.

3. B

BEHATOLÁS (intrusion)

- Védett rendszerbe jogosulatlan belépés a védelem megkerülésével.

BEJELENTKEZÉS (log in)

- A belépés kezdeményezése jelszóval védett rendszerbe.

BEJELENTKEZÉS MEGSZAKÍTÁS (time out)

- A hitelesítés alapján (ID, PW) engedélyezett felhasználói interaktív viszony bontása, meghatározott inaktivitási idő után.

BEKÖVETKEZÉSI VALÓSZÍNŰSÉG (probability)

- Az esélye annak, hogy egy esemény (incidens), például a veszélyforrás képezte fenyegetettség, támadás formájában bekövetkezzon.

BELÉPTETÉS TÁROLÓ (account).

- A felhasználói azonosítókat, jelszavakat, jogosultságokat tartalmazó tároló, amely a számon kérhetőséget is ellátja (audit log).

BÉRELT VONAL (leased line)

- Bérelt vonal, amelyet a felhasználó alkalmaz távközlésre meghatározott végpontok között.

BEHÍVÁS AZ INTERNETBE (dial up Internet connection),

- Lehetővé teszi egy telefonszám felhívását, ahonnan az Internet elérhető.

BIZALMAS CSATORNA (trusted channel)

- Eszköz, amelynek segítségével két biztonsági funkció megfelelő bizalmassággal tud egymással direkt kommunikálni.

BIZALMAS SZÁMÍTÁSTECHNIKAI BÁZIS (Trusted Computing Base)

- Hw és sw elemek együttese, amely kikényszeríti egy szervezet informatikai hozzáférés-védelmé biztonsági politikájának megvalósulását.

BIZALMAS ÚTVONAL (trusted path)

- A bizalmas útvonal az az eszköz, amelynek segítségével felhasználók, és rendszerek megfelelő bizalmassággal tudnak kommunikálni egymással.

BIZALMASSÁG (confidentiality)

- Gondoskodás arról, hogy az információhoz csak az férhessen hozzá, akit erre feljogosítottak.

BIZTONSÁG (security)

- A biztonság olyan kedvező állapot, amelynek megváltozása nem valószínű, de nem is zárható ki (az erőforrások bizalmasságának, sértetlenségének, és rendelkezésre állásának fenyegetettsége minimális). A biztonság összetevői: szervezési biztonság (adminisztratív, humán biztonság), technikai biztonság (fizikai, logikai, hálózati, életciklus biztonság).

BIZTONSÁGI ADMINISZTRÁTOR (authorised administrator)

- Humán felhasználó, aki jogosult olyan adminisztratív műveletek végrehajtására, amelyek kikényszerítik a biztonsági politikát.

BIZTONSÁGI CÉLOK (security objectives)

- Bizalmasság, ② Sértetlenség, ③ Rendelkezésre állás, ④ Számon kérhetőség, ⑤ Garanciák.

BIZTONSÁGI TUDATOSSÁG (security awaranness)

- A veszélyforrások felismerése, a védelmi intézkedések szükségességének elfogadása, és rendeltetésszerű végrehatására való törekvés.

BIZONYÍTÉK (evidence)

- Jogosulatlan, rosszindulatú tevékenységet, biztonsági eseményt alátámasztó elektronikus dokumentum.

BIZTONSÁGI ESEMÉNY (security incident)

- Minden olyan esemény, amely a biztonságra nézve fenyegetést jelent vagy jelenthet.

BIZTONSÁGI KÖRNYEZET (security enviroment)

- A biztonsági környezet a jogszabályok, a gazdasági szervezet belső szabályai, és elvárásai, szokások, szakértelem és tudás, amelyek meghatározzák azt a környezetet, amelyben az erőforrásokat a gazdasági szervezet használni akarja.

BÖNGÉSZŐ SW (browser software),

- SW, amely lehetővé teszi a világhálón a felhasználó számára hozzáférhető információ és erőforrások igénybe vételét, illetve a barangolást.

4. C

CSALÁS ÉSZLELÉS (fraud detection)

- + Annak a szándékos és eltitkolt, illegális tevékenységnek az észlelése/érzékelése, amelybe beleértendő az illegális haszon lehívása is.

CSATORNA (channel)

- * Adatátviteli út egymástól távoli készülékek között.

CSOMAG (packet)

- * A csomag a hálózati réteg adatátviteli egysége.

5. D

DEMILITARIZALT ZÓNA/övezet (demilitarized zone, DMZ)

- Két tűzfal közötti terület egy vállalati hálózat, és az Internet között.

