

# Bevezetés a kiberbiztonságba és biztonságtudatosság

Kiberfenyegetések

Szarvák Anikó

2023. Tavasz

# About

# Biztonság-tudatosság

Tudatosság az a képesség, melyben közvetlenül megismerjük és érzékeljük az eseményeket.

Olyan állapot, amelyben:

- az alany bír valamilyen információval,
- ez az információ rendelkezésére áll,
- és amely befolyásolja viselkedési folyamatait.

Azonosítható tudatos hozzáállással.

# Biztonság-tudatosság célja

A biztonság-tudatosság arra összpontosít, hogy

- tudatosítsa a gyorsan változó információs formák lehetséges kockázatait és
- az információ gyorsan növekvő veszélyeit,
- amelyek az emberi viselkedést célozzák meg.

A biztonságtudatosság az információbiztonság számos alapelve közül az egyik.

# Biztonság tudatosság szükségessége

**“Internet is not secure by design!”**

/Finnish security researcher/

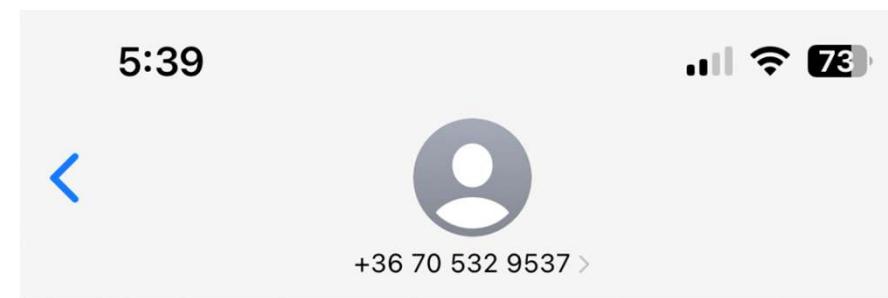
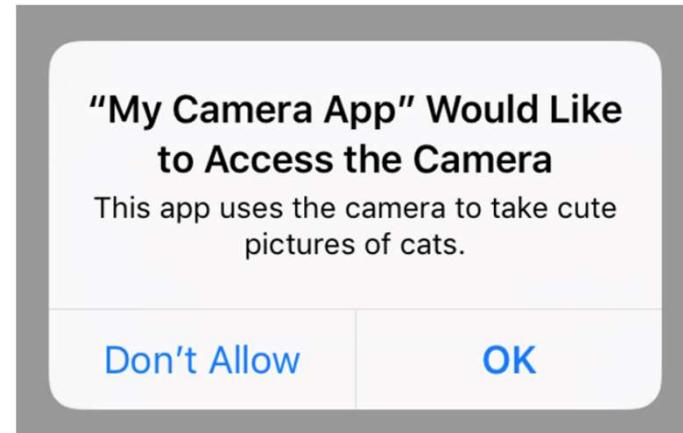
# Teszt!

