Az Informatikai Biztonság Alapjai

Dr. Varga Pál

BME Távközlési és MédiaInformatikai Tanszék

pvarga@tmit.bme.hu

RelNetik Szeminárium - 2018/09/18

Tartalom

- Információbiztonsági alapkérdések: CIA, AAA, TRV, TLA
- Miért kell megvédeni az információt?
- Mi az információbiztonság?
- Szabályozások, irányelvek
- Üzemeltetés biztonsága
- Titkosítás
- Hálózati titkosítás

- Köszönet: Jankó Árpád, T-Systems, TrustaaS

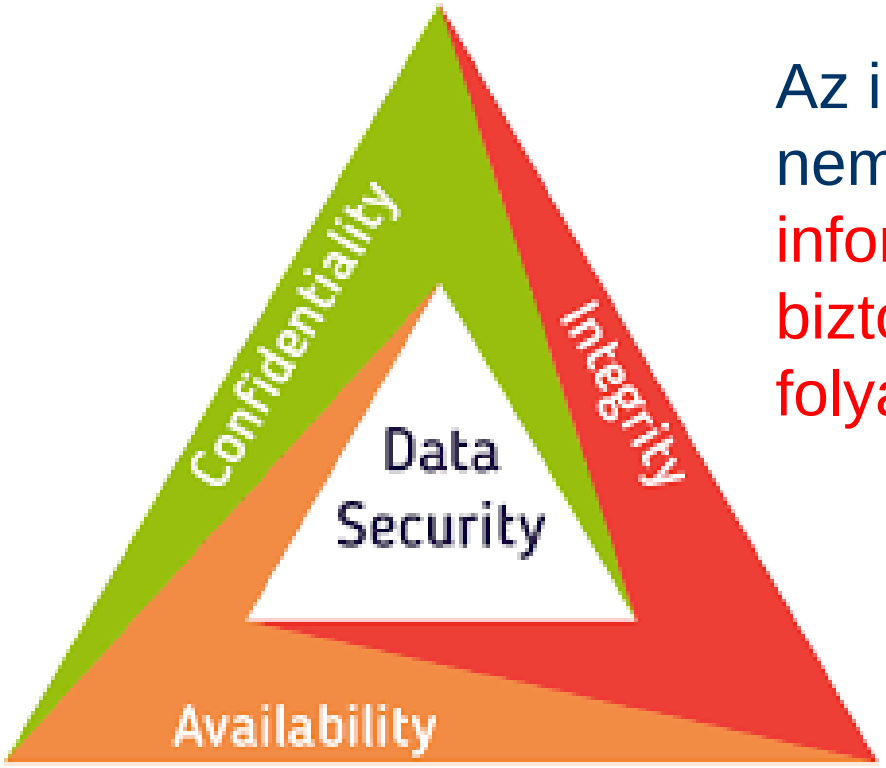
Információbiztonság

- Az információ értékes
- Az információ sokféle formában jelenhet meg:
  - papíron, **elektronikusan**
  - képekben, hangban, dokumentumban

- Az információvédelem: az információ bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása

Definíciók

Az információ-biztonság alapelvei



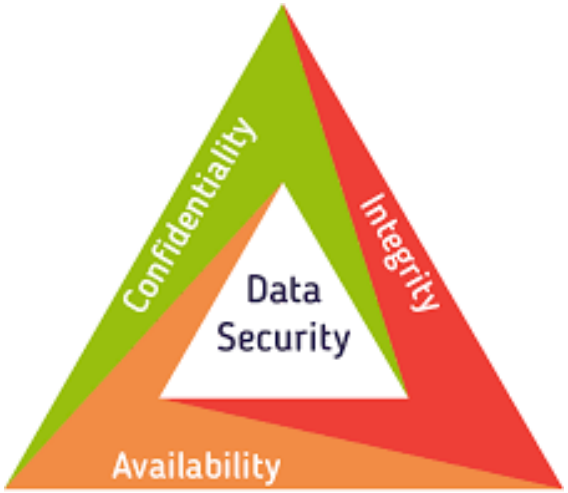
Az információvédelem nem más, mint az információval kapcsolatos biztonsági kockázatok folyamatos menedzselése

- Confidentiality – Bizalmasság
- Integrity – Sértetlenség
- Availability – Rendelkezésre állás

Az információ-biztonság alapelvei

- Confidentiality – Bizalmasság

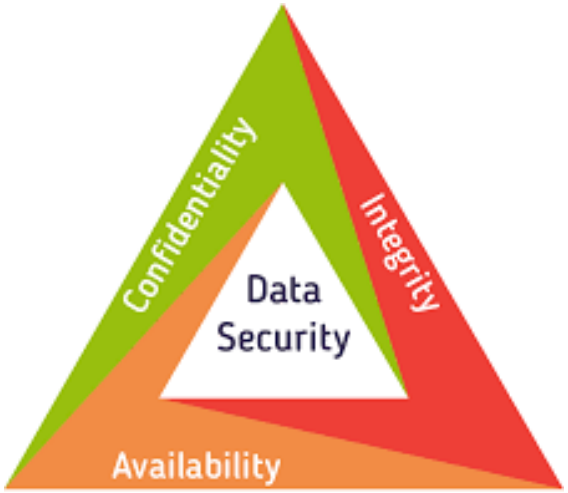
  (titkosság)



„annak biztosítása, hogy az információ csak az arra felhatalmazottak számára legyen elérhető” - Wikipedia

Az információ-biztonság alapelvei

- Integrity – Sértetlenség
  (integritás)

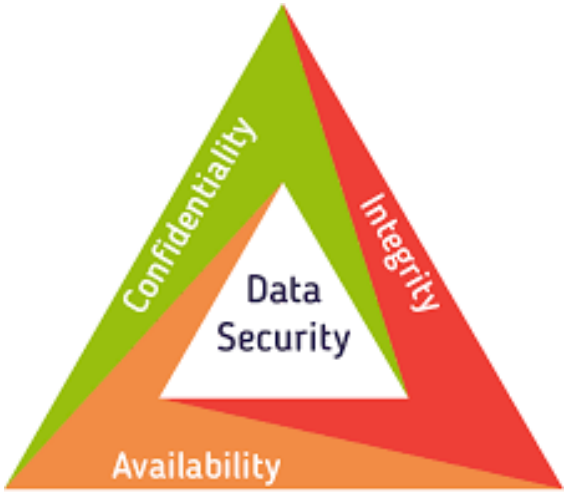


„az információk és a feldolgozási módszerek teljességének és pontosságának megőrzése” - Wikipedia

Az információ-biztonság alapelvei

- Availability – Rendelkezésre állás

  (elérhetőség)



„annak biztosítása, hogy a felhatalmazott felhasználók mindig hozzáférjenek az információkhoz és a kapcsolódó értékekhez, amikor szükséges” - Wikipedia

Információbiztonság

- Kockázatok csökkentése intézkedések alkalmazásával

- Intézkedések – kontrollok
  - Adminisztratív
  - Logikai
  - Fizikai
- Ezen belüli kategóriák
  - Megelőző (preventive)
  - Feltáró (detective)

Hozzáférés vezérlés (control)

Annak a képessége, hogy engedélyezzük, vagy megtagadjuk egy alany hozzáférését valamihez.

Három alapvető szolgáltatást nyújt:

- Authentication (az alany azonosítása)
- Authorization (engedélyezett-e neki az adott szolgáltatás használata?)
- Accountability (naplózza, mit csinált az alany)

Threat, Vulnerability, Risk

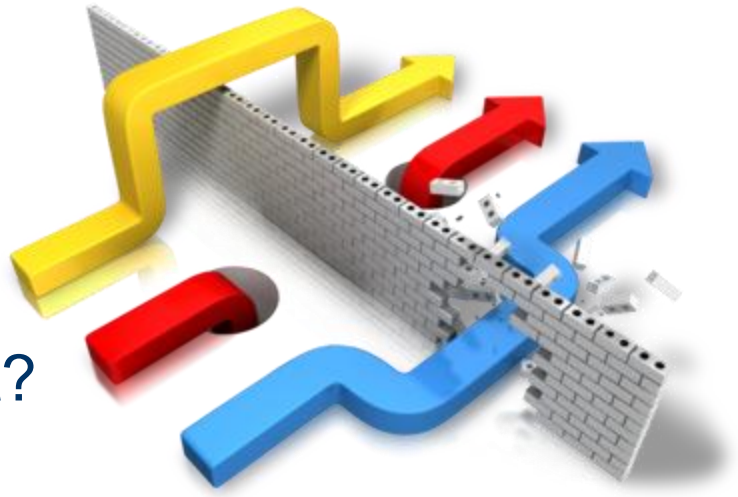
- Fenyegetés (Threat)
  - Bármilyen körülmény, vagy esemény, ami potenciális fenyegetést jelent a hálózati szolgáltatás működésére
- Sebezhetőség (Vulnerability)
  - Gyengeség a biztonsági folyamatokban, hálózati infrastruktúrában, vagy olyan rendszer-megvalósítás, amely kihasználható, és veszélyezteti a biztonságot
- Kockázat/veszély (Risk)
  - Egy adott gyengeség kihasználásának valószínűsége

Fenyegetés - Threat

- “motivált ellenfél, ami képes gondot okozni”
- Példák:
  - Emberi fenyegetések
    - Szándékos vagy akaratlan
    - Rosszindulatú, vagy jószándékú
  - Természeti fenyegetések
    - Földrengések, tornádók, vízözön, földcsuszamlás
    - Környezeti katasztrófák
    - Rövidtávú HW/SW eszköz meghibásodás
    - Hosszútávú áramkimaradás, szennyezés, folyadék-szivárgás