DIGITÁLIS ALÁÍRÁS (digital signature)

- A digitális aláírás, az aszimmetrikus elektronikus aláírás, amely az üzenet, az elektronikus okirat tartalma, és a küldő hitelesítésére szolgál.

DOMAIN NÉV (domain name)

- Egy cím vagy egy név, amely azonosít egy Internet helyet.

6. E

EGYENSZILÁRDSÁG (homogeneity)

- A biztonság a vállalatot, illetve az üzleti tevékenységet teljesen átfogja, és annak minden pontján legalább azonos erősségű (pl. nem kerülhető meg, lásd a meg nem kerülhetőség fogalmát is).

ELEKTRONIKUS HITELESÍTÉS (electronic authentication)

- Az állított azonosság megerősítése.

ELEKTRONIKUS ALÁÍRÁS (electronic signature)

- Elektronikus adatok, amelyek az adatok hitelesítésére szolgálnak, és amelyeket egyéb elektronikus adatokhoz csatolnak (gyűjtőfogalom).

ELLENŐRZÉSI NYOM (audit trail)

- ① Az **audit trail** a fájlon, eszközön vagy rendszeren végrehajtott tevékenységek rögzítésére szolgál, amelynek alapján az illegális tevékenységek fel lehet tártni, és jelenteni. ② Ugyanakkor az **audit log** az **accountokkal** beléptetett (ID, pw) személyek, és támadók által végrehajtott tevékenységek ID alapú naplója.

ELLENŐRZŐ SZÁM (checksum)

- Az a numerikus érték, amelyet az ellenőrzés tárgyából számítottak ki, és azért csatoltak hozzá, hogy lehetővé tegye annak az ellenőrizhetőségét, hogy a szám nem hibás, nem változtatták meg.

EGYÍRÁNYÚ KIVONATOLÁS (one way hash)

- Egy üzenet kivonat készítésére alkalmas algoritmus, amely gyakorlatilag alkalmatlan az eredeti üzenet visszaállítására, és az üzeneteket meghatározott hosszúságú kivonatban állítja elő.

ELREJTÉSI RENDSZER (concealment system)

- A bizalmasság elérése úgy, hogy érzékeny információkba elrejtjenek nem oda tartozó információkat.

EMBER (people)

- Az üzleti rendszer, illetve az információ-rendszer kiszolgálására, tudatos, és produktív tervezésére, szervezésére, beszerzésére, szállítására, támogatására, és követésére szolgáló személyzet.

E-mail (e-mail)

- Elektronikus levél küldése, és fogadása az interneten.

ERŐFORRÁS (resource)

- A gazdasági szervezet vezetősége (menedzserei) által az üzleti, illetve informatikai feladatok végrehajtásához rendelt emberek, eszközök. ① *Az informatikai erőforrások:* adat, alkalmazás, technológia (hw, rsw), kisegítő eszközök (klíma, energia ellátás stb.), ember. ② *Az üzleti erőforrások:* adat, tőke, értékek, áruk, technológia (ügyvitel technikai eszközök, személy, és teherszállító eszközök), üzleti folyamatok, illetve eljárások, kisegítő berendezések (épület, áramellátás, klíma stb.).

ENTITÁS (entity)

- Az entity, valami függetlenül létező. Az információ-rendszerben szubjektum, objektum vagy tevékenység.

ÉRTÉKRENDSZER (ÉR, value system)

- Az üzleti rendszer, és a termelési (szolgáltatási) rendszerből áll, és nem része az információ-rendszer.

ÉRZÉKENY INFORMÁCIÓ (sensitive information)

- Az az információ (amelyet egy kompetens személy határoz meg), és amelyet védeni kell a felfedéstől, megváltoztatástól, és törléstől.

EXTRANET (extranet)

- Az intranet kiterjesztése az INTERNETEN keresztül a távoli felhasználók felé.

7. F

FEJRÉS (header)

- Egy e-mail üzenet része, amely meghatározza a küldőt, a fogadót, az üzenet tárgyát.

FELADATSZÉTVÁLASZTÁS (segregation of duties)

- A biztonságkritikus munkakörök szétválasztása.

FELHASZNÁLÓ (user)

- Humán vagy gépi entitás (a hozzáférés-védelmi rendszeren kívül, amely a hf.v.-i rendszerrel kölcsönösen együtt tud működni, és nincs speciális jogosultsága a Biztonsági Politika kikényszerítésére).