<https://elearning.uni-obuda.hu/main/mod/quiz/view.php?id=652682>

# Teszt diák



A tanári kar  
fizetése.xlsx



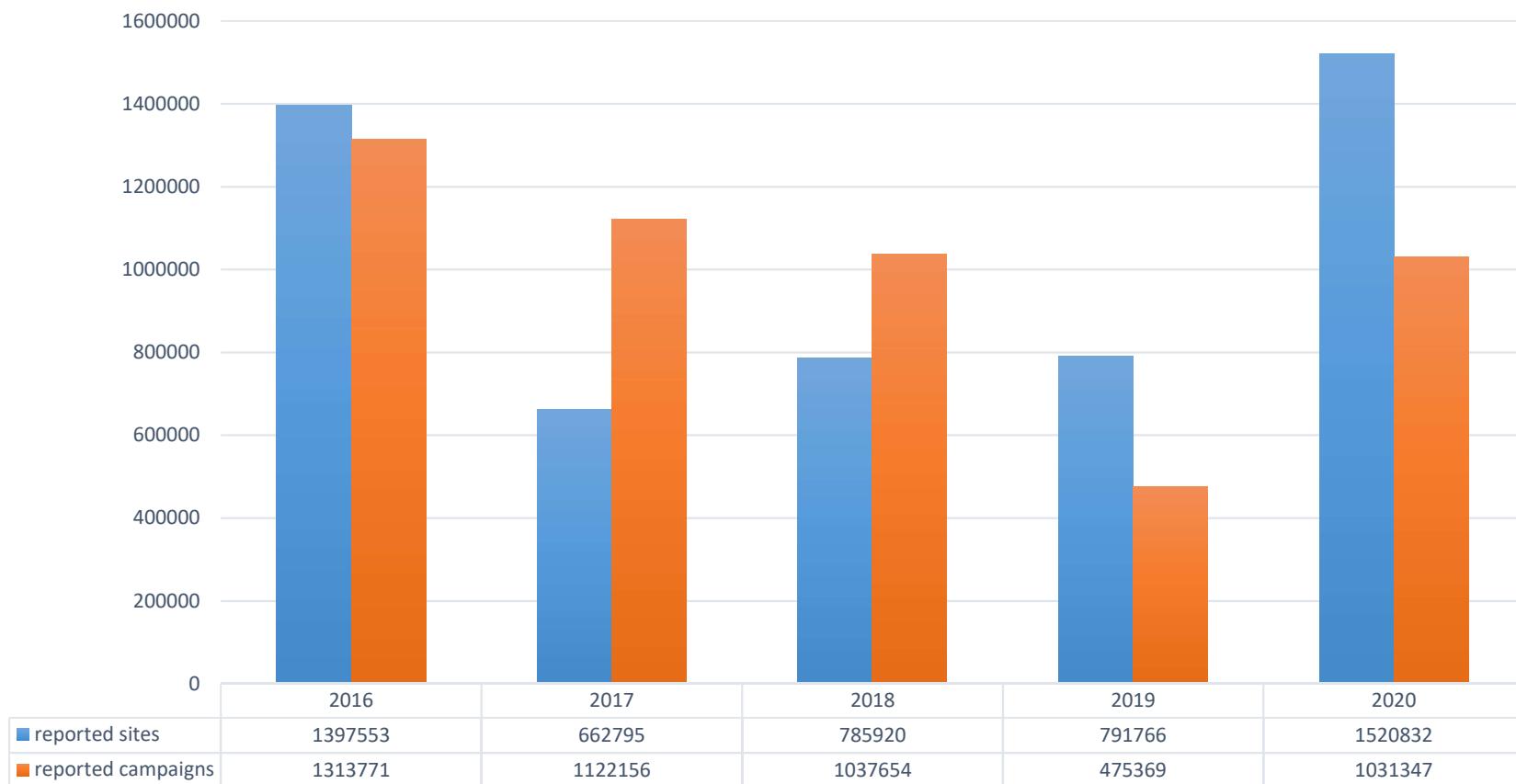
Megerkezett a csomagja, kovesse  
nyomon itt: [https://housespa.store/  
trck/?q1yoyho4zro](https://housespa.store/trck/?q1yoyho4zro)

## Támadási célpontok

	Against Companies	Against people
Malware	X	X
Web based attacks	X	
Phishing	X	X
Web application attacks	X	
Spam	X	X
Distributed Denial of Service (DDOS)	X	
Identify theft		X
Data breach	X	
Insider threat	X	
Botnets	X	
Physical manipulation, damage, theft and loss	X	X
Information leakage	X	
Ransomware	X	X
Cyberespionage	X	
Crytojacking		X