Sebezhetőség - Vulneraility

- Gyengeség a biztonsági folyamatokban, hálózati infrastruktúrában, vagy olyan rendszer-megvalósítás, amely kihasználható, és veszélyezteti a biztonságot
- Szoftverhibák (bug)
  - Konfigurációs hibák
  - Hálózattervezés hibák
  - Titkosítási hiányosságok
- Hol keressük a sebezhetőségeket?
- Exploit (kihasználás)
  - A sebezhetőség kihasztnálása, ezáltal a rosszindulatú cél elérése

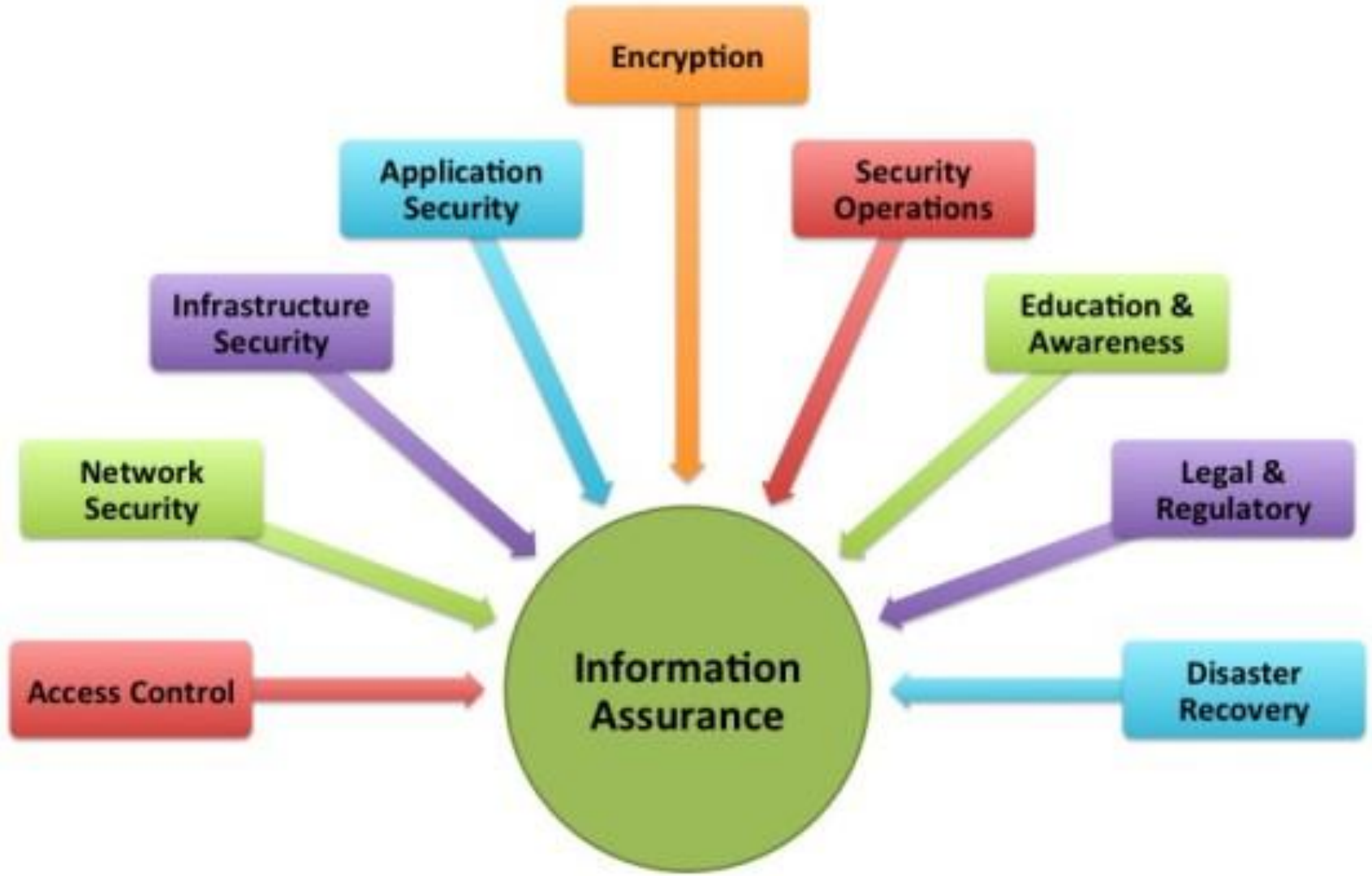


Kockázat/Veszély - Risk

- Adott gyengeség kihasználásának valószínűsége
- Néhány kérdés:
  - Milyen valószínű, hogy megtörténik?
  - Mit kockáztatunk, ha úgy döntünk, semmit nem teszünk?
  - Vezethet-e adatvesztéshez?
  - Milyen hatással lehet a vállalat reputációjára?
- Kategóriák:
  - Magas, közepes, vagy alacsony kockázat

Kockázat = Fenyegetés * Sérülékenység * Hatás

Az Információbiztonság körbejárása


Encryption
Application Security
Security Operations
Infrastructure Security
Education & Awareness
Network Security
Legal & Regulatory
Access Control
Information Assurance
Disaster Recovery

Miért vagyunk célpontok?

- Adatok nagy része elektronikus formában létezik
- Ezek egy része bizalmas, mások számára is értékkel bír
  - Anyagi, személyes, politikai célok
- IT eszközöktől erős függés (tárolás, alkalmazások, kommunikáció, stb.)
- A világ „nem barátságos”

Mit tehet a behatoló?

- Eavesdrop (hallgatózás) - routerek, linkek, szolgáltatások
- Önkényes üzenetek küldése
- Felvett üzenetek visszajátszása
- Üzenetek megváltoztatása (fejrész / tartalom)
- Rosszindulatú kódok futtatása / erre trükkel rávezetni embereket
- Bug kihasználása és „vezérlés átvétele” az eszközök felett

Milyen hatása lehet?

- Az üzleti folyamatok megszakadása
  - Szolgáltatás, gyártás
- Titkos adatokat megszerzi a konkurencia
- Személyes adatokkal visszaélés
- Bankszámlákhoz hozzáférés
- Jogi következmények (szerződések, törvények megsértése)
- Jó hírnév sérülése
- Üzleti előnyök elvesztése
- Közművek elérhetetlensége (SCADA)

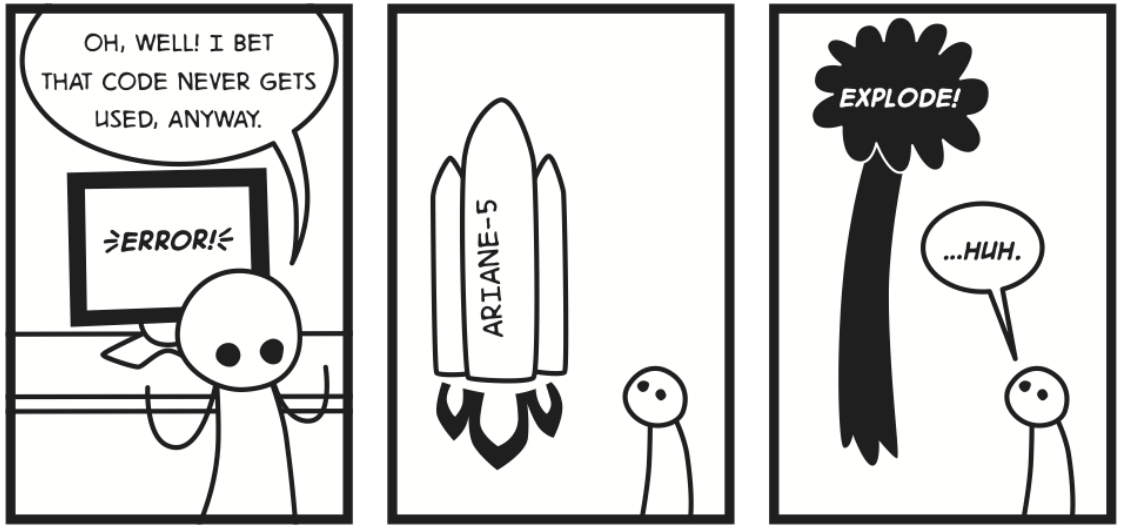
Mi a „Security osztály” célja?

- Adathozzáférés vezérlése
- Hálózati hozzáférés vezérlése
- Információ megóvása az átvitel során
- A hálózat elérhetőségének biztosítása
- Behatolás megelőzése, megakadályozása
- Incidensek le-reagálása

Mi határozza meg a biztonsági módszereket?

- A nyújtott szolgáltatások vs. Biztonsági szint
  - Minden szolgáltatáshoz tartozik külön rizikófaktor
- Könnyű használat vs. Biztonság
  - A legkönnyebben használható rendszer bárkinek hozzáférést biztosít, bármilyen megkötés vagy azonosítás nélkül
- A biztonság ára vs. A veszteség rizikója
  - Karbantartási költségek
- A célokat minden felhasználó, munkatárs, menedzser felé kommunikálni kell egy szabályrendszeren keresztül: „security policy”

Biztonsági problémák okai



- Protokoll hiba
  - Senkinek sem sikerül elsőre…
- Szoftverhibák
  - Is it a bug or feature?
- Aktív támadás
  - Cél a vezérlési-sík
  - Cél az adat-sík
  - Valószínűbb, mint gondolhatnánk…!
- Konfigurációs hibák
  - Gyakori, közismert probléma

A jó biztonsági vezérelv (policy) jellemzői

- Műszakilag kivitelezhető
- Szervezetileg kivitelezhető
- Érvényesíthető biztonsági eszközökkel és szankciókkal
- Világosan definiálja a felhasználók, adminisztrátorok, és a vezetőség felelősségi köreit
- Rugalmasan adaptálható a változó körülményekhez

Mit védünk?