FELHASZNÁLÓ HITELESÍTÉS (user authentication)

- A felhasználó hitelességének ellenőrzése (pl. a belépéskor minden felhasználó ellenőrzése). PW alkalmazás.

FENYEGETÉS (threat)

- A fenyegetés a támadás lehetősége, vagy a biztonság megsértésének lehetősége, a támadás tárgyát képező erőforrásra.

FENYEGETETTSÉG (threatness)

- Olyan állapot, amelyben az erőforrások felfedésre, módosításra vagy elpusztításra kerülhetnek.

FILE ÁTVITELI PROTOKOLL (FTP, File Transfer Protocol)

- Egy protokoll, amely lehetővé teszi az INTERNETEN keresztül egymással kommunikáló számítógépek között állományok (fájlok) átvitelét.

FIZIKAI BIZTONSÁG (physical security)

- A fizikai biztonság az erőforrások bizalmassága és sértetlensége, valamint rendelkezésre állása sérelmére bekövetkező szándékos vagy véletlen fizikai támadásokkal szembeni védelem.

FOLYAMATOSSÁG (continuity)

- Az üzleti tevékenység zavarmentes rendelkezésre állása.

8. G

GARANCIA, biztosíték (assurance)

- A bizalom abban, hogy a négy másik biztonsági célt (bizalmasság, sértetlenség, rendelkezésre állás, számon kérhetőség) a biztonsági alrendszer megfelelően ellátja/eléri.

GARANCIÁLIS KÖVETELMÉNY (assurance requirement)

- Lásd a garancia fogalom értelmezését.

GOPHER (gopher)

- Menü bázisú rendszer az Internet erőforrások feltárására.

GYAKRAN IDÉZETT KÉRDÉSEK (GYÍK, FAQ, frequently asked questions)

- Gyakran feltett kérdések, amelyeket a felhasználó olvashat mielőtt használni kezd egy programot.

9. H

HÁLÓZATI ÖSSZEFÜGGŐSÉG (interconnectivity)

- Eszközök közötti együttműködés lehetősége, amit azonos kommunikációs szabványok alapján lehet kihasználni.

HÁTTÉR (back up)

- Adat, berendezés, vagy folyamat, amely hiba, illetve rendszer kiesés esetén rendelkezésre áll.

HÁTTÉR AJTÓ (back door, trap door)

- Egy rejtett program, amelyet a behatoló a háttérben hagyva, lehetővé teszi később a bejutást, vagy adatok kijuttatását rosszindulatú programokhoz. Csapóajtó.

HIBÁS ADATOK (corrupt data)

- Adatok, amelyeket valamely program nem tud olvasni, vagy használni.

HELYREÁLLÍTÁS (restoration)

- A KATASZTRÓFA következtében megsérült erőforrások EREDETI állapotának újra előállítása, általában az eredeti helyen.

HÍD (bridge)

- Az adatkapcsolati szinten (data link level) működő készülék, amely összekapcsol két hasonló hálózatot

HITELESSÉG (authenticity)

- Valaminek a forrása az, amit megjelöltek, és a tartalma az eredeti.

HORDOZHATÓSÁG (portability)

- Különböző számítógépeken minimális változtatás nélkül futtatható program.

HOZZÁFÉRÉS (access)

- Az erőforrások felhasználásának lehetősége.

HOZZÁFÉRÉS-VÉDELEM (HFV, access control)

- **Tetszőleges hozzáférés-védelem. (Discretionary Access Control, DAC):** Tetszőleges hozzáférés egy objektumhoz, a szubjektum és/vagy csoport azonosítása alapján. A védelem tetszőleges abban az értelemben, hogy egy szubjektum egy hozzáférési engedélyt, a need to know elvet alkalmazva, más szubjektumnak továbbadhatja.
- **Szerepen alapuló hozzáférés-védelem. (Role Based Access Control, RBAC):** A hozzáférés a szubjektumokhoz a feladat szétválasztás, a szükséges tudás – szükséges tevékenység - elve alapján hozzárendelt szerepek, és az objektumokhoz rendelt szerepek (tevékenységek) alapján történhet. A szubjektum az objektumon a szerepek egyezősége esetén fejthet ki aktivitást. A szerepeket a biztonsági adminisztrátor határozza meg.
- **Kötelező hozzáférés-védelem (Mandatory access control).** A szubjektumokhoz, és az objektumokhoz egy címke (jelző) rendelése, azok titokvédelmi osztályozása szerint. A hozzáférés akkor engedélyezhető, ha a szubjektum titokvédelmi osztályozása uralkodik az objektum titokvédelmi osztályozása felett.

