HÁLÓZATI RENDSZEREK
ÉS SZOLGÁLTATÁSOK
TANSZÉK

Bevezetés az IT biztonságba

VIHIBB01 – Kódolás és IT biztonság (2020)

Dr. Buttyán Levente

CrySyS Lab, BME
buttyan@crysys.hu

www.crysys.hu

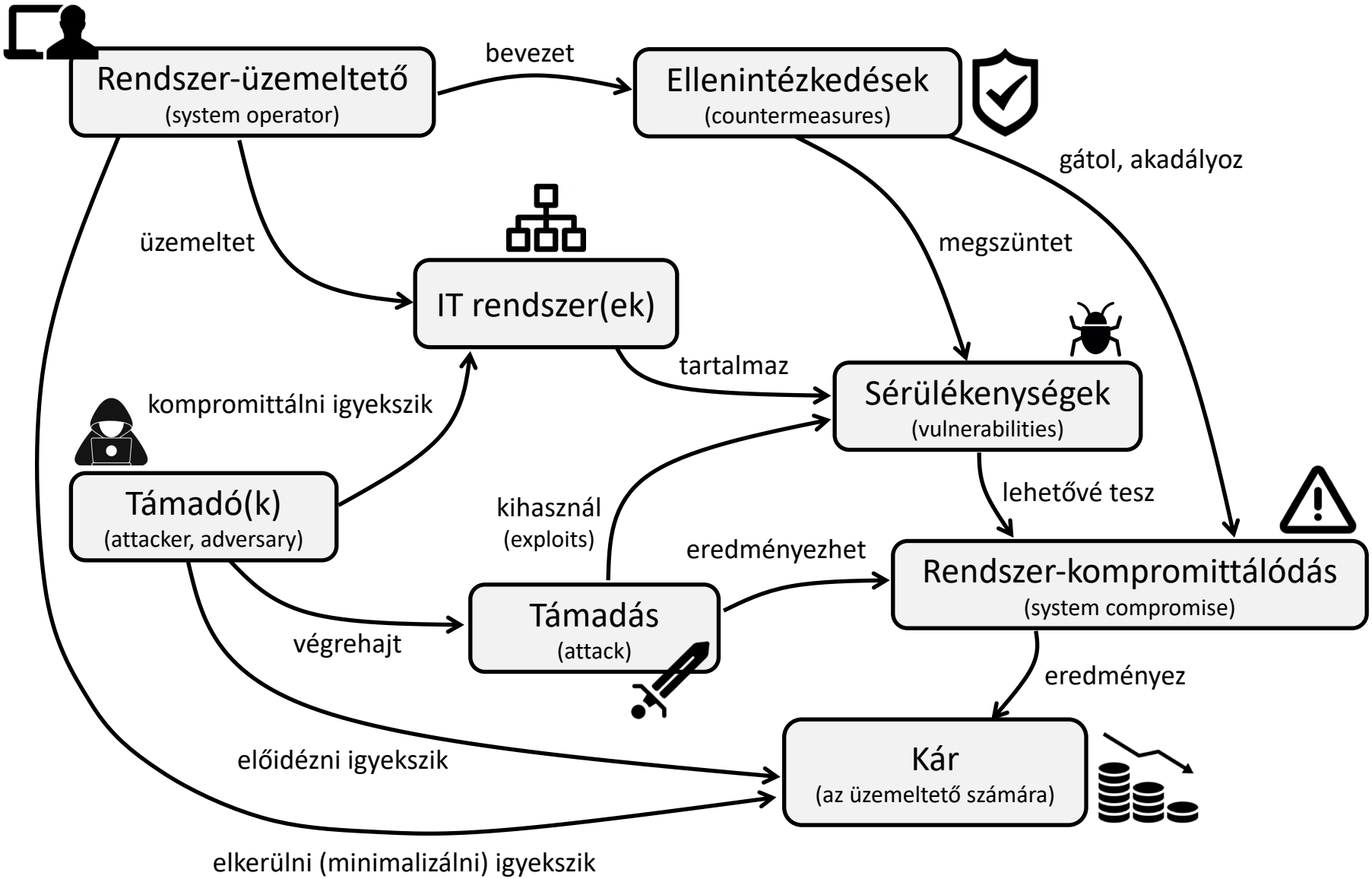
MŰEGYETEM 1782

Tartalom

- Az IT biztonság témakör főbb fogalmainak és összefüggéseinek bevezetése
- A biztonsági kockázatot befolyásoló tényezők vizsgálata
  - Támadók
  - Sérülékenységek, kihasználható gyengeségek
  - Biztonsági mechanizmusok, ellenintézkedések
- A biztonsági incidenskezelés alapjainak bevezetése

Mivel foglalkozik az IT biztonság?

Színtér, szereplők, alapkonfliktus



A kompromittálódás fajtái

- A rendszer szolgáltatásaihoz vagy erőforrásaihoz történő illetéktelen hozzáférés, azok illegitim módon történő használata, módosítása, vagy elérhetetlenné tétele

  Példák:

  – Illegitim belépés egy legitim felhasználó fiókjába
  – Számítógép kártékony programmal (malware) történő megfertőzése
  – Kiszolgáló (szerver) elárasztása nagy mennyiségű kéréssel, ami annyira leterheli, hogy nem tud legitim kéréseket kiszolgálni (Denial-of-Service, DoS)

- A rendszerben tárolt, feldolgozott, vagy továbbított információ bizalmasságának, integritásának, vagy rendelkezésre állásának sérülése

  Példák:

  – Jelszó vagy üzleti titok kiszivárgása
  – Adatbázisban tárolt adatok illegitim módosítása
  – Háttértáron tárolt adatok zsaroló vírus által történő rejtjelezése

A CIA triád

C = Confidentiality (bizalmasság)

- az **információhoz** történő jogosulatlan hozzáférés megakadályozása

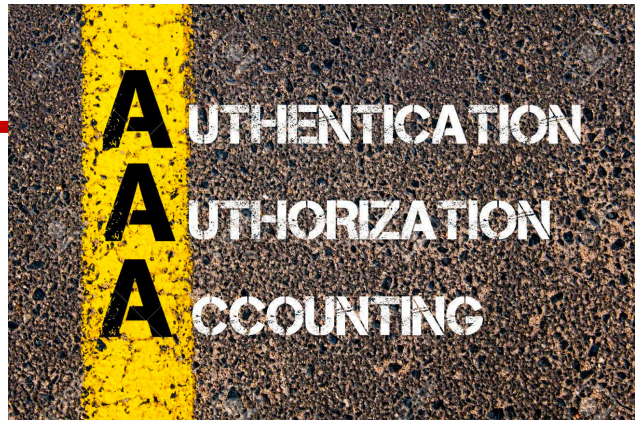
I = Integrity (integritás)

- az **információ** jogosulatlan módosításának megakadályozása

A = Availability (rendelkezésre állás)

- az **információ** elérhetőségének biztosítása az arra jogosultak számára

AAA



Authentication (hitelesítés)

- szolgáltatáshoz vagy erőforráshoz történő hozzáférés kezdeményezője identitásának ellenőrzése (ki akar hozzáférni?)