- Azonosítsuk a kritikus „kincseket”
  - Hardver, szoftver, adat, ember, dokumentáció,…
- Rendeljünk értéket a „kincshez”
  - Megfoghatatlan elem – fontosság / kritikusság
  - Megfogható elem – a csere értéke, a kiesés miatt felmerülő oktatás értéke, a veszteség rövidtávú hatása
- Határozzuk meg a biztonsági rések kihasználásának valószínűségét
  - Mik a fenyegetések és sebezhetőségek?

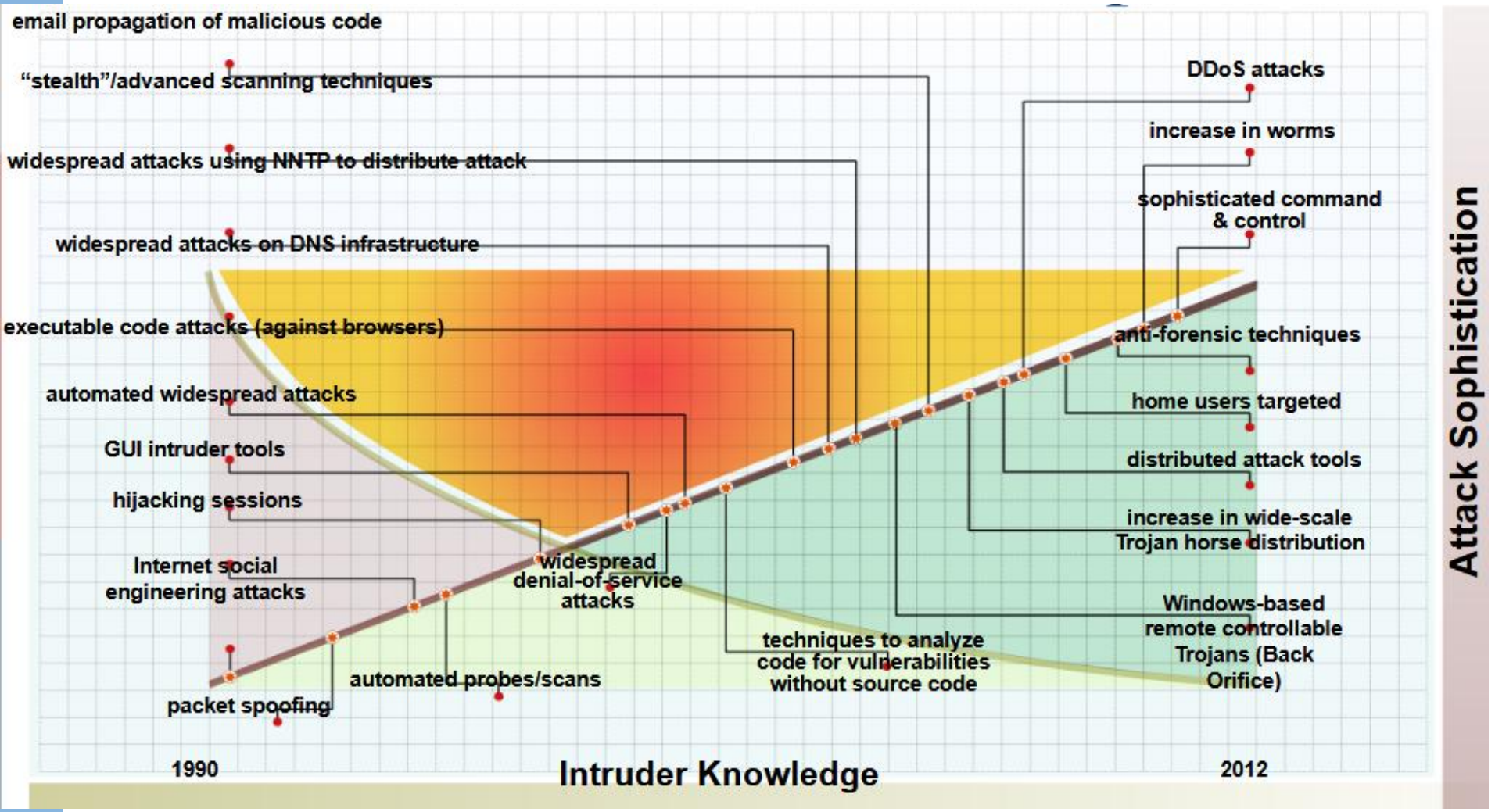
Milyen eseményektől kell félni?

- Személyazonosság ellopása, és azzal visszaélés
- Adatok integritása sérül
- Adatok vagy eszközök ellopása
- Adatok vagy eszközök elvesztése
- Illetéktelen hozzáférés
- IT szolgáltatások elérhetetlensége
- Kémkedés
- Rongálás
- Social Engineering
- Kiberháború

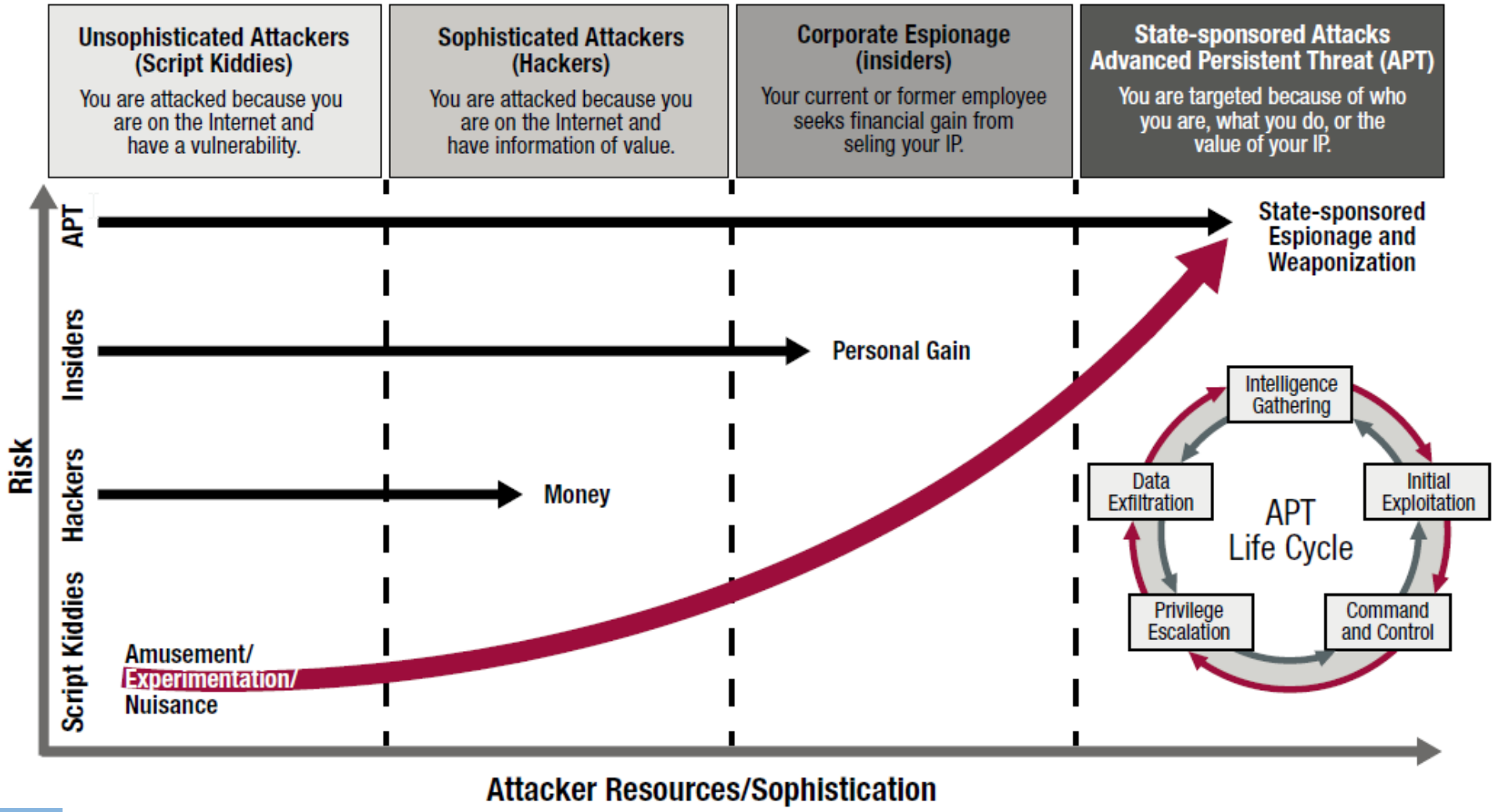
Risk Mitigation vs. Költségek

- Risk mitigation
  - Kockázatok mérsékése: a megfelelő módszerek kiválasztása a kockázatok elfogadható szintre való csökkentéséhez
- „A kockázat elfogadható szintje”
  - össze kell hasonlítani a biztonsági rés kihasználásának hatását a védelmi költségekkel
- Fel kell mérni a lehetséges veszteségeket
  - és ne költsünk többet a védelemre, mint amennyit a védendő dolog ér

A támadások evolúciója…



A támadók evolúciója…



A támadók motivációja

- Bűnöző
  - Az infrastruktúrát bűn elkövetésére használja
  - Pénzszerzés
- Háború/Kémkedés/Terrorizmus
  - …közismerten ezek támadják a kritikus infrastruktúrát
- Patriotikus / Elvi
  - Hasonló okból motivált emberek nagyobb csoportja; az ok lehet bármi a nemzeti büszkeségtől a szórakozásig…

Támadási motivációk

- Államok – TITKOKat szeretnének tudni
- Szervezett bűnözők – PÉNZT szeretnének
- Tüntetők / aktivisták – FIGYELMET szeretnének
- Hackerek és kutatók – TUDÁST szeretnének