HTML (Hypertext Markup Language)

- A www-en használatos programozási nyelv.

HTTP (HyperText Transfer Protocol)

- Fileok mozgatására szolgáló szabvány.

http://

- Az Internet szabványos átviteli protokollja. Minden interakció egy ASCII kérésből és egy RFC822 MIME-szerű válaszból áll.

HUMÁNBIZTONSÁG (human security)

- Az erőforrások bizalmasságának sérelmére — a vállalattal munkaviszonyban álló vagy a vállalatnál bármely szerződés alapján tevékenységet folytató vagy külső személyek által — elkövethető szándékos vagy véletlen humántámadások elleni védelem.

10. I

IDŐBÉLYEGZÉS (time stamping)

- Amikor egy üzenetbe beírják a keletkezésének, vagy az érvényességi idejének az időpontját.

INFORMÁCIÓ (information)

- A konvencionálisan, ugyanúgy értelmezik, mint az adatokat (lásd BS 7799).

INFORMÁCIÓ RENDSZER, IR (information system)

- Az adatok összegyűjtésére, tárolására, feldolgozására, és továbbítására szolgáló rendszer.

INFORMATIKAI BIZTONSÁG (information security)

- Az informatikai biztonság, az informatikai erőforrások bizalmasságának, sértetlenségének, és rendelkezésre állásának minimális fenyegetettsége.

INTERNET (Internet)

- A hálózatok világ hálózata, amely több millió összekötött címet jelent.

INTRANET (INTRANET)

- Az Internet protokollt használó belső hálózat. Egy telephelyen, épületen, vagy lakáson belül.

IP INTERNET PROTOKOLL (INTERNET PROTOCOL)

- Csomagkapcsolt átvitelt megvalósító hálózati réteg protokoll.

IP BIZTONSÁGOS (IP SEC)

- Az IP biztonságos verziója, csomag szinten hitelesítést, és rejtjelezést végez.

IP ÖSSZEKÖTÉS (IP splicing)

- Támadás, amikor egy viszonyban lehetővé teszik egy jogosult felhasználó megszemélyesítését.

ISMÉTELT TÁMADÁS (replay attacks)

- Érvényes csomagok másolása vagy hamisítása, és küldése sorozatosan egy címre.

IT IRÁNYÍTÁS (IT governance)

- A vállalatot irányító, és ellenőrző összefüggések, és folyamatok struktúrája, annak érdekében, hogy a vállalatok érték hozzáadással elérhessék céljaikat, mérlegelve a kockázatot az IT, és folyamatai használatával szemben.

11. J

JELSZÓ (password, pw)

- Védett karakter fűzér, amely a felhasználót, a belépni szándékozót azonosítja.

JELLEMZŐ (attribute)

- A szubjektumhoz és/vagy az objektumhoz rendelt információ, amelyet a biztonság kikényszerítéséhez használnak.)

JOGOSULTSÁG (authorisation)

- A lehetőség megadása tevékenység végrehajtására.

JOGOSULTSÁGGAL RENDELKEZŐ FELHASZNÁLÓ (authorised user)

- Egy olyan felhasználó, aki jogosult egy tevékenység végrehajtására.

12. K**KAPCSOLAT ELTÉRÍTÉS (connection hijacking)**

- Csomag(-ok) bejuttatása feljogosított viszonyba, amely állandóan működik, és hitelesítve van.

KÁRTYA KIBOCSÁTÓ BANK (issuer bank)

- A vásárló bankkártyáját kibocsátó bank az elektronikus kereskedelemben.

KATASZTRÓFA (disaster)

- ① A katasztrófa a vállalat üzleti tevékenysége folyamatos és rendeltetésszerű működésének megszakadása. ② Az **INFORMATIKAI KATASZTRÓFA** az üzleti folyamatokat kiszolgáló információ-rendszer kiesése, az informatikai szolgáltatások megszakadása.

KATASZTRÓFA TERV (disaster recovery plan)

- Egy katasztrófa bekövetkezése esetén keletkező vagyoni, és nem vagyoni kárkövetkezmények elhárítására készített intézkedési terv, amelyet hívnak ① üzletmenet folytonossági tervnek (**BUSINESS CONTINUITY PLAN**) is, míg korábban ② disaster recovery, vagy ③ contingency planként is hívták.

KATASZTRÓFA TERV MENEDZSMENT (Disaster recovery plan management)

- Az a tevékenység sorozat, amelyet a katasztrófaterv végrehajtásának irányítására, szervezésére, ellenőrzésére végeznek.