Authorization, access control (engedélyezés, hozzáférés-vezérlés)

- szolgáltatáshoz vagy erőforráshoz történő hozzáférés engedélyezése
- függhet a hozzáférést kezdeményező identitásától, a hozzáférés jellegétől (pl. írás, olvasás), és egyéb körülményektől (pl. idő)

Accounting (felelősségre vonhatóság)

- a rendszerhez történt hozzáférések, az elvégzett műveletek utólagos visszakereshetőségének, ellenőrizhetőségének, a hozzáférést végző entitás azonosíthatóságának és felelősségre vonhatóságának lehetősége

Szándékos vs. véletlen

- A kompromittálódás mindig valamilyen szándékos tevékenység (támadás) eredménye
- A véletlen hibákból, természeti katasztrófákból származó nem kívánatos állapot (failure) nem kompromittálódás

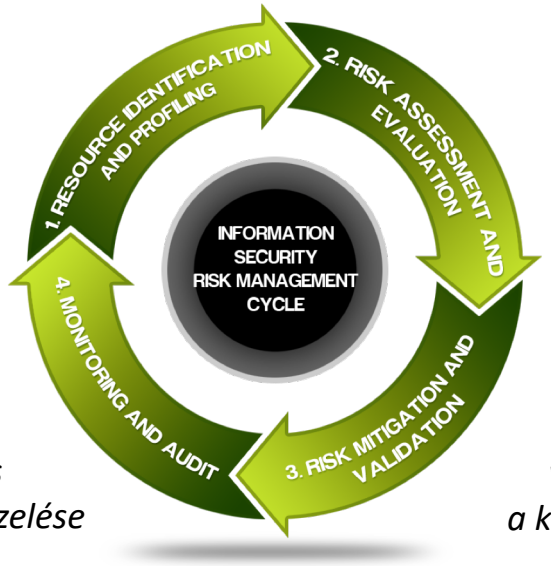
  Példák:

  - A háttértár fizikai meghibásodása miatt az adatok elérhetetlenek
  - Kommunikációs hiba miatt egy üzenet tartalma módosul
  - A rendszer tűzvészben fizikailag megsemmisül
- Bár az eredményük hasonló lehet, a szándékos támadások és a véletlen hibák kezelése különböző technikákat igényel
  - szándékos támadások → biztonság (security), megbízhatóság (trustworthiness)
  - véletlen hibák → hibatűrés (fault tolerance), megbízhatóság (reliability), (üzem)biztonság (safety)

Az üzemeltető nézőpontja

biztonság = kockázat (risk) menedzsment

- a kockázat a sikeres támadásból eredő veszteség várható értéke
- a kockázat általában nem eliminálható teljesen, mert minden elképzelhető támadás megakadályozása túl drága (még ha egyáltalán lehetséges is volna)
- az üzemeltető célja tehát a kockázat minimalizálása adott költségvetés (budget) mellett
- ezt nevezzük kockázat-menedzsmentnek, ami egy ciklikus folyamat...



Security operations

biztonsági mechanizmusok bevezetése és használata támadások megelőzése vagy észlelése céljából, illetve a sikeres támadásokból származó incidensek kezelése

Security engineering

biztonsági mechanizmusok tervezése és implementációja, vagy kiválasztása és integrációja a kockázat csökkentése érdekében

A kockázatot befolyásoló tényezők

Risk = Likelihood x Impact
(of attacks)

- Impact:
  - a sikeres támadásból bekövetkező potenciális veszteség
    - » közvetlen veszteség (pl. bevétel kiesés, a helyreállítás költségei)
    - » közvetett veszteség (pl. jó hírnév elvesztése, bizalom csökkenése)

- Likelihood:
  - a sikeres támadás valószínűsége, mely függ
    - » a támadótól (motiváció, szándék, lehetőség, képesség, erőforrások)
    - » a rendszer sérülékenységeitől (kihasználható gyengeségek)
    - » az alkalmazott ellenintézkedésektől (biztonsági mechanizmusok)

„ … ha ismerjük az ellenséget és ismerjük magunkat is, akkor száz csatában sem jutunk veszedelembe; ha azonban nem ismerjük az ellenséget, csak magunkat ismerjük, akkor egyszer győzünk, másszor vereséget szenvedünk; és ha sem az ellenséget, sem magunkat nem ismerjük, akkor minden egyes csatában feltétlenül végveszély fenyeget bennünket.”

— Szun Ce, *A háború művészete*

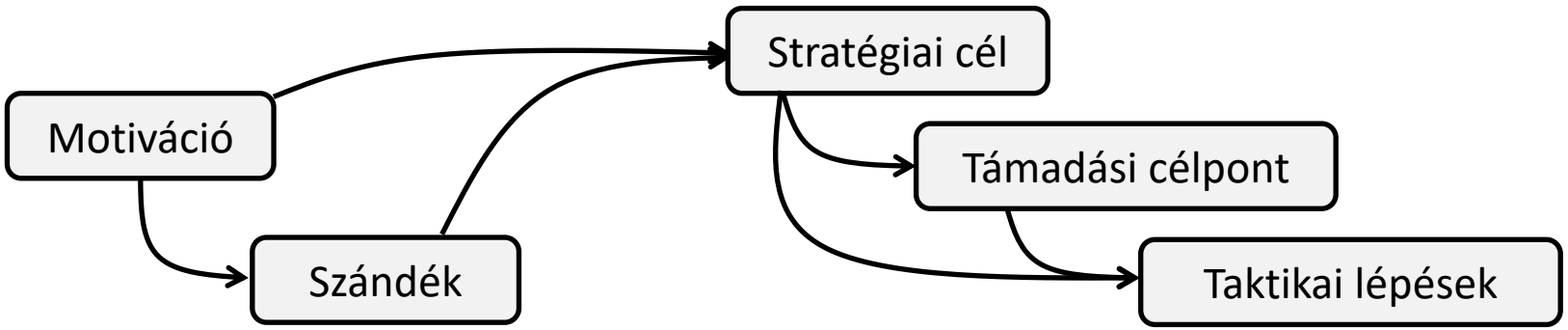
A támadó

A támadó jellemzői

- Motiváció
- Szándék (intent)
- Lehetőség (opportunity)
- Képességek
  - Információszerző képesség
  - Műszaki tudás, szakértelem
  - Megtévesztési képességek
- Erőforrások

Motivációk

- Gazdasági haszonszerzés
- Politikai célok elérése
- Társadalmi üzenet közvetítése
- Vallási üzenet közvetítése, cél elérése
- Bosszú
- Erő, képesség demonstrációja
- ...