Általános Fenyegetések

- Masquerade
  - Másnak adja ki magát
- Eavesdropping
  - Egy alany olyan információt ismer meg, amit nem szabadna neki
- Authorizációs sértés
  - Egy alany olyan szolgáltatást / erőforrást használ, amit nem szabadna neki
- Információ-vesztés vagy -módosítás
  - Az adat módosításra, vagy megsemmisítésre kerül
- A kommunikációs lehetőségek megtagadása (repudiation)
  - A kommunikációban való részvétel megtagadása, engedélyezés helyett
- Információ hamisítás
  - Valaki más nevében kreálunk információt
- Szabotázs
  - Bármilyen akció, ami szolgáltatások, vagy rendszerek működését elérhetőségét korlátozza

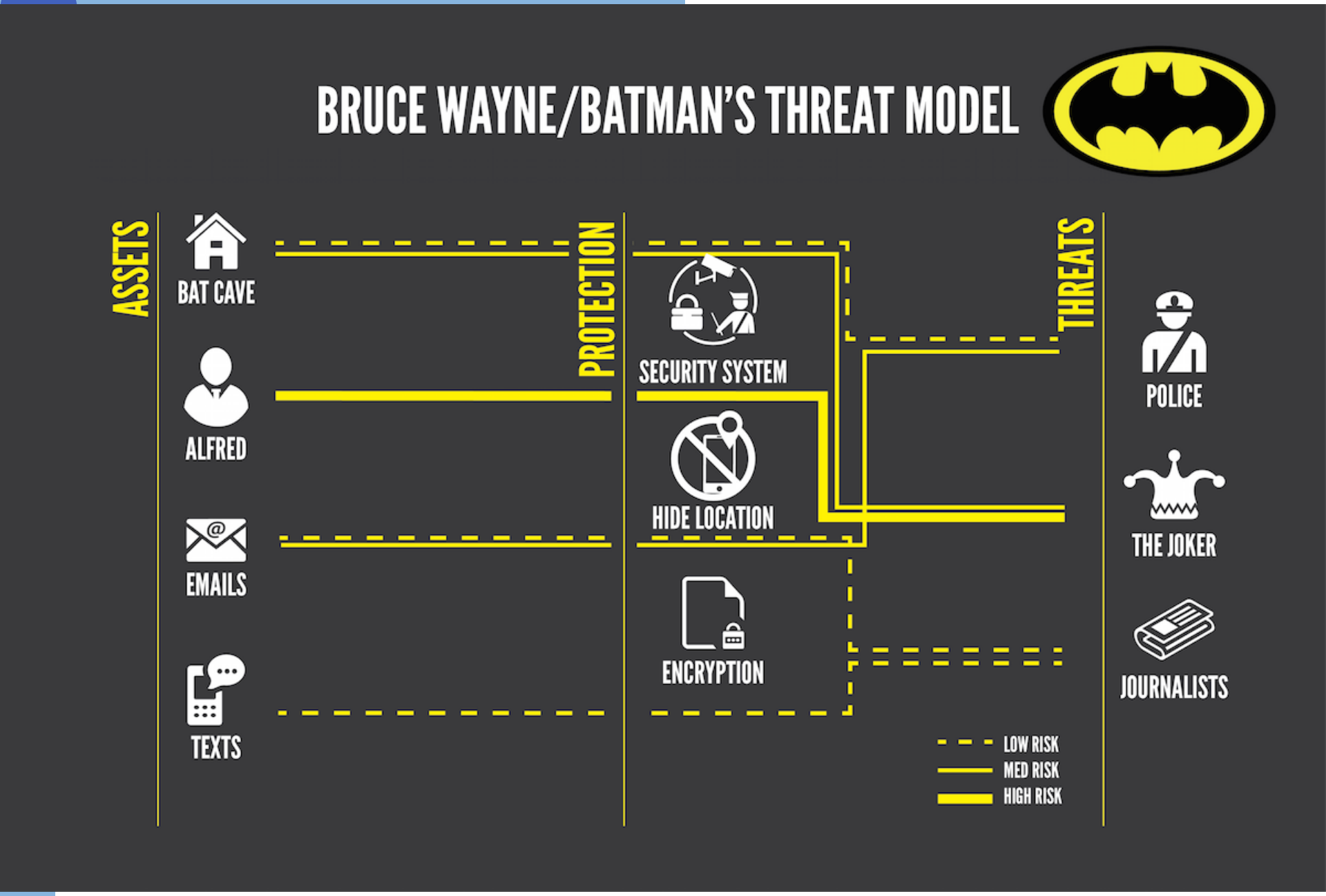
Támadások forrása (as of RFC 4778)

- Aktív támadás: adatot ad a hálózati forgalomba.
- Gyakori a küldő címének meghamisítása (két típusú sérelem).
- Passzív támadás: az adatokhoz való hozzáférés, a titkosság megszüntetése a cél.

Active Attacks	Passive Attacks
Denial of Service attacks	Reconnaissance
Spoofing	Eavesdropping
Man in the Middle	Port scanning
ARP poisoning	
Smurf attacks	
Buffer overflow	
SQL Injection	

Összegzés - A leggyakoribb fenyegetések és támadások

- Unauthorized access – nem jól biztosított eszközök feltörése
- Eavesdropping – hozzáférés az átvitel adataihoz
  - jelszavak, hitelkártya-adatok, üzleti titkok keresése
- A kommunikáció eltérítése
  - Az adatok vizsgálata és módosítása átvitel során
- IP spoofing vagy hálózati cím módosítása
  - Imperszonalizáció, a hozzáférési mechanizmusok kijátszására
  - A forgalom hamis kiszolgáló felé irányítása
- DOS attacks
  - Szolgáltatás-megtagadás kikényszerítése a rendszer működésének ellehetetlenítésével, pl. túlterheléssel
  - CPU, memory, sávszélesség


BRUCE WAYNE/BATMAN'S THREAT MODEL
ASSETS
BAT CAVE
ALFRED
EMAILS
TEXTS
PROTECTION
SECURITY SYSTEM
HIDE LOCATION
ENCRYPTION
THREATS
POLICE
THE JOKER
JOURNALISTS
LOW RISK
MED RISK
HIGH RISK

Külső és Belső Szabályozás

Megfelelés

- Törvényi szabályozás, szabványok, legjobb gyakorlatok

- Kötelező érvényűek
  - Pénzügyi iparági törvények
  - PSZÁF ajánlások
  - Adatvédelmi törvény
  - PCI DSS (Payment Card Industry Data Security Standard)

Megfelelés

- Nem kötelező érvényűek
  - ISO17799/ISO27002 – Az információbiztonság irányítási gyakorlatának kézikönyve
  - ISO27001 – Információbiztonság irányítási rendszerei: Követelmények
  - Cobit v4 – Control Objectives for Information and Related Technology

Szabályozás

- Információbiztonsági Politika
  - Általános irányelvek, felelősségi körök
  - A legfelső vezetés biztonsági elkötelezettsége
  - Hosszú távra készül
  - Legfelső szintű vezetői jóváhagyást igényel

- Információbiztonsági Szabályzat
  - IBP-nek megfelelő intézkedések
  - Középtávra készül
  - Legfelső szintű vezetői jóváhagyást igényel

Szabályozás

- Eljárások, utasítások
  - Technikai, technológiai irányultságú intézkedések
  - Folyamatok
  - Rövidtávra készülnek
  - Informatikai vezetői jóváhagyást igényelnek
  - Pl. mentési rend, incidenskezelési folyamat, vírusvédelmi eljárás, stb.

Információbiztonsági szerepek

- Információbiztonsági vezető
  - Információbiztonsági keretrendszer kidolgozása és működtetése
  - Információbiztonsági stratégiai tervezés
  - Információbiztonsági operatív feladatok felügyelete
  - Törvényeknek, szabványoknak való megfelelés biztosítása