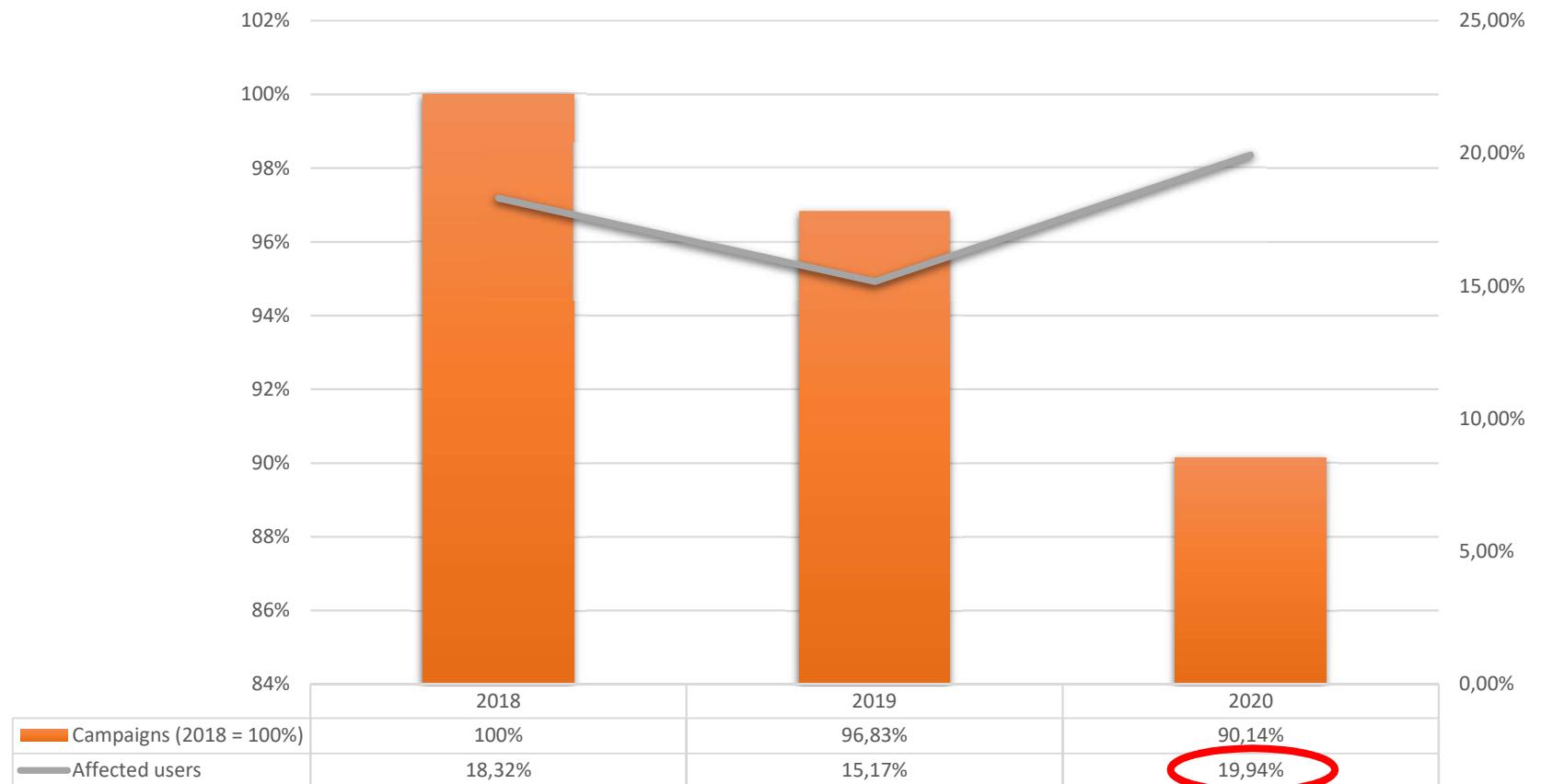
The European Union Agency for Cybersecurity (ENISA) articulates in their research "List of top 15 threats" [12]: "During the next decade, cybersecurity risks will become harder to assess and interpret due to the growing complexity of the threat landscape, adversarial ecosystem and expansion of the attack surface."

## Phishing campaigns: Anti Phishing Working Group (APWG)



Source: Anti Phishing Working Group (APWG) reports  
<https://apwg.org/trendsreports/> Accessed: 2021. 03. 05.

## Phishing campaigns: Kaspersky Antiphish data



Sources: <https://securelist.com/spam-and-phishing-in-2018/89701/>  
<https://securelist.com/spam-report-2019/96527/>  
<https://securelist.com/spam-and-phishing-in-2020/100512/> Accessed: 2021. 03. 05.