KERESKEDŐ BANKJA (acquirer bank)

- Az elektronikus kereskedelemben a kereskedő bankja.

KIHÍVÁS/VÁLASZ (challenge / response)

- A hitelesítés egy módszere, amikor egy készülék meghatározott úton kihívást intéz egy másik készülékhez, amely a kihívásból képzett jelszóval bizonyítja a hitelességét (pl. egyszer használatos jelszóval).

KISEGÍTŐ BEREDEZÉSEK (facilities)

- Az erőforrások elhelyezésére, és kiszolgálására szolgáló eszközök berendezések.

KIBER TÉR (cyberspace)

- Minden az interneten, a hálózat, a programok, az erőforrások, ami elektronikusan hozzáférhető és igénybe vehető.

KIBOCSÁJTÓ BANK (issuer bank)

- Az elektronikus kereskedelemben a bank, amely kibocsájtotta a vásárló bankkártyáját.

KIESÉSI IDŐ (down time)

- Az információ-rendszer leállításától a háttéren történő újraindításig eltelő idő.

KOCKÁZAT (risk)

- A kockázat annak a lehetőségnek a valószínűsége, hogy egy fenyegetés támadás útján kárkövetkezményeket okoz.

KOCKÁZAT ELEMZÉS (risk analysis)

- A kockázat azonosításának, és a lehetséges kárkövetkezmény felbecsülésének módszere.

KOCKÁZATKEZELÉS (risk management)

- A biztonsági kockázatoknak az azonosítása, elfogadható költségen a minimalizálása, és az ellenőrzése.

KOMPROMITTÁL (compromise)

- A Biztonsági Politika megsértése egy rendszerben, az érzékeny információk felfedésével.

KÖRNYEZETI BIZTONSÁG (natural security)

- Az erőforrások rendelkezésre állásának és sértetlenségének a természeti katasztrófákkal szembeni védettsége.

KÖZÖS FELADATVÉGREHAJTÁS (interoperability)

- Eszközök (sw-ek) közös feladat végrehajtási képessége.

KULCS LETÉTI RENDSZER (key escrow)

- A titkos kulcs másolatát őrző rendszer, vészhelyzetre, vagy jogosult szerv lekérésére.

KÜLDETÉS-KRITIKUS ALKALMAZÁS (mission-critical applicatrion)

- Alkalmazás, amely alapvető a vállalat üzleti tevékenységéhez.

KIVONATOLÁS (hashing)

- Algoritmus, amellyel egy üzenet kivonat állítható elő (pl. digitális aláírás készítéséhez).

13. L

LEFOJTÁS (flaming)

- Egy Internet cím lezárása üzenetekkel való bombázással.

LEGKEVESEBB JOGOSULTSÁG (least privilege)

- Rendszer, amely a kockázatok csökkentésére a legkevesebb jogosultsággal működik.

LETÖLTÉS (download)

- A letöltés egy file átvitele egy számítógépről a felhasználó számítógépére.

LEMEZ TÜKRÖZÉS (disk mirroring)

- Egy lemezművelet (írás) két háttértárolóra történő szimultán elvégzése.

LEHALLGATÁS (wire tapping)

- A távközlési hálózaton átvitt információk jogosulatlan lehallgatása.

LETAGADHATATLANSÁG (non repudiation)

- Annak a biztosítéka, hogy az üzenetek eredete a későbbiekben egyik fél részéről sem tagadható le.

LOGIKAI BIZTONSÁG (logical security)

- Az információ-rendszer adatainak és programjainak bizalmassága és sértetlensége, valamint rendelkezésre állása sérelmére technológiai eszközökkel bekövetkező szándékos vagy véletlen, támadásokkal szembeni védettség.

LOGIKAI BOMBA (logic bomb)

- Egy szoftver kód, amelyet elhelyeznek egy rendszerben, és meghatározott feltétel mellett lép működésbe.

14. M

MARADVÁNYKOCKÁZAT (residual risk)

- Az a kockázat, amely a védelmi intézkedés megtétele után marad fenn.

MÁS JOGOSULTSÁGÁNAK FELHASZNÁLÁSA (piggybacking)

- Jogosulatlan hozzáférés, más jogosultságának felhasználásával.

MEGHIBÁSODÁS VÉDETT (fail safe)

- A fellépő hw, vagy sw hibáktól automatikusan védett program és/vagy folyamat.

MEGKERÜLÉS (penetration)

- Egy rendszer biztonsági alrendszerének (védelmi intézkedéseinek) sikeres megkerülése, támadási (behatolási) céllal.