Információszerző képesség

- A támadás sikere nagy mértékben függ attól, hogy mennyi és milyen jellegű információval rendelkezik a támadó a megtámadott rendszerről
- Az információszerzés megelőzheti magát a támadást, és folytatódhat a támadás alatt is
- A támadó számára hasznos információk:
  - a rendszer általános felépítése, elérhető szolgáltatásai, hardver és szoftver komponensei és azok konfigurációja, a hálózati topológia, az alkalmazott protokollok, ...
  - az alkalmazott biztonsági mechanizmusok (pl. tűzfalak, behatolás detektáló rendszerek, anti-vírus szoftverek, ...)
  - a rendszer és az alkalmazott biztonsági megoldások ismert sérülékenységei
  - kik a rendszer felhasználói, milyen jogosultságokkal rendelkeznek?
  - ...

Műszaki tudás, szakértelem

- A támadó szakértői tudása segítségével transzformálja a megszerzett információt sikeres támadássá
- A műszaki tudás, szakértelem az információszerzést is segítheti
- A támadói szakértelem szintjei:
  - alapvető műszaki és informatikai ismeretek (hardver; operációs rendszerek; hálózati technológiák, protokollok; elosztott rendszerek; alkalmazások; ...)
  - ismert sérülékenységek és támadási módszerek, eszközök ismerete; IT biztonsági szakértelem
  - új sérülékenységek felfedezésének, új támadási módszerek és eszközök kifejlesztésének képessége

Erőforrások

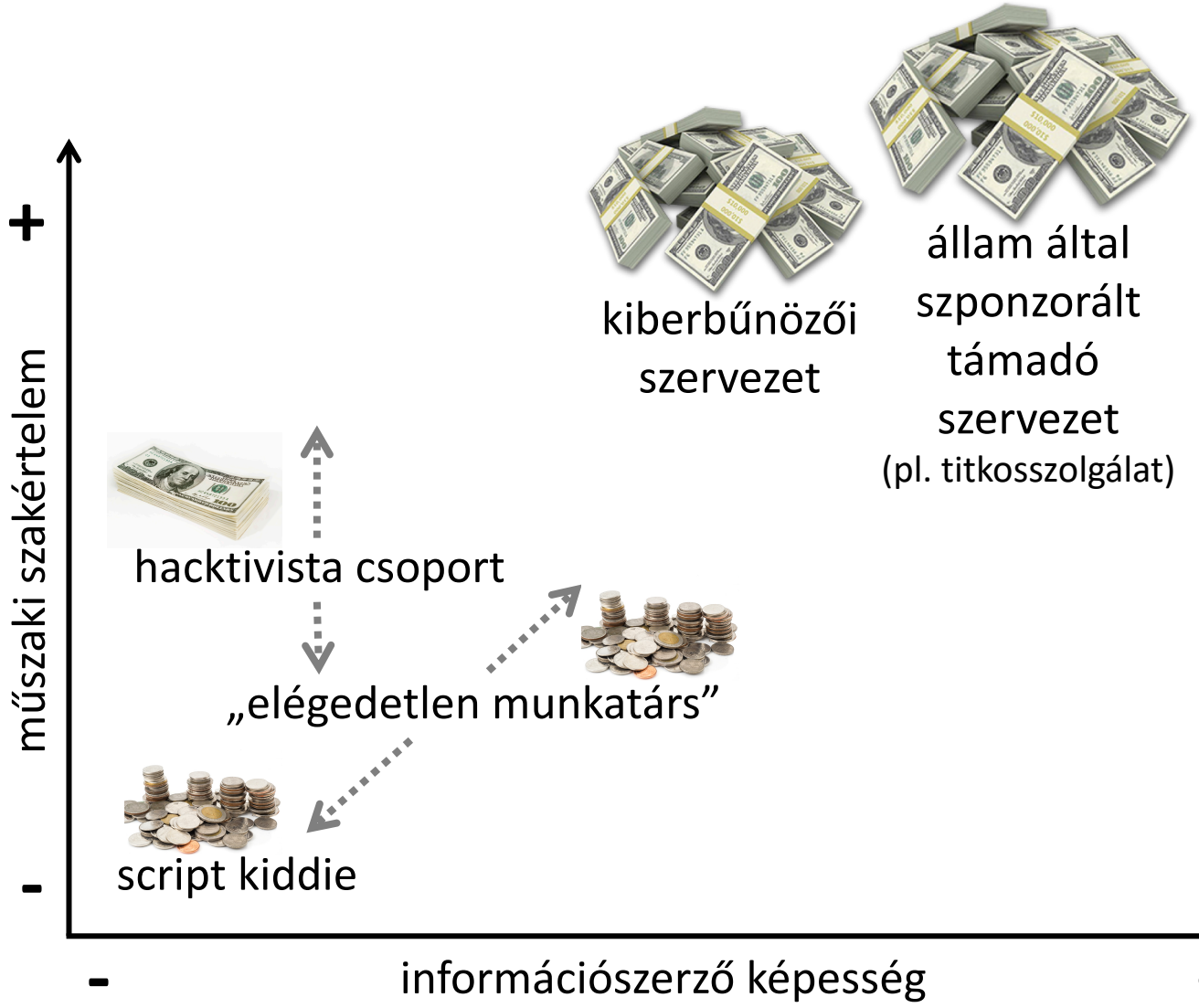
erőforrás = pénz

- szabadon konvertálható információvá, tudássá, szakértelemmé, emberi erőforrássá, ...