# Megtörtént esetek

2000+, SSHD, hullámtámadás

2012, Lockheed Martin vs RSA

2022, Facebook fiók-lopás

# Kérdés?

# Bevezetés a kiberbiztonságba és biztonságtudatosság

Böngészés az interneten

Szarvák Anikó

2023. Tavasz

# Böngésző



- Mi látható a képen?
- Mit jelképez a lakkat szimbólum?
- Milyen gyakran gépelünk el webcímeket?
- Mi történik, ha egy hivatkozás fölé visszük az egeret a webböngészőben?
- Mik azok a web sütik (cookie)?  
Érdemes reklámblokkolót használni? Miért?
- Érdemes privát böngészési módot használni? Miért?

# Webcímek

Uniform Resource Locator (URLs):

- Példa URL: <https://en.wikipedia.org/wiki/URL>
- Az RFC 1738 definiálja
- „feltaláló”: a világháló atyja (Tim Berners-Lee)

Általános formátum:

- scheme://[user[:password]@]host[:port]][/path][?query] [#fragment]

# A domain

TLD – Top Level Domain:

- “.hu”, “.com”

Restricted / korlátozott domainek:

- “.mil”, “.gov”

Domain:

- “uni-obuda.hu”

Aldomain:

- neptun.uni-obuda.hu

# Webcímek formátuma

Séma szerinti web url:

`http://user:pass@example.tld:8080`

Milyen problémák vannak egy ilyen típusú használattal?

# Protokollok

Szokásos protokollok:

- http
- https

“szokásostól eltérő” protokollok használata:

- ftp
- gopher
- Stb.

# Weboldalak felépítése

A weboldalak tartalmát hierarchiába lehet rendezni:

<https://neptun.uni-obuda.hu/hallgato/login.aspx>

“/” után:

- Könyvtár struktúrát vagy logikai struktúrát írhat le
- Hivatkozhat fájlra, egyéb állományokra.

Speciális karakterek dinamikus oldalak esetén:

- pl.: “?”, “&”, “#”

“Escape” karakter és használata:

- ASCII – UNIcode
- “%20”

# Hol van a HTTP?

OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example	Central Device/Protocols	DOD4 Model
<b>Application (7)</b> <small>Serves as the window for users and application processes to access the network services.</small>	<b>End User layer</b> Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management	User Applications SMTP	
<b>Presentation (6)</b> <small>Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.</small>	<b>Syntax layer</b> encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • Character Set Translation	JPEG/ASCII EBCDIC/TIFF/GIF PICT	Process
<b>Session (5)</b> <small>Allows session establishment between processes running on different stations.</small>	<b>Synch &amp; send to ports</b> (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.	Logical Ports RPC/SQL/NFS NetBIOS names	
<b>Transport (4)</b> <small>Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.</small>	<b>TCP</b> Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	F I L T E R P A C K E T I N G	TCP/SPX/UDP
<b>Network (3)</b> <small>Controls the operations of the subnet, deciding which physical path the data takes.</small>	<b>Packets</b> ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting	Routers	Host to Host
<b>Data Link (2)</b> <small>Provides error-free transfer of data frames from one node to another over the Physical layer.</small>	<b>Frames</b> ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control	Switch Bridge WAP PPP/SLIP	IP/IPX/ICMP
<b>Physical (1)</b> <small>Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.</small>	<b>Physical structure</b> Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts	Hub	Can be used on all layers

# HTTPS

Az SSL/TLS legfontosabb szolgáltatásai:

- Felek azonosítása külső tanúsító szervezetek (Certificate Authorities, CA) segítségével,
- Lehetőséget biztosít hibásan azonosított weboldalak automatikus tiltására – feltételezhető valamilyen rosszindulatú cselekmény,
- Adatok védelme erős titkosítás segítségével.

