2025.02.17

Információ biztonság: bármilyen információ biztonásga (papír alapú pl), írás-olvasás védése, elérhetőség

Kiberbiztonság: ^ digitális rendszerekben, akár terméyszeti katasztrüfa elleni védelem

Kritikus infrastruktúra: őket nyújtó szervezetekkel szemben nagyobb kiberbiztonsgi elvárás

Pl bank, közmű (áram, víz)

Iso 27000-27001: információ biztonsági tanusítvány, amit cégek tudnak szerezni, harmadik személy állítja ki, biztonságos kommunikáció v adatkezelést biztosít

**Information security is the preservation of confidentiality, integrity, and availability of information.**

Egyediség (authenticity): Biztosítja, hogy az adat, média, vagy más digitális tartalom valóban az állítólagos forrástól származik.

Deepfake probléma, megkülönböztetés

Hogyan lehet megbizonyosodni arról, hogy egy aláírás hiteles?

Megoldás: pl kriptográfia (digitális aláírás)

Visszavonhatatlanság(non-repudiation): Biztosítja, hogy egyik kommunikációs fél sem tudja visszautasítani a saját aláírásának egyediségét és az üzenet küldését.

Cél: elszámolhatóság

Megbízhatóság(reliability): Biztosítja, hogy a rendszerek, szolgátatások minimális hibával ellátják a kitűzött céljukat.

Elréhetetlenség minimalizásása, redundancia

**CIA triad:** Confidetiality, Integrity, Availability

Kalsszikus kiberbiztonsági célok

Confidetiality: illetéktelenek ne jussanak az adathoz

Integrity: illetéktelenek ne módosítsák az adatot

Availability: a saját felhasználóknak elérhető legyen a rendszer

**Confidetiality**

Titkosítottság (confidetiality): Az a tulajdonság, miszerint az információhoz nincs hozzáférése illetéktelen személyeknek, folyamatoknak, entitásoknak.

Érzékeny személyes adatok (orvosi adatok)

Általános veszélyek: adatlopás (külső), adatszivárgás (belső), szándékos szivárgás

Kontrol:

Hozzáférési szabályozás (access control): AAA: Authentication, Authorisation, Accounting

Authentication: személyazonosság megbizonyosodása

Authorisation: személyazonossághoz jogosultság rendelése

Accounting: feljegyzés, dokumentálás

**Integrity**

Adatintegritás (data integrity)**:** Az a tulajdonság, miszerint az adatot nem szerkesztették vagy törölték a megfelelő jogosultság nélkül.

Kontrol:

Autentikáció, kriptográfia, biztonsági mentések, fizikai védelem

**Availability**

Elérhetőség (availability)**:** Az a tulajdonság, miszerint az adat elérhető és felhasználható egy jogosult felhasználó igényére.

**Countermeasures (security controls):** Technology, Policy & Practice, People

Különböző kontorollok csoportosítása

**Technology**

Hardver és szoftver

Intrusion detection/prevention system

**Policy & Practice**

Szabálykönyv, cégesz/folyamat szintű

Kontrollok arányosak a cég céljaival (emberi és technológiai is)

**Adatállapotok:** Data at Rest, Data in Transit, Data in Process

Más-más kockázat és megelőzés

**Data at Rest**

DAS (Direct Attached Storage): usb, hard drive

NAS (Network Attached Storage): központi tár amit a hálózaton keresztül érünk el

Kockázatok: jogosulatlan hozzáférés, fizikai sérülés

Védelmi intézkedések: titkosítás, kozzáférés korlátozása

**Data in Transit**

Fiziaki átvitel, internet, wifi, üvegkábel

**Data in Process**

Begyüjtés és elmentés, számolás, kiírás

Kockázat: integritás sérülése, pl hardver/szoftver meghibásodás

**Threats, Vulnerabilities, Incidents, Impacts**

**Threat Actor:** direkt támadó, lehet természeti katasztrófa

**Threat Scenario:** támadó által megtett lépések sorozata

**Vulnerability:** serülékenység, ami lehetővé tesz egy fenyegetettségi szenáriót, sérülékenységi felület

**Incident:** kárt szenved a CIA, lehet eltervezett vagy más okokból

**Impact:** az elszenvedett kár, pénzgyi, szolgáltatás kimaradása, hírnév serülése, jogi

**Risk:** kockázat, incidens valószínűsége és a hatás mértéke adja

**Security Controls:** sérülékenységek kezelése, kockázat csökkentése, actor lépéseinek megszakítsa

**Hacker kategóriák (sapkák szerint)**

Black(devious, vagyonszerzés a cél pl), White(etikus profi), Gray(előző kettő között), Blue(amatőr), Red(black ellen harcol), Green(lelkes zöldfülű)

**Script Kiddie:** fiatal és tapasztalatlan actorok akik szkripteket használnak, kárt okozhat

**Vulnerability Broker:** piacon eladja a sérülékenységeket

**Hacktivist:** DedSec my beloved

**Kiberbűnöző:** Black hat, pénzügyi céllal

**State-Sponsored Hacker:** adott állam által pénzelt, céljait teljesítű hackerek