MEG NEM KERÜLHETŐSÉG (non circumventability),

- Annak biztosítása, hogy a védelmi intézkedések kikényszerítik a védelmi követelményeket, s így nem válik lehetővé a biztonság megsértése.

MEGSZAKADÁS NÉLKÜLI ÁRAM ELLÁTÁS (uninterruptible power supply)

- Háttér berendezés, amely az áramellátást biztosítja, annak megszakadása, vagy zavarai esetén.

MEGSZEMÉLYESÍTÉS (personalisation)

- Folyamat, amikor az IC kártyába betöltik a felhasználó adatait.

15. N

NETIQUETT (NETIQUETT)

- Az Internet felhasználókat irányító magatartási szabályok.

NYILVÁNOS KULCSÚ INFRASTRÚKTÚRA (public key infrastructure. PKI)

- Egy rendszer, amely a nyilvános kulcsok tanúsítását készíti, és azokat szétosztja.

NAPLÓ (log)

- Események, tevékenységek rögzítésére szolgáló papír alapú vagy elektronikus dokumentum.

16. O

OBJEKTUM (object)

- Az objektum (pl. file, program, printer) tartalmaz vagy kap információt (passzív).

OBJEKTUM ÚJRA FELHASZNÁLÁS (object reuse)

- Egy vagy több objektum (file, diszk szektor, mágnes szalag) újra kijelölése-érzékenységi szempontból - egy szubjektum részéről, annak újra allokálása előtt.

ŐRZÉS (guard)

- Különböző biztonsági szintű rendszerek működés közbeni szűrése, szétválasztása, illetve a felhasználó termináljának leválasztása az adatbázisban azoktól az adatoktól, amelyek hozzáférése nem jogosult.

OSZTÁLYOZÁS (classification)

- Adatok, alkalmazások, helyiségek, eszközök biztonságkritikusságuk függvényében történő biztonsági osztályokba sorolása (adatoknál az állam, és szolgálati titok esetében minősítés).

17. P

PROTOKOLL (PROTOCOL)

- Két számítógép közötti kommunikáció szabályai.

PROXY (proxy)

- Tűzfalon futó alkalmazás változat, amely a felhasználó felé Internet szerverként, az Internet felé kliensként mutatkozik.

18. R

REGISZTRÁCIÓS SZOLGÁLTATÓ (registration authority)

- Egy bizalmas harmadik fél, amely egy tanúsítás szolgáltató számára ellenőrzi a kapcsolatot a felhasználó, és a nyilvános kulcsa között.

REJTJELEZÉS (encryption)

- Egy eljárás, amely az adatokat kódolva, azokat a jogosulatlan olvasó számára értelmezhetetlenné teszi.

REJTETT CSATORNA (covert channel)

- Lehetővé teszi olyan adatok közlését, amelyek megsértik a biztonsági politikát (rosszindulatú adatok).

RENDELKEZÉSRE ÁLLÁS (availability)

- A rendszer olyan állapota, amelyben eredeti rendeltetésének megfelelő szolgáltatásokat tud nyújtani (funkcionalitás) meghatározott helyen és időben (elérhetőség).

RENDSZER (system)

- Az egymással valamilyen módon meghatározható kapcsolatban álló elemek összessége.

RENDSZERSZERVEZÉS (organisation of system)

- A gazdasági szervezetben végbemenő folyamatok, valamint irányításuk és ellenőrzésük szervezése.

RÉSZLEGES KOCKÁZAT (partial risk) - ÁTFOGÓ KOCKÁZAT (global risk)

- ① A *részleges kockázat*, amely egy erőforrást vagy az erőforrások egy részét fenyegető támadások esetleges bekövetkezése miatt áll fenn, míg ② az *átfogó kockázat* a teljes rendszert fenyegető támadás esetleges bekövetkezése miatt fennálló kockázat.

19. S

SCANNER

- Hálózati csomópont nyitott kapuit feltáró segédprogram (port-scanner).

SEBEZHETŐSÉG (vulnerability)

- A veszélyforrás képezte sikeres támadás bekövetkezése esetén az erőforrások sérülésének lehetősége.

SEBEZHETŐSÉGI ABLAK (window of vulnerability)

- Az az időtartam, amelyet a katasztrófa bekövetkezésétől számítva az üzleti tevékenység megszakadása nélkül képes a vállalat elviselni.

SÉRTETLENSÉG (integrity)

- Valami az eredeti állapotának megfelel, teljes, avagy az információ és feldolgozásmódja pontosságának és teljességének a megóvása.