Információbiztonsági szerepek

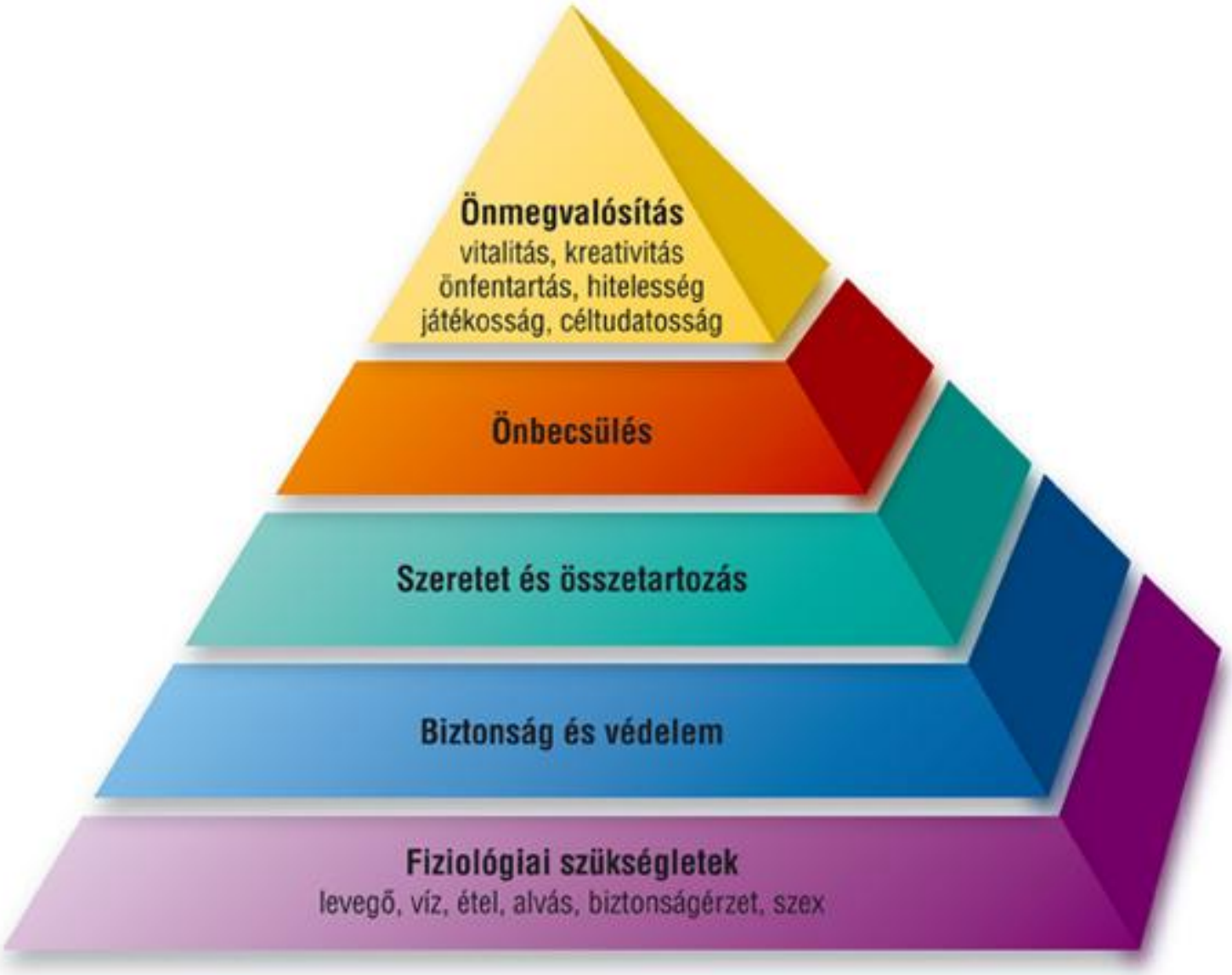
- Információgazda, -kezelő, -használó
  - Egy adott információ, információs rendszer vonatkozásában értendő
- Információ gazda
  - Adat-, rendszer-, alkalmazás- és hálózatgazda
  - Általában üzletági vezetők
  - Teljes felelőséggel tartoznak a hozzájuk rendelt információ és információs rendszerek biztonságáért

Információbiztonsági szerepek

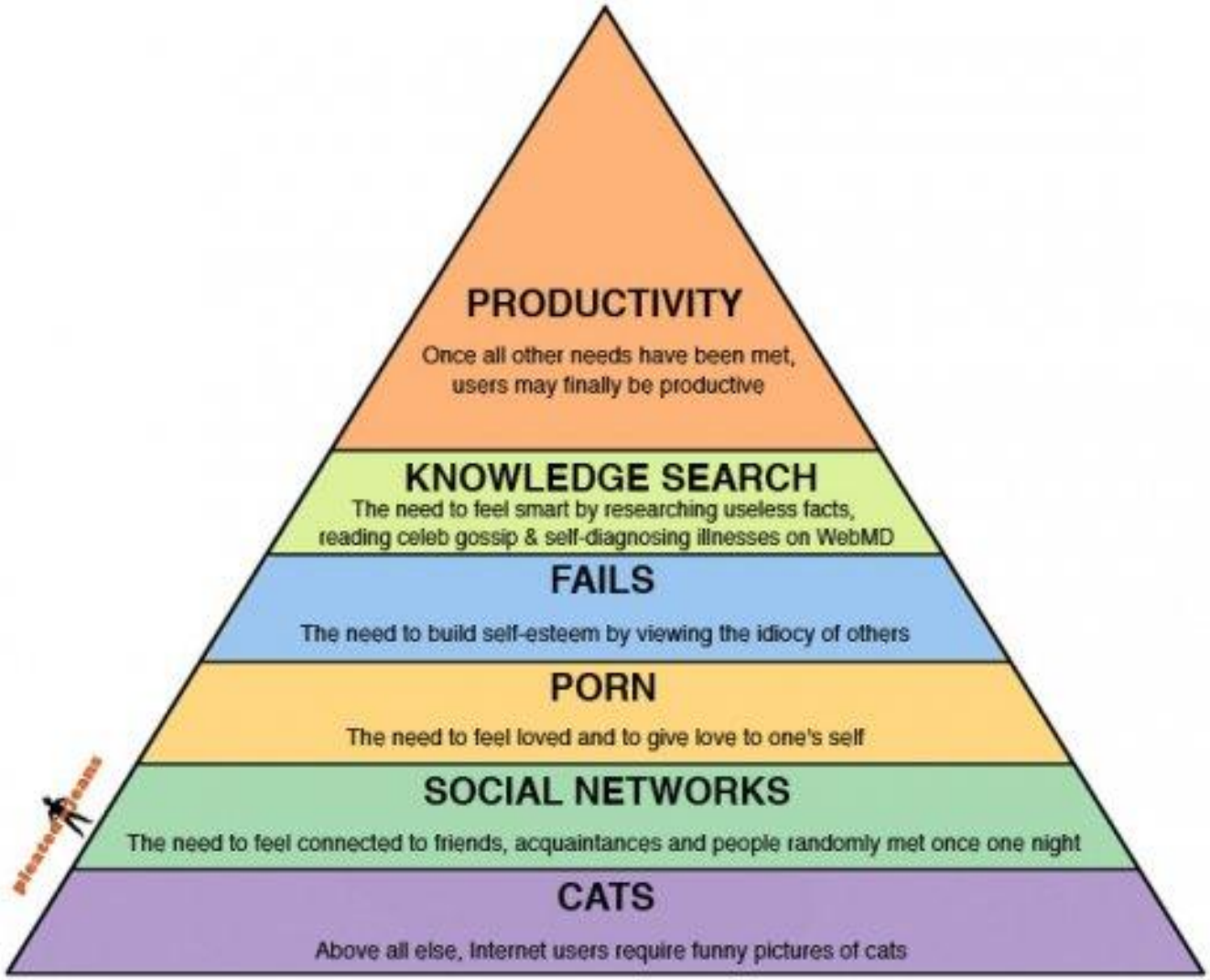
- Információkezelő
  - Az információgazdák a napi feladatokat az információkezelőknek delegálják
  - Rendszer-, hálózatadminisztrátorok, ügyfélszolgálat (help desk)
- Információ-felhasználó
  - Bárki aki az információt napi munkája során használja
  - Belső munkatársak és külső felek
- Belső ellenőrzés
  - Az információbiztonság független „minőségbiztosítója”

Üzemeltetői szemmel nézve

A Maslow piramis



Maslow's Hierarchy of Internet Needs



Üzemeltetés biztonsága

- Tipikus üzemeltetési biztonsági feladatok
  - Védelem rosszindulatú kódok ellen
  - Adatmentés és -megőrzés
  - Naplózás
  - Biztonsági frissítések
  - Adathordozók kezelése
  - Logikai hozzáférések kezelése
  - Kriptológiai megoldások

Fizikai biztonság

- Fizikai biztonsági zónák, beléptetés
  - Beléptető rendszer, őr, lakat, korlátok, zárható szekrények, kamera, riasztó, stb.
  - Látogatókontrol
- Környezeti hatások elleni védelem
  - Tűz, víz, földrengés
- Áram, légkondicionálás
  - UPS, generátorok, redundáns tápellátás

Fizikai biztonság

- Sugárzás elleni védelem
  - Titokszobák, NATO helyiségek, stb.
  - Tempest
- Berendezések védelme, karbantartás
- Eszközök telephelyről/re történő kivitele/bevitele

Internet biztonság

- Internet, Intranet, Extranet
- Belső IT infrastruktúrát meg kell védeni a nyilvános hálózati szegmenstől
- Határvédelem
  - Tűzfalak, IDS/IPS
- Külső kapcsolatok elérése csak engedélyezett kapcsolatokon keresztül
  - Modemek (3G/4G is) és WIFI eszközök használata

Internet biztonság

- Kommunikáció
  - Protokollok
    - HTTPS, SSL, SSH, SFTP, SNMPv3
    - FTP, Telnet, SNMPv1, NFS
  - VPN
- Architektúra
  - Dedikált server a DMZ-ben
  - Funkciók szétválasztása -> 2 vagy 3 szintű architektúra
- Szolgáltatások biztonsága