Példák:

- Információszerző képesség növelése
  - » megvesztegetés, zsarolás
  - » műszaki dokumentációk megvásárlása
  - » kifinomult megtévesztési módszerek (social engineering) támogatása
  - » fejlett OSINT, SIGINT módszerek alkalmazásának lehetősége
- Műszaki tudás, szakértelem növelése
  - » szakértők szerződtetése
  - » saját kompetenciák növelése képzéssel, tréninggel
- Speciális támadói képességek növelése
  - » 0-day sérülékenységeket kihasználó exploit-ok vásárlása
  - » fejlett kripto-analízis eszközök használata (kódfeltörés, hamisítás)
  - » nagy számítási kapacitás bérlése

Tipikus támadó profilok (modellek)



Kiberbűnözői szervezet

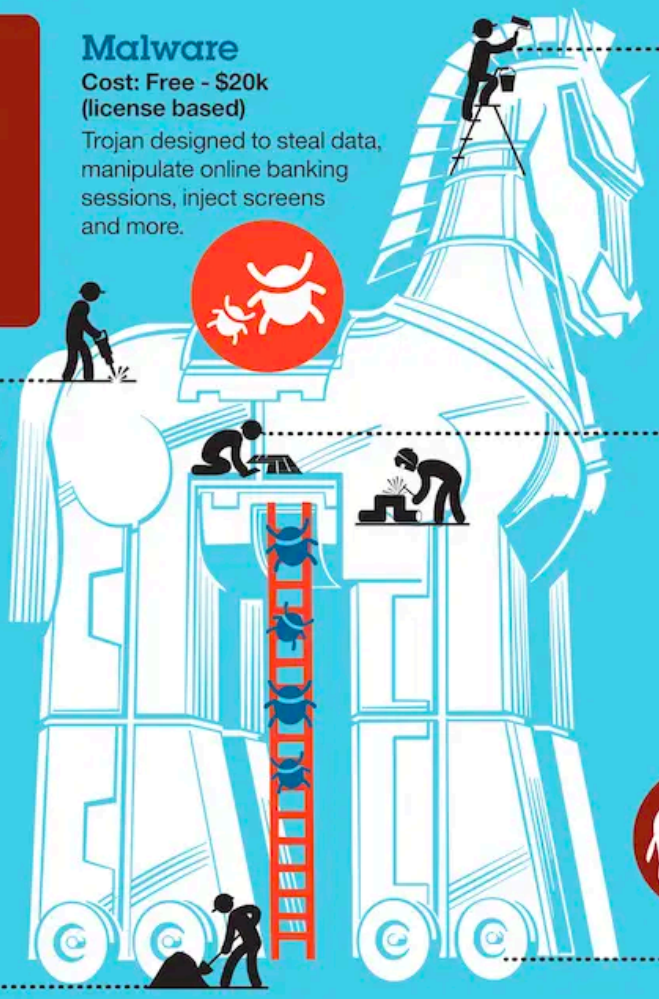
- Legnagyobb probléma ma egy átlagos felhasználó vagy cég számára
- Motiváció: gazdasági haszonszerzés
- Információszerző képesség: **potenciálisan fejlett**
  - műszaki megoldások (spyware telepítése; szerverek, felhasználói fiókok feltörése)
  - megtévesztés (phishing, social engineering)
- Műszaki tudás, szakértelem: **potenciálisan fejlett**
- Erőforrások: **potenciálisan gazdag**
  - „szakértők, specialisták” alkalmazása
  - információk és eszközök (pl. exploit-ok, malware) vásárlása
  - komoly háttér infrastruktúra fenntartása
  - térben és időben kiterjedt támadó kampányok futtatása

Cybercriminal Ecosystem

IBM

Cybercrime is no longer a one man operation. Within the cybercrime underground an attacker can find a wealth of tools and services that can be bought or rented to facilitate different aspects of the attack lifecycle.*

Fraud as a service is constantly changing and adapting to new security solutions, offering end to end technologies, multiple SLA levels and low prices for everything a cybercriminal might need.



Malware

Cost: Free - $20k (license based)

Trojan designed to steal data, manipulate online banking sessions, inject screens and more.

Exploit Kits

Cost: $2K (monthly rental)

Toolkits designed to exploit system and software vulnerabilities resulting in a malicious download.

Droppers

Cost: Free - $10K

Software designed to download malware to an infected device, evading antivirus and research tools.

Infrastructure

Cost: $50 - $1,000 (Rental per month)

Hosting services for malware update, configuration and command and control servers. Some are fast flux or TOR based.

Money Mules

Cost: Up to 60% of account balance

A person who receives thestolen money from a hacked account and transfers the funds via an anonymous payment service to the mule operator.

Spammers

Cost: $1 - $4 per 1000 emails

Spam botnet operators that spread emails with attachments or links leading to a Trojan infection.

* This infographic shows one possible scenario of a cybercriminal attack lifecycle. Prices for this scenario are estimates.

Állam által szponzorált támadó szervezet

- Legnagyobb probléma ma kormányzatok és bizonyos cégek számára
- Motiváció: politikai vagy gazdasági célok elérése
  - világos stratégiai célok (kémkedés vagy szabotázs)
- Információgyűjtő képesség: **fejlett**
  - fejlett megfigyelő (surveillance) eszközök (pl. telefonra telepítve)
  - „hagyományos” lehallgatás, információszerzés (SIGINT)
- Műszaki tudás, szakértelem: **fejlett**
  - komplex K+F és tréning programok
- Erőforrások: **gazdag**
  - „szakértők, specialisták” alkalmazása vagy kiképezése
  - információk és eszközök (pl. exploit-ok, malware) vásárlása
  - komoly háttér infrastruktúra fenntartása
  - körültekintő tervezés, hosszú élettartamú, célzott támadások
- Példák:
  - PLA Unit 61398 (Kína)
  - TAO (USA)

Célzott támadások

- célzott = az áldozat kiszemelt, nem véletlen választott
  - az áldozat lehet egy cég, szervezet, egyén, vagy egyének kisebb csoportja
- Testreszabott támadó eszközök és behatolási technikák
  - spear phishing vagy fejlett social engineering
  - támadás szerződéses partneren, beszállítón keresztül
  - több különböző exploit alkalmazása (gyakran 0-day vagy nagyon friss)
- Időben kiterjedt (perzisztens), mégis rejtve maradó (stealthy) működés
  - anti-vírus és behatolás detektáló eszközök kijátszása
  - körültekintő tervezés és tesztelés
- Erőforrásokban gazdag háttér
  - katonai egységek, titkosszolgálatok
  - nagy cégek (célzottan versenytársakat támadnak)

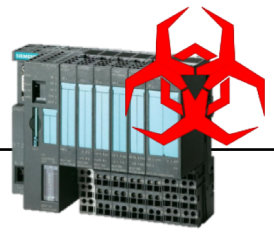
Stuxnet (2010. június)

- “the Most Menacing Malware in History” (Kim Zetter, Wired)
- Cél: natanz-i uránium dúsító üzem Iránban
- Forrás: USA és/vagy Izrael (feltételezés)
- Motiváció: Irán atomprogramjának szabotálása (képesség demonstrációja)
- kifinomult malware, több 0-day exploit, hamis digitális aláírás

WinCC PLC menedzsment szoftvert futtató PC

A Stuxnet megfertőzte a PC-t, átvette a PC és a PLC-k közötti kommunikáció irányítását, módosította az üzeneteket, ...

Az uránium centrifugák forgását vezérlő PLC



... és átprogramozta a PLC-ket. A módosított program helytelenül vezérelte a centrifugák forgását.