SNIFFER

- A hálózati csomópontot elérő teljes hálózati forgalom megjelenítésére alkalmas segédprogram (utility). Alapértelmezésben a hálózati csomópont csak a saját címére érkező adatokat dolgozza fel.

SZABAD SZOFTVER (Freeware)

- Szabadon letölthető és korlátozások nélkül használható szoftver.

SZÁMÍTÓGÉPES VISSZAÉLÉS (computer abuse)

- Az informatikai erőforrások jogosulatlan felhasználása, megváltoztatása, megzavarása vagy rombolása.

SZÁMONKÉRHEŐSÉG (accountability)

- Az a tulajdonság, hogy a rendszerben végrehajtott tevékenységek ellenőrzés céljára rögzítésre kerülnek azért, hogy visszakövethetők legyenek, bizonyíték álljon rendelkezésre.

SZEMÉLY AZONOSÍTÓ SZÁM (personal identification number, PIN)

- A személyt azonosító szám hitelesítés céljára.

SENNYEZETTSÉG (contamination)

- A különböző érzékenyséű (különbözö biztonsi osztályba sorolt) adatok összekeverése, amelynek következtében az érzékenyebb adatok nem kapják meg a szükséges védelmi szintet.

SZEREP (role)

- A szerep a felhasználó részéről végrehajtható műveletek sorozata, amely tevékenységeket, információ-folyamokat, és hozzárendelt adatokat foglal magában.

SZOLGÁLTATÁS MEGSZAKÍTÁSI TÁMADÁS (denial of service attack)

- Egy támadás, amely üzenetekkel áraszt el egy rendszert, hibás működést okozva, vagy időlegesen leállítva annak működését.

SZUBJEKTUM (subject)

- A szubjektum egy személy vagy egy folyamat, amely az objektumok között információ-folyamot indít vagy a rendszernek az állapotát változtatja meg, azaz az objektumon műveletet végezhet (aktív).

SZÜKSÉGES TUDÁS ELVE (need to know)

- Az érzékeny információ tulajdonosa részéről az információk elérésére, birtoklására, és azokon tevékenység végrehajtására vonatkozó jogosultságok meghatározása egy felhasználó részére, annak a munkaköri kötelezettségei függvényében.

20. T

TÁMADÁS (attack)

- A támadás egy az erőforrások bizalmassága, sértetlensége és/vagy rendelkezésre állása ellen, egy veszélyforrásból kiinduló folyamat.

TANÚSÍTVÁNY (certificate)

- A tanúsítványszolgáltató által kiállított dokumentum, amely tanúsítja, hogy egy nyilvános kulcs azé, akit állítanak róla.

TANÚSÍTVÁNY SZOLGÁLTATÓ (Certificate Authority)

- Egy bizalmas harmadik fél, amely tanúsítványt szolgáltat az üzenet fogadó számára aláírás hitelesítés céljára arról, hogy egy nyilvános kulcs azé, akit állítanak róla.

TCP (Transmission Control Protocol)

- A TCP/IP protokoll-párnak a szállítási réteget vezérlő protokollja, mely megbízható összeköttetés-alapon bonyolít hibamentes sokbájtos csomagtovábbítást, bármely két hálózati csomópont között.

TCP/IP (Transmission Control Protocol/Internet Protocol),

- Hivatkozási modell, mely rugalmas (flexibilis) és hibátűrő átvitelt tesz lehetővé a forrás- és célállomások között még akkor is, ha a két csomópont közötti eszközök bármelyike meghibásodik.

TELJES KIPROBALÁS (brute force attack)

- A rejtjelfejtés egy módszere, amikor minden lehetséges kulcsot kipróbálnak.

TELNET (TELNET)

- Az az Internet alkalmazás, amely lehetővé teszi, hogy a felhasználók elérjenek számítógépeket, illetve azokon tárolt adatokat.

TECHNOLÓGIA (technology)

- ① ÉR: az üzleti cél megvalósítására szolgáló eszközök.
② IR: a hw, és a rendszer szoftver(-ek).

TERMELÉSI FOLYAMAT (production process)

- A termelési cél érdekében végrehajtott tevékenységek láncolata.

TISZTOGATÁS (purge)

- A visszavonása az információknak egy tárolóból, vagy egy perifériából a feldolgozás befejezése után.

TITOKTARTÁSI NYILATKOZAT (NON DISCLOSURE AGREEMENT, CONFIDENTIALITY AGREEMENT)

- Megállapodás, amelyet felhasználókkal, tanácsadókkal, szállítókkal kötnek, a titkok fel nem fedésére.