Cloud biztonság

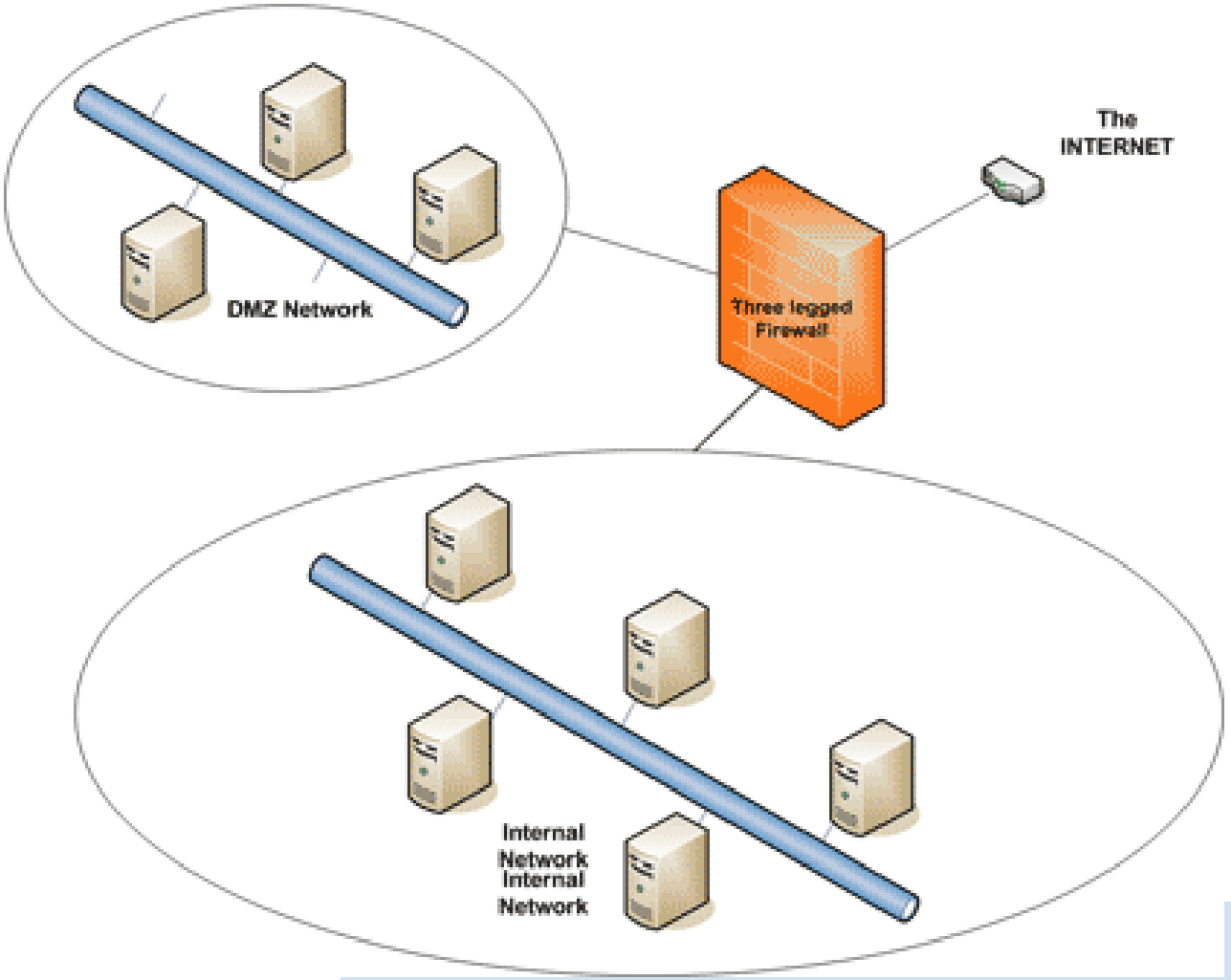
- A Cloud Computing számos üzleti előnnyel jár
  - Opex vs Capex, fizetés igény szerint, agilitás, gyors bevezethetőség, új üzleti lehetőség, stb.
- DE adatok kikerülnek a szervezet ellenőrzése alól.
- Hagyományos és új kockázatok

Cloud biztonság

- Cloud specifikus kockázatok (pl.)
  - Adatok fizikai helye
  - Megfelelőségi kényszer
  - Közös bérlők (osztott infrastruktúra)
  - Korlátozott monitoring
  - Korlátozott auditálási lehetőség
  - Szolgáltató váltás nehézsége
  - Támadások vonzó célpontja az aggregáció miatt

Infrastruktúra biztonság - Hálózatbiztonság

- Biztonsági zónák kialakítása



Infrastruktúra biztonság – Hálózatbiztonság

- Tűzfalak
  - Biztonsági zónák közötti forgalom ellenőrzése
    - Internet, DMZ, belső hálózat
  - Layer 3 – Layer 7
  - Típusai
    - Csomagszűrő
    - Stateful inspection
    - Proxy
      - alkalmazás-szintű, összeköttetés-szintű
  - Default policy

Infrastruktúra biztonság – Hálózatbiztonság

- IDS/IPS - Behatolás-észlelő és megakadályozó rendszerek
  - Internet kilépési pontoknál
  - Működés szerint
    - Minta-alapú (signature-based)
    - Anomáliadetektorok
    - Honeypot
  - Leglényegesebb funkciók
    - Aggregálás
    - Korrelálás
    - Riasztás

Infrastruktúra biztonság

- Egyéb infrastruktúra biztonsági eszközök
  - NAC (Network Access Control)
  - Webtartalomszűrő
  - Email tartalomszűrő
  - Spam szűrő
  - VPN gateway
  - DLP (Data Loss Prevention) eszköz

Infrastr. biztonság – Szerverek és munkaállomások biztonsága

- Dedikált szerverek
- Távoli adminisztráció csak titkosított kapcsolatokon keresztül
- Titkosítatlan protokollok letiltása (pl. FTP, SNMPv1)
- Gyártó alapbeállításainak megváltoztatása
- USB portok kontrolálása
- Naplógyűjtés, monitorozás, riasztás
- Szoftver telepítési szabályok

Infrastr. biztonság – Szerverek és munkaállomások biztonsága

- Fizikai elhelyezkedés
- Patch menedzsment
- Mentés
- Antivírus program alkalmazása
- Személyes tűzfalak alkalmazása
- Eszközök biztonságos megsemmisítése
- Incidenskezelés és katasztrófa-elhárítás
- Rendszeres audit

Incidenskezelés

- Incidens
  - Minden olyan esemény, amely negatívan befolyásolja az információ és információs rendszerek biztonságát
  - Pl. DDoS, vírusfertőzés, jogosulatlan hozzáférés, stb.
  - Hatókör
    - Csak informatikai incidensek (természeti katasztrófa nem)
    - Fizikai: pl. lopás
    - Logikai: pl. jogosulatlan hozzáférés

Incidenskezelés

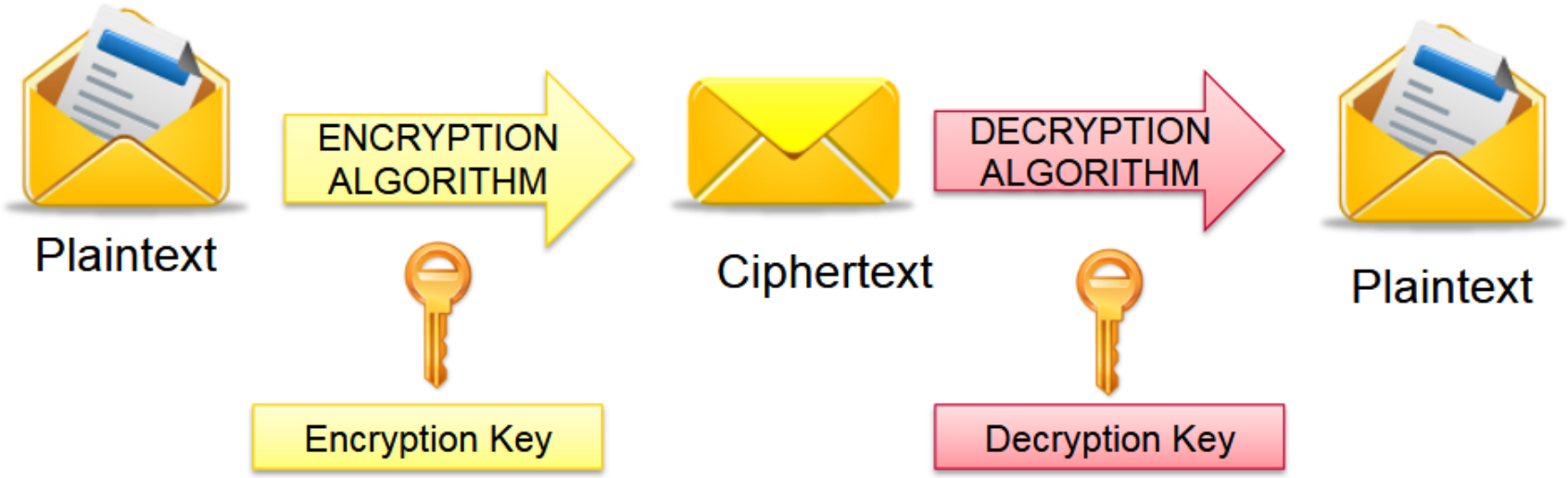
- Az Incidenskezelés legfontosabb előnyei
  - Strukturált megközelítés
  - Gyors és hatékony helyreállítás
  - Korábbi incidenseknél nyert tapasztalatok felhasználása
- Folyamat

Titkosítás

Titkosítás

- Folyamat, melynek során olvasható információból (plaintext) titkosítottat állítunk elő (ciphertext) a titkosító kulcs segítségével
- Körülvesz minket
  - Alkalmazási réteg: secure email, adatbázis-lekérdezések, messaging
  - Session réteg – using Secure Socket Layer (SSL) or Transport Layer Security (TLS)
  - Hálózati réteg – olyan protokollok használata, mint az IPSec
- A jó titkosító algoritmus előnyei:
  - Ellenáll a kriptográfiai támadásoknak
  - Különböző hosszúságú kulcsokat támogat: skálázható
  - Lavina-effektust hoz létre (a bemenet kis változásával a kimenet nagyon más lesz)
  - Nincsenek exportálási vagy importálási megkötései

Titkosítás – Encryption & Decryption



Szimmetrikus kulcsú algoritmus

- Ugyanazt a kulcsot használja a be- és kititkosításhoz
- A.k.a. „titkos kulcs” algoritmus
  - A működéshez a kulcsot titokban kell tartani
  - Ez mindig privát kulcs
- Ez a tradicionális módszer, 40..256 bit hosszú kulcsokkal.