# Tanúsítványok

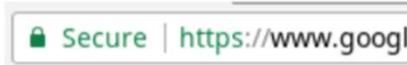
- Nincs titkosítás



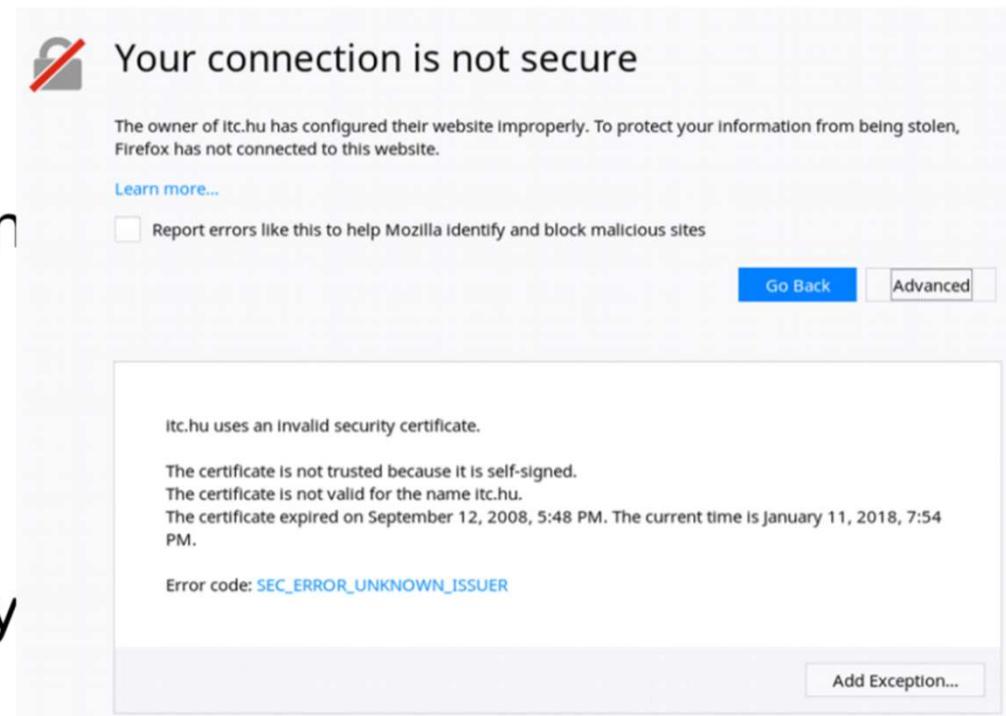
- Saját belső tanúsítván



- Domain tanúsítvány



- Kibővített tanúsítvány



# Támadások

**Adatgyűjtés tudatos hozzájárulás nélkül**

**Bizalmasság megsértése:**

- **Lehallgatás (snifng, wiretapping)**
- **Közbeékelődés (MitM)**

**Kérések eltérítése:**

- **Címhámisítás (DNS, DHCP, IP, ARP)**
- **Trükkös kódolás (URL kódolás, homoglyph támadás)**

# Támadások (folyt.)

Social engineering:

- Phishing (“A fiókod lejárt, újítsd meg itt”),
- Kattintásvadászat (“Sosem fogod kitalálni, hogy aztán mi történt...”),
- Rémisztgetés (“A számítógéped fertőzött, kattints a segítségért”).

Rendszer (böngésző) elleni támadások:

- Szkriptelés (CSRF, XSS),
- Puffer túlcsordulások, stb.

# Támadások (folyt.)

A felhasználó megtévesztése kibővített unicode karakterek segítségével.

Például:

- <http://google.com> (vegyük észre a kis eltéréseket)

A valóság:

- <http://g%u03BF%u043E%u0261%u217C%u0435.com>
- <http://xn--gl-jgb31l6qtb.com>
- <http://xn--g-s1a36hsnmb7023a.com>

# Zárókérdések

- Miért fontos a webes hivatkozásokat ellenőrizni a meglátogatásuk előtt?
- Hogy ellenőrizhetünk egy hivatkozást anélkül, hogy meglátogatnánk?
- Miért használjunk HTTPS protokollt azokon az oldalakon, ahol adatokat lehet rögzíteni?
- Ez a kereső űrlapokra is vonatkozik? Miért?
- Hogy győződhetünk meg arról, hogy valóban a bankunkkal kommunikálunk a weben?
- Mit jelent számunkra a domain birtoklás, vagy a kibővített tulajdonos ellenőrzés?