Uránium dúsító centrifigák

A helytelen vezérlés fizikailag tönkretette a centrifugákat.

Duqu (2011. október)

Home / News & Blogs / Zero Day

Hungarian Lab found Stuxnet-like Duqu malware

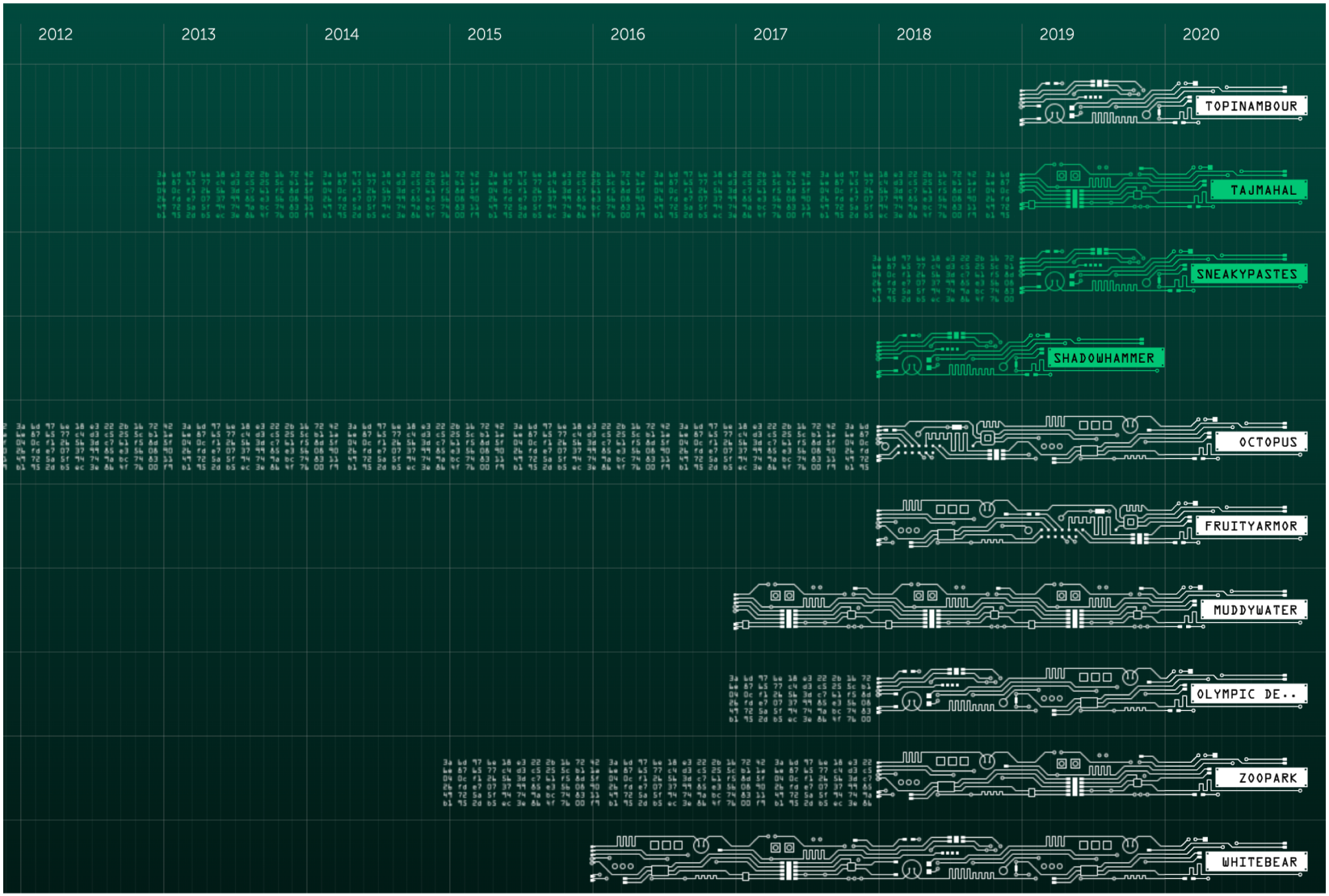
By Ryan Naraine | October 21, 2011, 9:11am PDT

Summary: *The Laboratory of Cryptography and System Security (CrySyS) in Hungary confirmed its participation in the initial discovery of the Duqu cyber-surveillance Trojan.*

A security lab attached to the Budapest University of Technology and Economics in Hungary has come forward as the mystery outfit that found the Stuxnet-like "Duqu" cyber-surveillance Trojan.

According to Symantec's initial report on Duqu [PDF], the malware sample was passed along by an unnamed "research lab with strong international connections," a statement that led to speculation about the origins and intent of the threat.