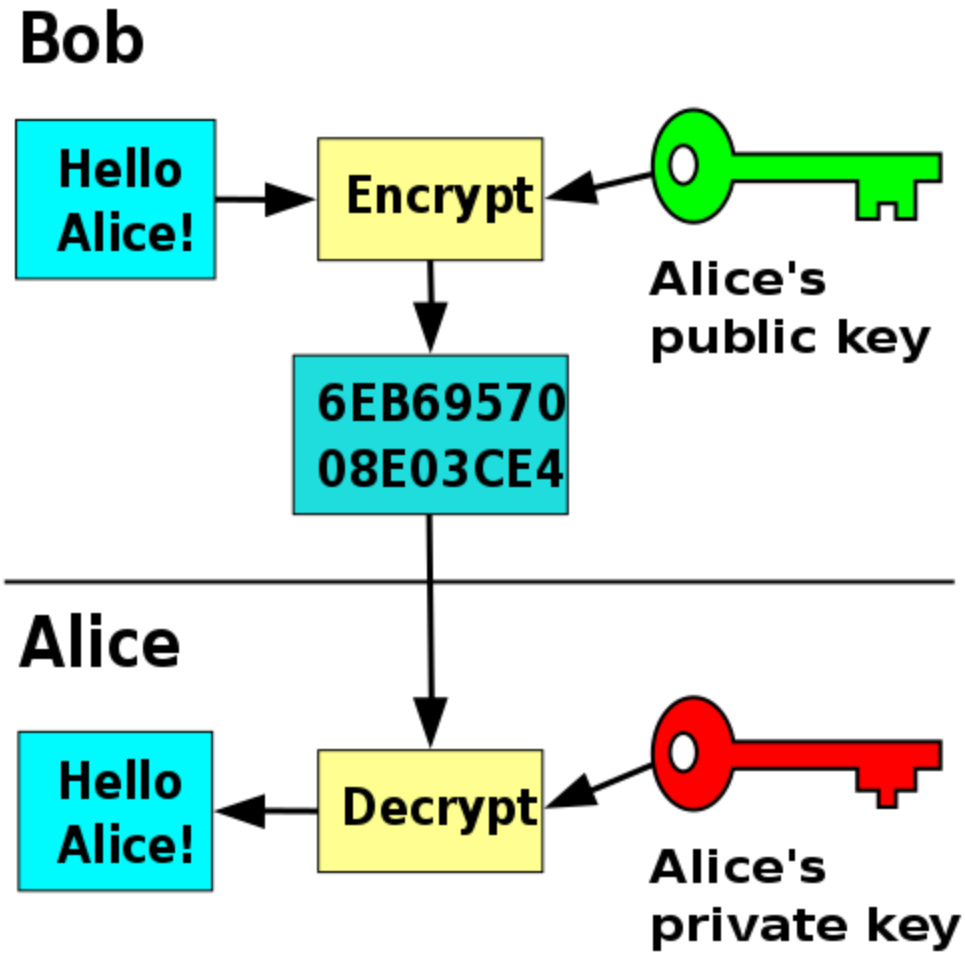
Szimmetrikus kulcsú algoritmus

- DES – blokkos titkosítás, elosztott kulcsú, 56-bit
- 3DES (Triple DES) – háromszor alkalmazza a DES-t ugyanazon a blokkon
- AES – a DES helyett van; ez a jelenleg elfogadott
- RC4 – változó hosszúságú kulcs, “stream cipher” (a kulcsot a stream-ből generálja, majd „stream XOR data)
- RC6
- Blowfish

Aszimmetrikus kulcsú algoritmus

- RSA – az első és leggyakoribb algoritmus
- DSA – a NIST Digital Signature Standard (DSS) írja le, digitális aláírásra, és üzenet-authentikációra használják
- Diffie-Hellman – csak titkos kulcs-cserére használják, aláírásra vagy hitelesítésre nem
- ElGamal – mint a Diffie-Hellman…
- PKCS – együttműködő szabványok és iránymutatások halmaza

Jellemző példa publikus és privát kulcsra



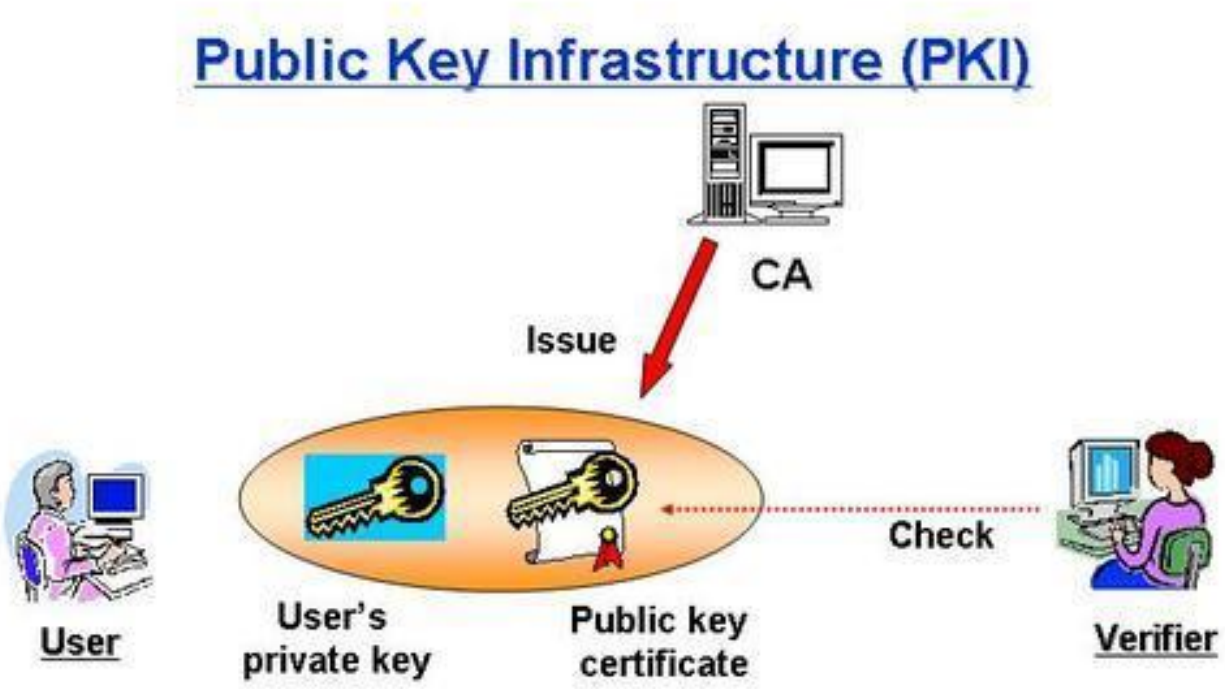
Symmetric vs. Asymmetric Key

Symmetric	Asymmetric
generally fast Same key for both encryption and decryption	Can be 1000 times slower Uses two different keys (public and private) Decryption key cannot be calculated from the encryption key Key lengths: 512 to 4096 bits Used in low-volume

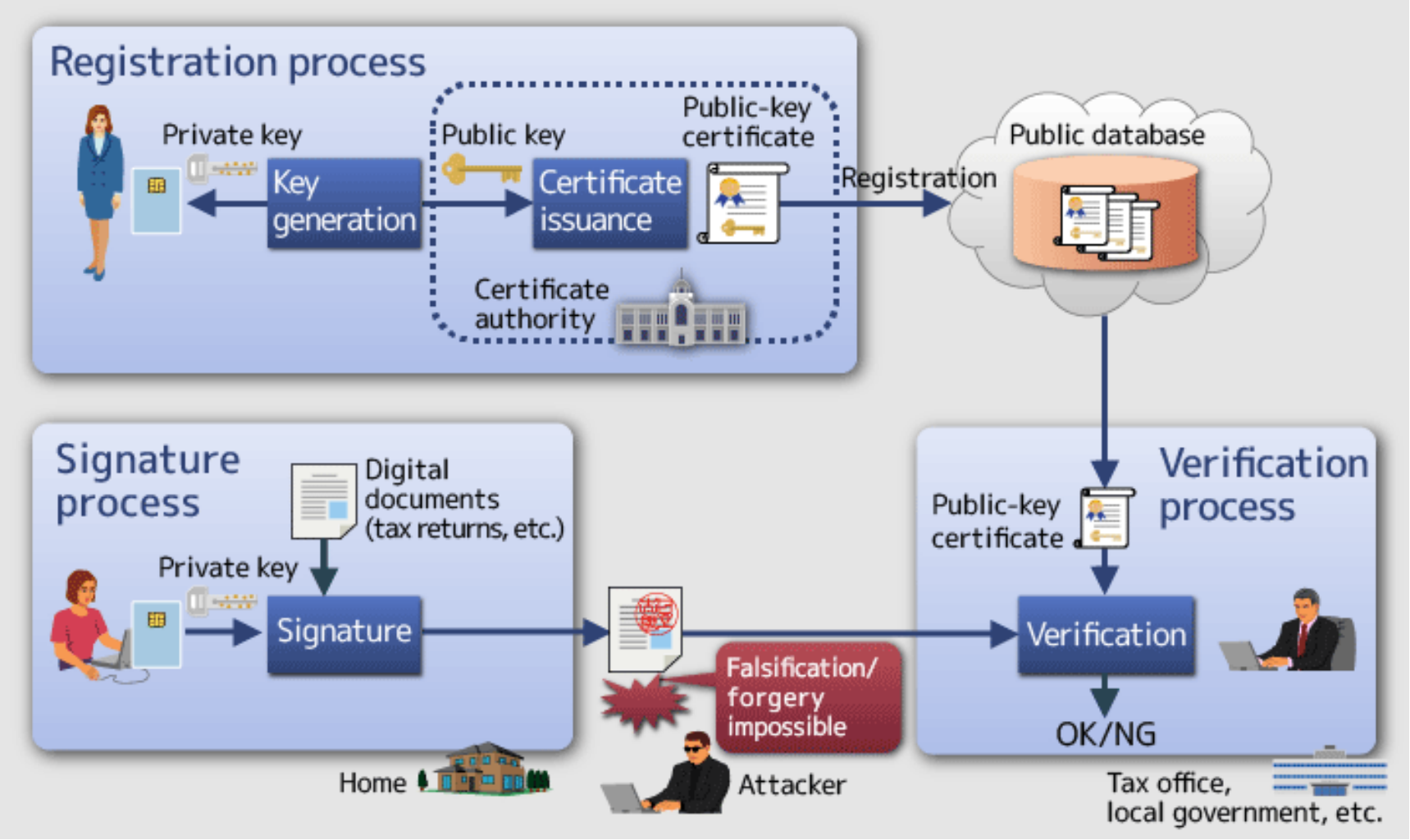
Public Key Infrastructure

- Keretrendszer, ami a Bizalom (Trust) hálózatára épül
- Kombinálja a publikus kulcsó titkosítást, a digitális aláírást, hogy biztosítsa a C.I.A. funkciókat és a hozzáférés vezérlést
- A magasfokú védelmet igénylő alkalmazásokat védi