# Bevezetés a kiberbiztonságba és biztonságtudatosság Levelezés biztonsága

Levelezés biztonsága

Szarvák Anikó

2023. Tavaszi félév

# E-mail szolgáltatások

- Milyen gyakran kapunk ismeretlen feladóktól származó leveleket?
  - Mit tehetünk velük?
- Miért tekinthetők károsnak a SPAM (kéretlen) levelek?
- Mennyire tekinthetők privátnak a magánleveleink?
  - Ki és mikor olvashatja el őket?

# Levelezőrendszerek - kliens

Levelező kliens (Mail User Agent, MUA)

- Elsődleges felhasználói felület
- Feladata az üzenetek megjelenítése és elkészítése
- Az RFC524 és MIME (Multipurpose Internet Mail Extensions) szabványokat használja
- Egyéb protokollok: SMTP, MAPI, IMAP, POP3

# Levelező szerver

Levelező kiszolgáló (Message Transport Agent, MTA)

- Feladata az üzenetek küldése és fogadása
- Az SMTP (Simple Mail Transfer Protocol) szabványt használja

# E-mail: fejléc

## Fejléc mezők (kulcs- értékek)

- From (üzenet feladó)
- To (üzenet címzett)
- CC (másolat)
- Dátum (a feladó rendszerben)
- Subject (tárgy)
- A tartalom típusa és sok minden más...

# Tartalom

## Üzenettörzs (fő tartalom)

- Tartalom típusok
  - multipart/mixed – több rész
  - text/plain – szöveges rész
  - text/html – formázott szöveges rész
  - application/octet-stream – mellékletek
- Számos kódolási típus

# SMTP protokoll alapok

Szöveg alapú űsprotokoll:

- SMTP bővítmények

Küldő oldali üzenetek:

- HELO – kezdő üzenet
- MAIL FROM – boríték feladó
- RCPT TO – boríték címzett DATA – e-mail adatok

(fejlécek és törzs)

(új sorban álló pont) – adat vége

Protokoll kiegészítések (eg. 8 bit a 7 bit helyett)

- SASL (felhasználó/jelszó)
- PKI (tanúsítványok) Titkosítás
- SSL/TLS

# E-mail biztonsági lehetőségek

## Üzenet hitelesítés:

- S/MIME – megbízható külső felek (CA-k)
- PGP – bizalmi háló („kulcsaláíró bulik”)
- Nem terjedtek el – elég – széles körben

## Titkosítás:

- Üzenetek: S/MIME és PGP
- Kommunikáció: SMTPS (SSL/TLS)
- Nem oldanak meg minden!

## Küldő fél azonosítása:

- Sender Policy Framework (SPF)
- Domain Keys Identified Mail (DKIM)