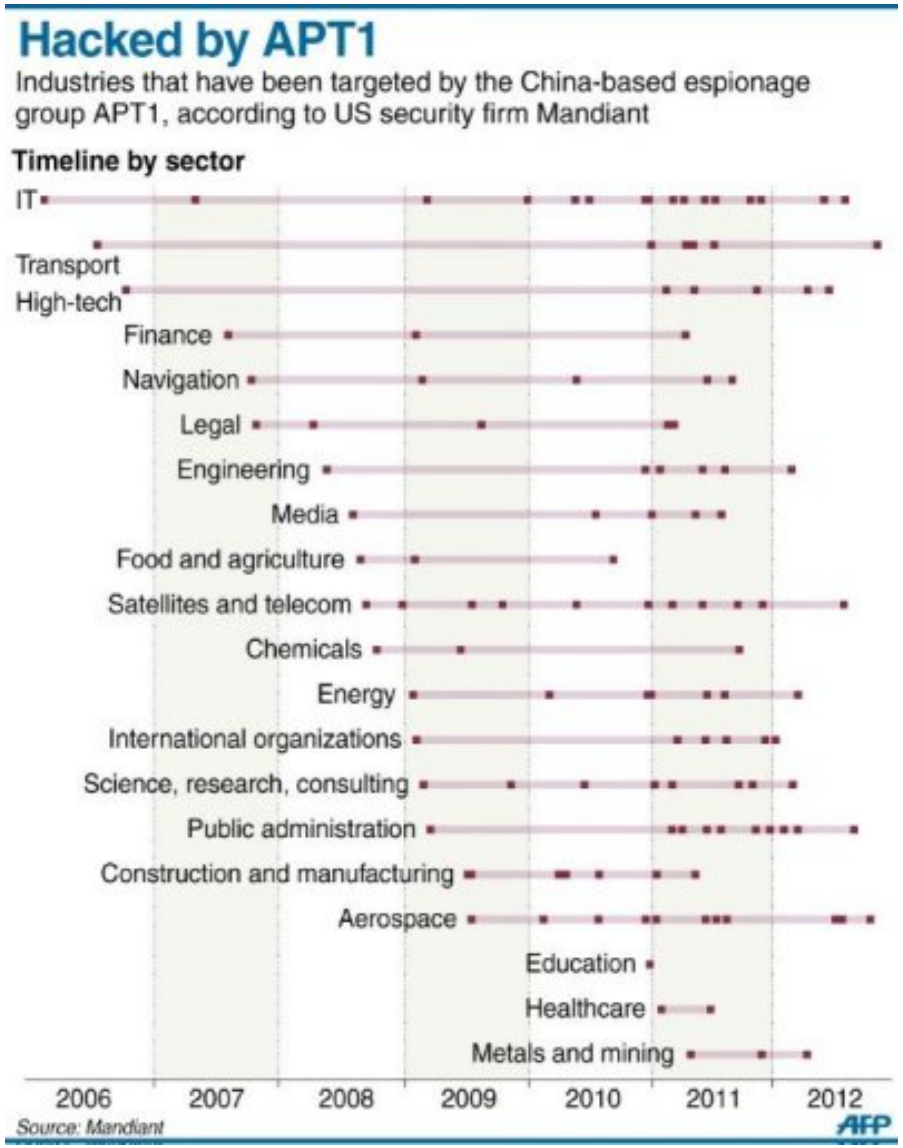
Néhány aktuális példa



https://apt.securelist.com/

PLA Unit 61398 (aka APT1)

- Közel 150 áldozat 7 év alatt
- Átlagosan 356 napig volt bent az áldozatok rendszerében
- Az azonosított székhely mérete a szervezet méretét is jelzi: potenciálisan több száz fő!



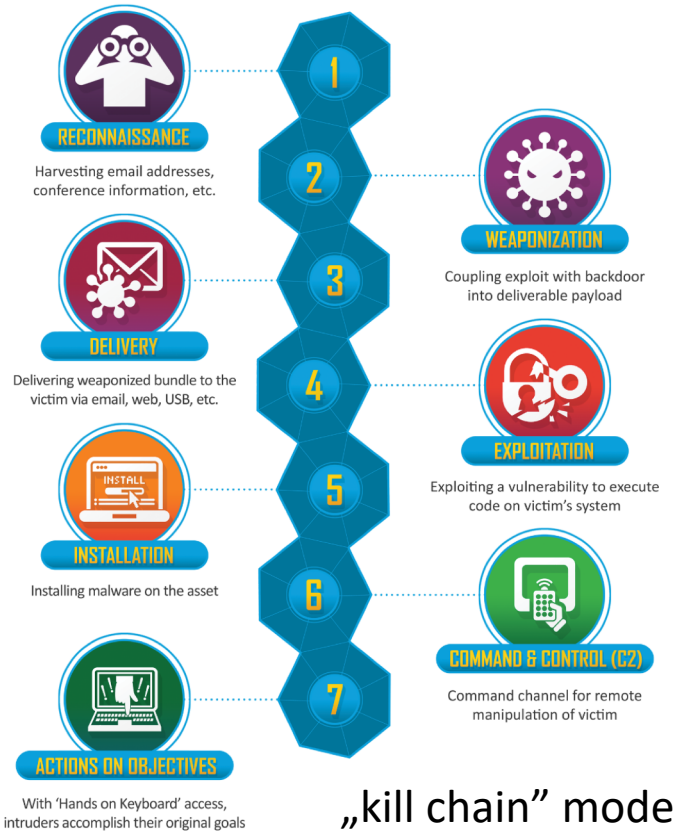
Office of Tailored Access Operations (TAO)

- „a számítógépes hadviselés egyik információgyűjtő egysége az NSA-n belül”
- „feladata a külföldi szervezetek által működtetett számítógépes hálózatok azonosítása, megfigyelése, az azokba való behatolás és azokból információszerzés.”
- „az adott hálózat védelmi rendszerét, testre szabott, az adott feladatra koncentráló módszerrel törik fel”
- „több mint 1000 katonai és polgári hackert, információ-elemzőt, és más számítógépes szakembereket foglalkoztat”
- „2013-ig valószínűleg összesen 85 ezer számítógépet fertőzött meg, közöttük demokratikusan megválasztott kormányok számítógépes rendszereit is”

Forrás: https://hu.wikipedia.org/wiki/Tailored_Access_Operations

Támadás

- A támadás az a folyamat vagy tevékenység, mely során a támadó kompromittálja a támadott rendszert, annak sérülékenységeit kihasználva
- A támadás általában egy komplex folyamat/tevékenység
- A támadás felépítésének, az alkalmazott technikáknak az ismerete elengedhetetlen a támadás megakadályozását célzó biztonsági mechanizmusok tervezéséhez



„kill chain" modell

Sérülékenységek

A sérülékenységek fajtái

- **Műszaki (logikai) –** tervezési és implementációs hibák a rendszert alkotó hardver és szoftver komponensekben, a komponensek közötti interfészekben, a komponensek között használt protokollokban
- **Fizikai –** olyan gyengeségek, melyek kihasználása fizikai hozzáférést eredményezhet a rendszerhez, vagy annak valamely komponenséhez (pl. folyosón elhelyezett router)
- **Üzemeltetési –** kihasználható gyengeségek a rendszer üzemeltetése során alkalmazott eljárásokban (pl. alapértelmezett jelszó megváltoztatása nincs kikényszerítve)
- **Személyi –** az üzemeltető személyzetet, alkalmazottakat, szerződéses partnereket érintő gyengeségek (pl. biztonságtudatosság hiánya, szakértelem hiánya, lefizethetőség, megzsarolhatóság)

A sérülékenységek okai

- A rendszerek nagy komplexitása
  - ami bonyolult, abban több a hibalehetőség
- Alkalmas tervezési, implementációs, ellenőrzési és tesztelési módszerek hiánya vagy hiányosságai
  - pl. a javasolt formális ellenőrzési módszerek nem skálázódnak
  - pl. a tesztelés sosem lehet kimerítő a gyakorlatban használt rendszerméretek és –komplexitás mellett
- Korlátozott erőforrások
  - pénz
  - idő
  - szakértelemmel bíró emberi munkaerő
- Rossz feltételezések használata a tervezés vagy az üzemeltetés során
  - pl. egy adott támadó típus, támadási módszer figyelmen kívül hagyása
- Gyenge minőségű specifikáció az implementáció számára
  - következményként a szakértő tervező helyett a kevésbé hozzáértő programozó hoz tervezési döntéseket