PKI - egyszerű példa



PKI - példa

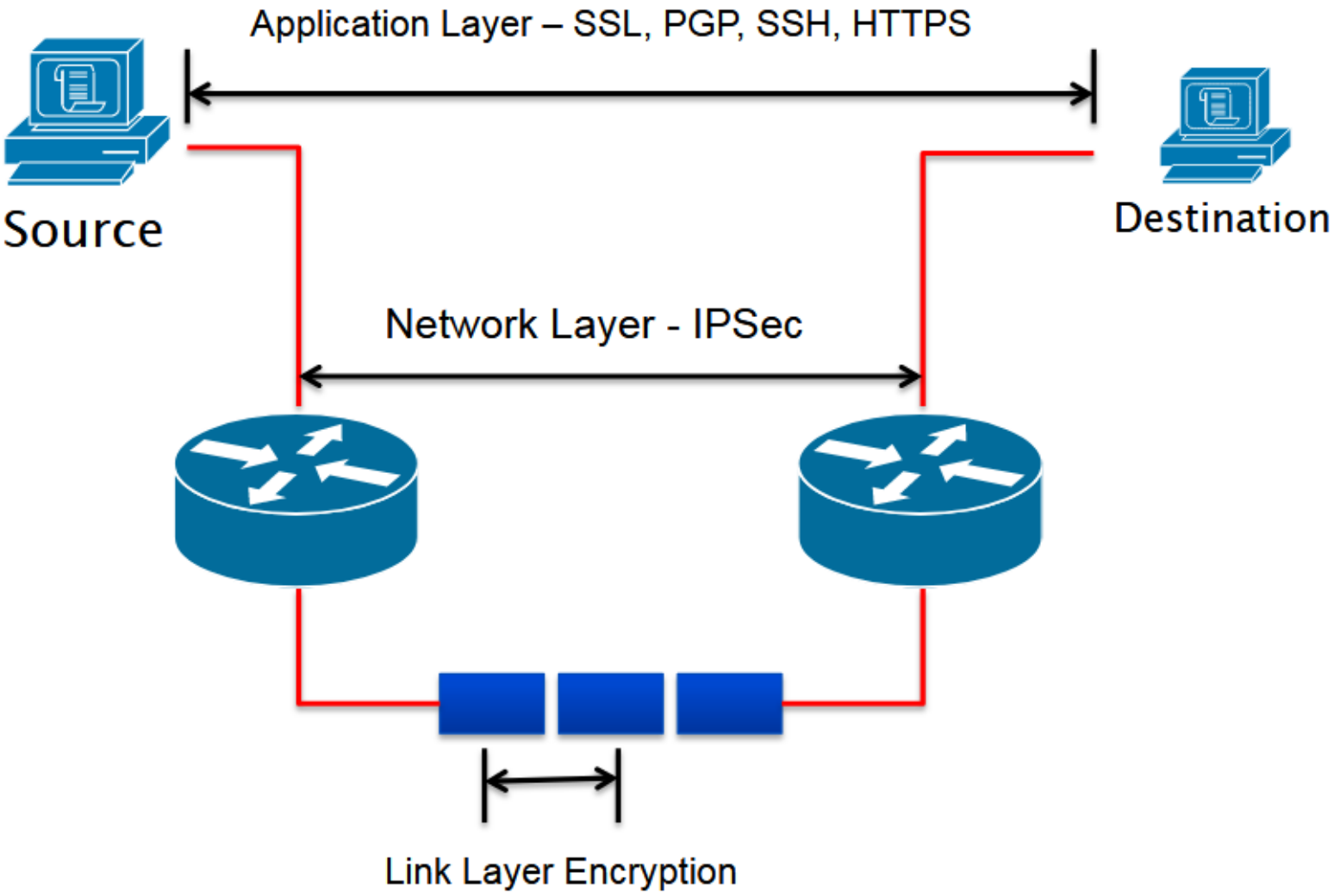

Registration process
Private key
Key generation
Public key
Certificate issuance
Public-key certificate
Certificate authority
Registration
Public database
Signature process
Digital documents (tax returns, etc.)
Private key
Signature
Falsification/ forgery impossible
Home
Attacker
Verification process
Public-key certificate
Verification
OK/NG
Tax office, local government, etc.

A PKI komponensei

- Certificate authority
  - Megbízható harmadik fél
  - Mind a bizonyítvány (certificate) birtokosa, mind az azt elfogadó fél megbízik benne
- Validation authority
- Registration authority
  - A nagy CA-k esetén külön RA-k tehermentesítik a CA
  - Identitás-azonosítás és regisztráció a bizonyítványért folyamodó részére
- Central directory

Hálózati titkosítás

Titkosítás a különböző rétegekben



Virtual Private Network

- Titkosított csatornát képez a publikus infrastruktúrán
  - Klienstől a tűzfalig
  - Routertől routerig
  - Tűzfaltól tűzfalig
- Remote access VPNs – távoli hozzáféréshez, „virtual private dial-up networks (VPDNs)”
- Site-to-site VPN, amikor több fix site van összekötve a publikus Interneten keresztül
- Point-to-Point VPN - „leased-line VPNs”

VPN Protokollok

- PPTP (Point-to-Point tunneling Protocol)
  - By Microsoft, @ data-link layer
- L2F (Layer 2 Forwarding Protocol)
  - By Cisco, mint a PPTP
- L2TP (Layer 2 Tunneling Protocol)
  - IETF standard , kombinálja a fenti kettő funkcióit
- IPSec (Internet Protocol Security)
  - VPN implementálásához használt nyílt szabvány
  - A hálózati rétegben működik

IPsec

- Layer 3 security (RFC 2401)
  - Transzparens az applikációknak (nem kell „támogatniuk”)
- Protokollok és algoritmusok halmaza, ami a hálózati rétegben nyújt adatbiztonságot
- Különféle komponensekből áll:
  - Security associations (SA)
  - Authentication headers (AH)
  - Encapsulating security payload (ESP)
  - Internet Key Exchange (IKE)
- VPN csatornán létrehozott „security context” az ISAKMP-n keresztül támogatott (Internet Security Association and Key Management Protocol)

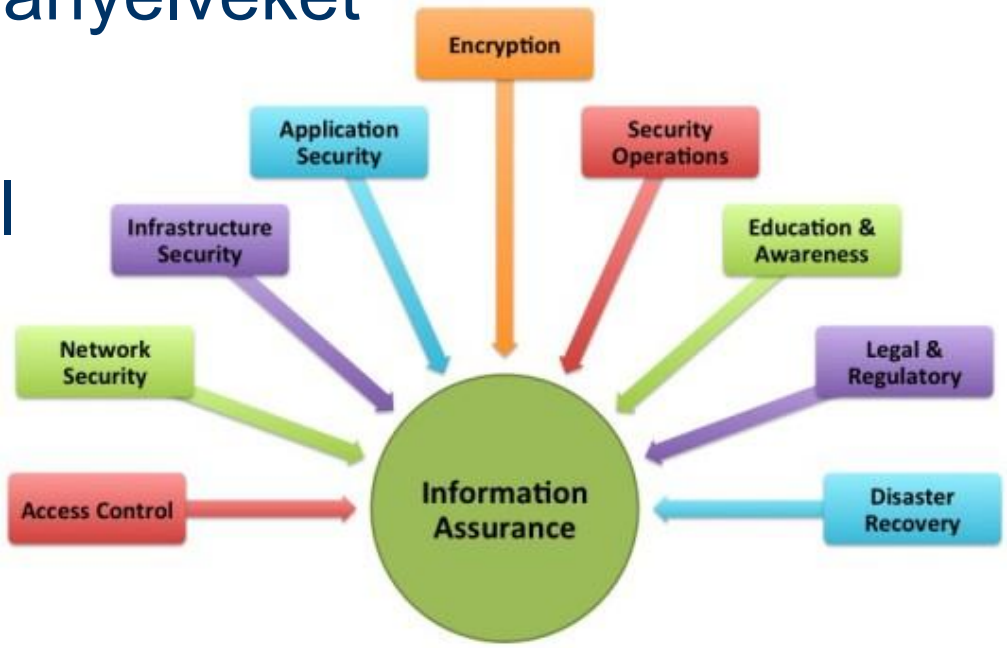
Az IPsec előnyei

- Confidentiality
  - Az adatok titkosításával
- Integrity
  - Az átvitel mindkét végén lévő router kiszámolja az adat checksum-ját vagy hash értékeit
- Authentication
  - Aláírások és bizonyítványok
  - A meglévő IP infrastruktúrát használja, meghagyva annak minden képességét

Összefoglalás

Konklúziók

- **Confidentiality / Integrity / Availability**
- Létzezzen biztonsági stratégia
- …és tartsuk be az irányelveket
- Az ár-érték arány figyelembe vételével



Köszönöm a figyelmet!

Pal Varga
pvarga@tmit.bme.hu