TITOKVÉDELEM (secret protection)

- A titokvédelem az adatvédelem körébe tartozó, és egyéb adatok, és más biztonság kritikus erőforrások (alkalmazások, helyiségek, eszközök) bizalmasságának, sértetlenségének, és rendelkezésre állásának a védelme.

TRÓJAI FALÓ (Trojan horse)

- Szoftveres támadási forma, amely elrejtí eredeti célját, és a rendszerbe kerülése után nem kívánatos (jogosulatlan) tevékenységet hajt végre.

TULAJDONOS (owner)

- Egy menedzser (manager) vagy rendszergazda, aki egy meghatározott adatállományért, illetve alkalmazói rendszerért felelős.

TUNNELING

- A rejtjelezés gyakorlata két pont között.

TŰZFAL (firewall)

- A tűzfal egy számítástechnikai eszköz, amely fizikailag, és logikailag elválaszt egy hálózatot egy másiktól [① lehet forgalomszűrő (Traffic Filter Firewall **TFF**) a hálózati és transzport rétegben vagy ② alkalmazásszintű az alkalmazási rétegben (Application Level Firewall **ALF**)].

21. Ü

ÜZENETHITELESÍTŐ KÓD (message authentication code, MAC)

- Szimmetrikus kriptográfiai algoritmust alkalmazó elektronikus aláírás, amikor az üzenet ellenőrző összegét (MAC) vagy az üzenet kivonatát (hashed MAC) rejtjelezzik, azaz egy kriptográfiai ellenőrző összeget képeznek, és azt csatolják hitelesítés céljából az aláírandó adatokhoz.

ÜZEMBIZTONSÁG (safety of operation)

- A biztonság a termelési (szolgáltatási) rendszerben, amikor is a termelési rendszer erőforrásainak bizalmassága, sértetlensége, és rendelkezésre állása fenyegetettsége minimális.

ÜZLETI KÖVETELMÉNYEK (business requirements)

- ① Minőség, ② Megbízhatóság, ③ Biztonság.

ÜZLETI FOLYAMAT (business process)

- Az üzleti cél érdekében végrehajtott tevékenységek láncolata.

ÜZLETI RENDSZER, ÜR (business system)

- Az üzleti rendszer az üzleti folyamatokból áll, és kétirányú kapcsolata van a termelési (ha van), és az információrendszerrel.

ÜZLETMENET FOLYTONOSSÁG MENEDZSMENT (BUSINESS CONTINUITY MANAGEMENT)

- A katasztrófa bekövetkezése esetén az üzletmenet folytonosság tervszerű visszaállítása, majd az eredeti konfiguráció helyreállítása.

22. V

VAGYONBIZTONSÁG (property security)

- A gazdasági szervezet olyan állapota, amelyben az Üzleti rendszer erőforrásainak rendelkezésre állása, bizalmassága és sértetlenségének a fenyegetettsége gyakorlatilag minimális.

VÉDELMI INTÉZKEDÉS (protective measure, control)

- ① Védelmi intézkedés a fenyegetettség bekövetkezési valószínűsége, illetve a bekövetkezéskor jelentkező kár csökkentésére szervezési vagy technikai eszközökkel alkalmazott intézkedés. ② Egyes szabványok magyar fordításában óvintézkedés.

VESZÉLYFORRÁS (exposure)

- A veszélyforrás mindaz, aminek bekövetkezésekor (egy fenyegetést megvalósító támadás eredményeképpen) a rendszer működésében nem kívánt állapot jön létre, az erőforrások biztonsága sérül.

VÉGPONTTÓL VÉGPONTIG REJTJELEZÉS (end-to-end encryption)

- Az indulási ponttól, a végpontig történő rejtjelezés.

VISSZAÁLLÍTÁS (recovery)

- A szolgáltatások (ÉR,IR), az eredeti rendszer kiesése esetén, háttérből történő újraindítása.

TARTALOMJEGYZÉK

1.	BEVEZETÉS	3
2.	A.....	3
3.	B.....	4
4.	C.....	5
5.	D.....	5
6.	E.....	6
7.	F.....	7
8.	G	7
9.	H.....	8
10.	I.....	9
11.	J.....	9
12.	K.....	10
13.	L.....	11
14.	M.....	12
15.	N.....	12
16.	O.....	12
17.	P.....	13
18.	R.....	13
19.	S	13
20.	T.....	14
21.	Ü.....	16
22.	V.....	16