Publikusan ismert sérülékenységek

- Olyan (általában műszaki jellegű) sérülékenységek, melyeket nyilvánosságra hoztak, így bárki (beleértve a támadót) számára ismertek lehetnek
- Sérülékenységek rutinszerűen kerülnek így nyilvánosságra, általában egy kontrollált folyamaton (responsible disclosure procedure) keresztül
- A publikus sérülékenységek egyedi azonosítót kapnak
  - CVE ID – Common Vulnerabilities and Exposures (cve.mitre.org)
- A publikus sérülékenységekkel kapcsolatos információkat publikus sérülékenység-adatbázisokban tárolják
  - strukturált, kereshető
  - példa: US National Vulnerability Database (nvd.nist.gov)
- A nyilvánosságra hozatal lehetővé teszi az ismert sérülékenységekből származó problémák eliminálását, mely önmagában drasztikusan csökkenti a biztonsági kockázatot
  - Sajnos vannak olyan rendszerek, ahol az ismert sérülékenységek eliminálása lassú vagy nem is lehetséges, más megfontolások, szabályok miatt

Zero-day sérülékenységek

- Olyan sérülékenységek, melyek csak a támadó számára ismertek
  - vannak olyan cégek, melyek abból élnek, hogy sérülékenységeket keresnek és adnak el potenciális támadóknak (pl. bűnözőknek, kormányzatoknak)
- A 0-day sérülékenységek nagy problémát jelentenek, mert nem lehet rájuk hatékonyan felkészülni, nem lehet ellenük védelmet kialakítani
- Szerencsére a 0-day sérülékenységek ritkák és drágák, ezért főként célzott támadásokban használják őket, ahol
  - a támadás sikere nagyon fontos
  - a támadás észlelésének (és így a sérülékenység napvilágra kerülésének) esélye viszont elég alacsony

Ellenintézkedések

Az ellenintézkedések fajtái

- **Műszaki (logikai) –** a hosztokon és a hálózatokban használt biztonsági mechanizmusok, megoldások
  - pl. tűzfalak, anti-vírus szoftverek, jelszavas hitelesítés, kritpográfiai algoritmusok és protokollok, ...
- **Fizikai –** fizikai védelmet biztosító mechanizmusok
  - pl. zárak, kerítések, biztonsági őrök, bontásellenálló (tamper resistant) hardver elemek, ...
- **Üzemeltetési –** a rendszer üzemeltetésével és a személyzet menedzsmentjével kapcsolatos szabályzatok és eljárásrendek
  - pl. jelszócserére és –erősségre vonatkozó szabályozás, rendszeres biztonsági tesztelés, ...
  - pl. felvétel és elbocsátás során alkalmazott eljárások, kötelező szabadság, ...
- **Személyi –** a személyzet biztonságtudatosságának, megbízhatóságának, lojalitásának növelését célzó mechanizmusok
  - pl. tréning, gyakorlat, jó fizetés, vonzó munkakörülmények, ...

Műszaki (logikai) biztonsági mechanizmusok

Megelőzést célzó mechanizmusok ⟷ **Észlelést célzó mechanizmusok**

Példák:

Rejtjelezés,
Hitelesítés,
Hozzáférés-vezérlés,
Address Space Layout Randomization (ASLR),
Control Flow Integrity (CFI),
Víruskeresés (scanning),
Tűzfal,
Network Intrusion Prevention Systems (IPS),
Bontásellenálló borítás,
Biztonsági képzés,
…

Példák:

Üzenet integritásvédő ellenőrzőösszeg,
Rootkit detekció,
Network Intrusion Detection Systems (IDS,)
log analízis,
Security Information and Event Management (SIEM),
“tamper evident” borítás,
…

Kockázat menedzsment

- A kockázat minimalizálása adott költségvetés mellett
- Tipikusan vizsgálandó kérdések:
  - Milyen értékek, vagyonelemek vannak a rendszerben?
  - Kik lehetnek plauzibilis támadók?
  - Milyen ismert és potenciális sérülékenységek vannak a rendszerben?
  - Mekkora az esélye annak, hogy ezeket a sérülékenységeket a plauzibilis támadók sikeresen ki tudják használni?
  - Mekkora a sikeres támadásokból származó potenciális veszteség?
  - Mik a legnagyobb kockázatú fenyegetések?
  - Milyen ellenintézkedésekkel lehet a kockázatot hatékonyan elfogadható szintre csökkenteni?
- Az eredmény mindig valamilyen kompromisszum:
  - biztonság ←→ szolgáltatások, feature-ök, használhatóság, hatékonyság, ár...
  - Mindig lesz pozitív maradvány-kockázat, a kérdés, hogy elfogadható-e számunkra annak mértéke

Biztonsági incidensek kezelése

Biztonsági incidens

- Biztonsági incidens alatt egy sikeres támadásból származó, ***észlelt*** rendszer-kompromittálódást értünk

  Példák:

  - a Facebook fiókunkat feltörék (hogyan észlelhetjük?)
  - a fájljainkat rejtjelezte egy zsaroló virus (hogyan észlelhetjük?)
  - a webszerverünk le van terhelve, nem tudja kiszolgálni a legitim kéréseket (hogyan észlelhetjük?)