# Spam, malware

## Kéretlen levél (spam):

- Hirdetés
- Phishing levél
- Malware-t terjesztő levelek

## Rosszindulatú kód (Malware):

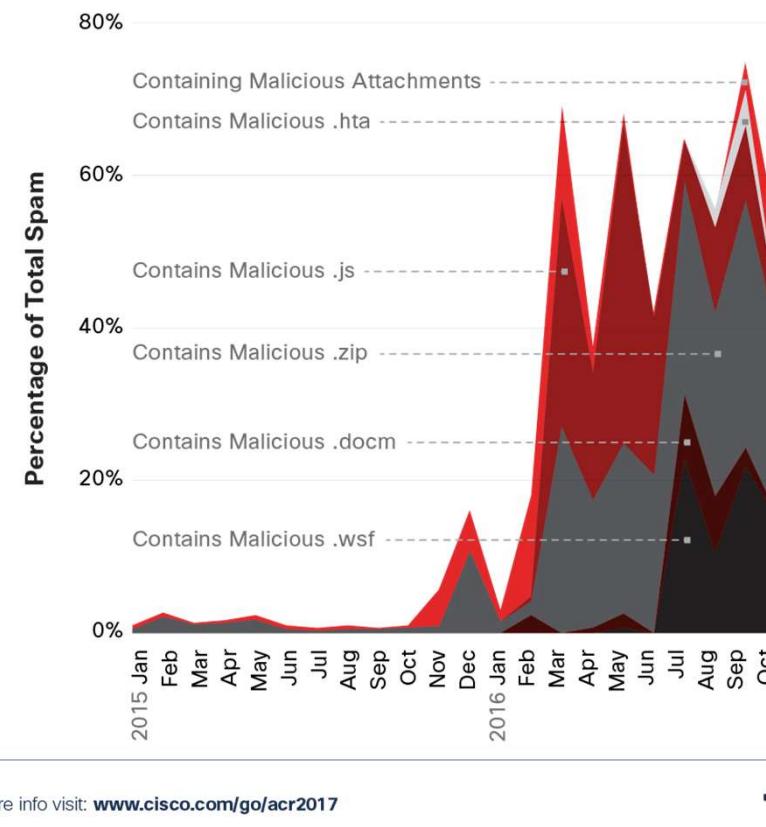
- Vírus, féreg, kémprogram
- Reklámprogram
- Zsarolóprogram

» USPS®	Aszarvak 🚧 We were unable to deliver yo...
» Lowe's®	Re: You have won an Club Car Golf Cart
» Walmart™	Aszarvak - You have won an iPad Pro
» FedEx™	Please confirm!! FedEx signature required mi...
» Shell Gas Station	Aszarvak, You have won an \$500 Shell Gas ...
» Fidelity_Life_Insur.	Hi Aszarvak; \$250K Life Insurance Coverage ...
» \$ PayApp \$	You received a payment of \$1000.00 USD
» @USPS📦	(2nd attempt) 🚧 NOTIFICATION OF YOUR P...
» \$ PayApp \$	You received a payment of \$1000....
» SpiTech Conference	SpiTech 2023 - Deadline is approaching!
» Track&Trace	Aszarvak , your package is out for delivery! ⏱
» UPS®	Aszarvak 📩 your package is out for delive...

# Spam + Malware

Figure 17 Percentage of Total Spam Containing Malicious Attachments

Source: Cisco Security Research



For more info visit: [www.cisco.com/go/acr2017](http://www.cisco.com/go/acr2017)



# Védekezés

## SPAM és Malware elleni küzdelem:

- DNS alapú szűrőlisták
- Azonosítás (SPF/DKIM)

## Szabályrendszer alapú szűrések

- Antivirus rendszerek (általános célú) Antispam rendszerek (specifikus)
- Adatelemzés (pl. bayes alapú szűrés, képfelismerés)
- Protokoll alapú trükkök (pl. graylisting)

# További támadások

Scam-ek, csaló üzenetek (pl.: nigériai levelek)

- Kártékony szoftver terjesztés
- Phishing (“Fiókja felfüggesztésre került, kattintson ide: URL”)

Feladó hamisítás:

- üzenet küldő (RFC524 From fejléc)
- boríték küldő (SMTP MAIL FROM)

Rendszerek (MUA, MTA) elleni támadások

- Pufer túlcsordulás...

# E-mail szolgáltatások – záró kérdések

- Hogy ellenőrizhetünk egy eddig ismeretlen levél feladót?
- Miért van jelentősége a külső erőforrások (pl. beágyazott képek) letöltésének a HTML e-mailek megjelenítésekor?
- Mit tegyünk egy jelszóval védett ZIP fájlt tartalmazó e-mail esetén, ha a jelszó a levél törzsében megadásra került?
  - Mi lehet egy ilyen üzenet küldésének az oka?

# Bevezetés a kiberbiztonságba - Biztonságtudatosság

EU Általános Adatvédelmi Rendelet (GDPR)

Bonifert Tamás

2023. 03. 30.