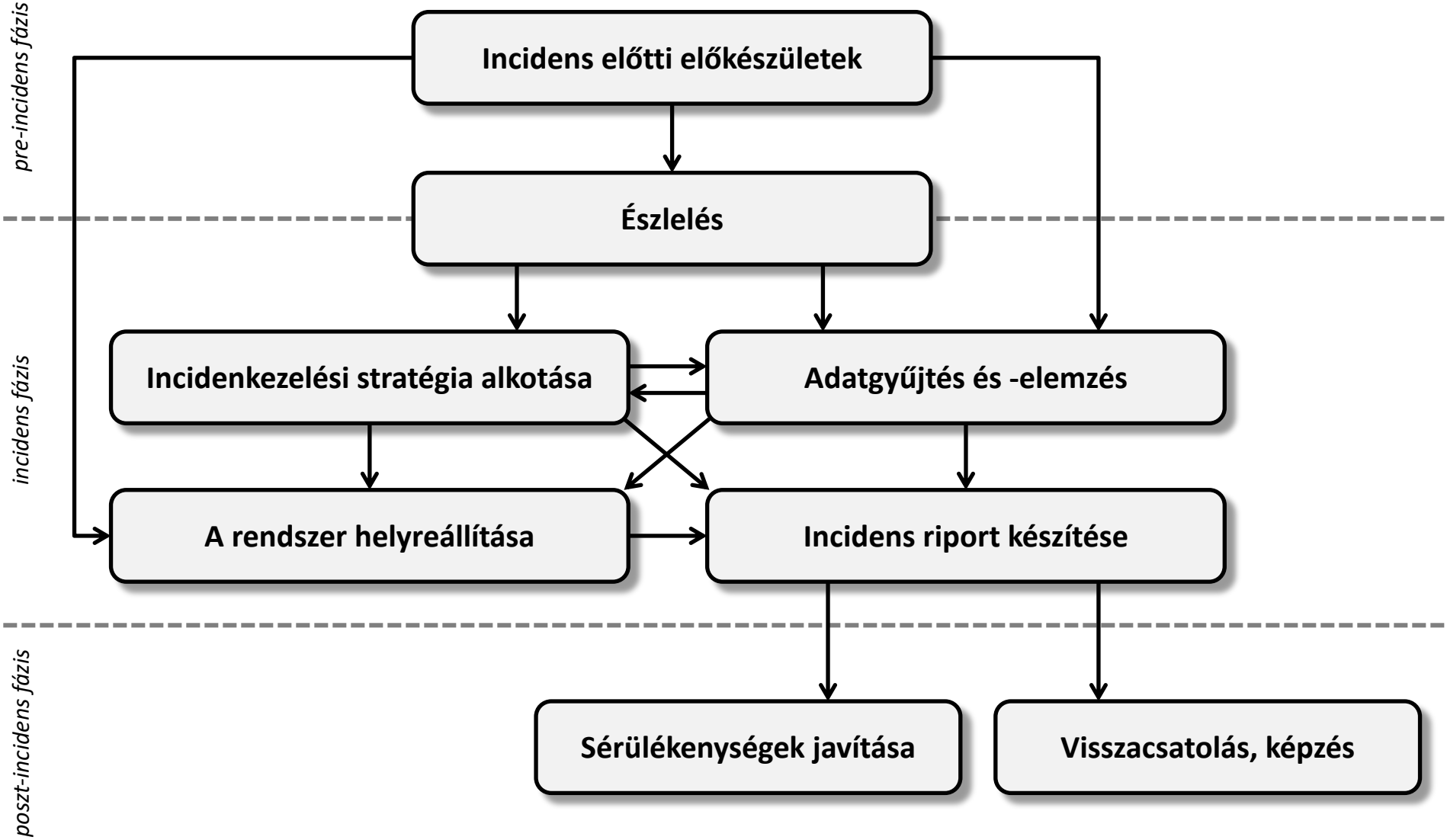
- A biztonsági incidenseknek komoly negatív hatása lehet az üzemeltetőre (cég, szervezet, egyén) nézve
  - közvetlen anyagi veszteség
  - jó hírnév elvesztése
  - személyes értékek (pl. pótolhatatlan személyes fotók) elvesztése

- Ezért a hatásos és hatékony incidenskezelés fontos feladat

Az incidenskezelés céljai

- Üzletfolytonosság megszakadásának minimalizálása
  - A kompromittálódás behatárolása (containment)
  - A rendszer mielőbbi helyreállítása eredeti állapotába
- Hasonló incidensek jövőbeli bekövetkezésének megelőzése
  - Az incidens részleteinek megértése elemzés által
  - Az incidensben szerepet játszó sérülékenységek eliminálása
- Igaszságügyi eljárás, nyomozás támogatása
  - Bizonyítékok gyűjtése, tárolása igazságügyi eljárásban felhasználható módon
  - Részletes incidens-elemzés és -riport

Az incidenskezelés lépései



→ bemenet vagy befolyás

Összefoglalás

- Az IT biztonság a szándékos támadásból származó rendszer-kompromittálódás megelőzésével, észlelésével, illetve kezelésével foglalkozik
- A rendszer üzemeltetője szempontjából a biztonság lényegében kockázat menedzsmentet jelent
  - A biztonság tehát egy kedvező (kellően védett) állapot fenntartását célzó, ciklikus folyamat
- A kockázat a sikeres támadásból származó várható veszteség, amit az alábbi tényezők befolyásolnak:
  - a potenciális veszteség mértéke
  - a támadást kivitelező támadó jellemzői (motiváció, képességek, erőforrások)
  - a rendszer sérülékenységei, melyeket a támadó kihasználhat
  - az alkalmazott ellenintézkedések, melyek a támadó dolgát nehezítik
- A gyakorlatban a kockázat sosem eliminálható teljesen, a cél, hogy a maradvány kockázat elfogadható szintű legyen
- Fel kell készülni arra, hogy minden védekezés ellenére is lesznek sikeres támadások, melyek észlelése biztonsági incidenshez vezet
- Az incidensek hatásos és hatékony kezelése fontos üzemeltetői feladat

Ellenőrző kérdések

Alapfogalmak, kockázat menedzsment

- Milyen jellegű problémákkal foglalkozik az IT biztonság?
- Mi az a támadó, és miért lehetnek támadások sikeresek egy rendszer ellen?
- Hogyan védekezhet a rendszer üzemeltetője a támadások ellen?
- Mit értünk rendszer-kompromittálódás alatt?
- Definiálja az alábbi fontosabb fogalmakat:
  - Bizalmasság, integritás, rendelkezésre állás (CIA)
  - Hitelesítés, engedélyezés, felelőségre vonhatóság (AAA)
  - Security engineering, security operations
- Hogyan definiáljuk a biztonsági kockázatot?
- Mik a kockázatot befolyásoló tényezők?
- Mik a kockázat menedzsment főbb megválaszolandó kérdései?
- Mi az a maradvány-kockázat? Miért nem csökkenthető nullára?

Támadók

- Milyen tényezők alapján jellemezhetők a támadók?
- Milyen információkat érdemes megszerezni támadás előtt?
- A támadó műszaki képességeinek, szakértelmének milyen szintjei lehetnek?
- Miért fontos az anyagi erőforrás a támadó számára?
- Milyen tipikus támadó profilok vannak? Minden profil esetén foglalja össze az adott támadó típus motivációját, képességeit, és erőforrásait!
- Milyen szolgáltatások érhetők el a kiberbűnözők számára az underground piacon?
- Mik a célzott támadás jellemzői?
- Mi az a Stuxnet, és miért fontos?
- Mi az a „kill chain” modell?

Sérülékenységek, ellenintézkedések, incidensek

- Milyen típusú sérülékenységek lehetségesek IT rendszerekben?
- Mik a műszaki jellegű sérülékenységek okai?
- Hogyan kezeljük a publikusan ismert sérülékenységeket?
- Mik azok a 0-day sérülékenységek? Miért veszélyesek?
- Milyen kockázat csökkentő ellenintézkedések lehetségesek IT rendszerekben?
- Soroljon fel néhány megelőző jellegű és néhány észlelést célzó biztonsági mechanizmust!
- Mi az a biztonsági incidens?
- Miért fontos az incidensek hatásos és hatékony kezelése?
- Mik az incidenskezelés céljai?
- Mik az incidenskezelés főbb lépései?