# GDPR jellemzői

- Az EU általános adatvédelmi rendelete
- 2016-ban fogadták el, ekkor is lépett hatályba, de 2018-tól kell alkalmazni
- A személyes adatok védelméhez kapcsolódó jogokat rögzíti
- Adatkezelők, adatfeldolgozók számára jelentős változásokat jelent
- Jogharmozációt a 2018. évi XIII. és XXXVIII. tv. biztosítja

# GDPR előzményei

- 1992. évi LXIII tv (Avtv.) a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról
  - adatvédelmi biztos
- 2011. évi CXII. tv (Infotv) az információs önrendelkezési jogról és az információszabadságról
  - adatvédelmi hatóság (NAIH)

# Kapcsolódó fogalmak

- Érintett
- Személyes adat
- Különleges személyes adat
- Adatkezelés
- Adatkezelő
- Adatfeldolgozó



# Adatkezelés elvei

- jogoszerűség, tiszteességes eljárás és átláthatóság
- célhoz kötöttség
- adattakarékosság
- pontosság
- korlátozott tárolhatóság
- integritás és bizalmas jelleg

# Érintettek jogai

- tájékoztatáshoz való jog
- hozzáféréshez való jog
- helyesbítéshez való jog
- törléshez való jog („az elfeledtetéshez való jog”)
- adatkezelés korlátozásához való jog
- adathordozhatósághoz való jog
- tiltakozáshoz való jog
- jogorvoslathoz való jog

# Adatkezelési tájékoztató

- minden adatkezelő számára kötelező az elkészítése
- megelőzi az adatkezelést
- tartalma:
  - adatkezelő megnevezése
  - adatkezelés célja, kezelt adatok köre
  - adatkezelés jogalapja, kezelésük időtartama
  - érintett kapcsolódó jogai

# Az adatkezelések biztonsága

*„A személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve” (GDPR 5. cikk, (1) bekezdés f) pontja)*

## Az adatkezelő feladatai:

- szükség esetén anonimizál, titkosít
- folyamatosan biztosítja az adatok bizalmasságát, integritását és rendelkezésre állását
- incidens esetén tájékoztat, helyreállít
- rendszeresen teszteli a fentiek teljesülését

# Adatvédelmi incidensek kezelése

*„adatvédelmi incidens”: a biztonság olyan sérülése, 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;” (GDPR 4. cikk, 12. pontja)*

## Az adatkezelő feladatai:

- incidensek nyilvántartása
- illetékes hatóság tájékoztatása (72 órán belül)
- érintettek tájékoztatása, ha szükséges
- incidens kezelése (helyreállítás, megelőzés)

# Adatkezelések nyilvántartása

- az adatkezelők és adatfeldolgozók számára is kötelező az adatkezelési tevékenységekről nyilvántartást vezetni (eltérő tartalommal)
- 250 főnél kevesebb személyt foglalkoztatató vállalatoknál nem kell ilyen nyilvántartás, ha az adatkezelés az érintettek jogaira nézve valószínűíthetően nem jár kockázattal, illetve az adatkezelés alkalomszerű

# Adatvédelmi hatásvizsgálat

- magas kockázatú adatkezelések esetén kötelező
- különösen személyes jellemzők automatizált gyűjtése, valamint nyilvános helyek nagymértékű, módszeres megfigyelése esetén
- elemei:
  - adatkezelési műveletek, célok bemutatása
  - szükségesség és arányosság vizsgálata
  - kapcsolódó kockázatok vizsgálata
  - kockázatok kezelésének bemutatása

# Érdekmérlegelési teszt

Adatkezelés szükségességének  
megállapítása

Jogos érdek definiálása

Adatkezelés paramétereinek  
meghatározása

Érintettek érdekeinek megállapítása

Adatkezelői jogos érdekek és az  
érintettek jogainak összevetése

# Adatvédelmi tisztviselő

- kötelező kijelölni:
  - közfeladatot ellátó szervek esetében
  - szisztematikus, nagymértékű megfigyelés esetén
  - különleges adat kezelése esetén
- feladatai:
  - a GDPR előírásainak és az érintettek jogainak érvényesülésének biztosítása
  - az adatkezelést végzők szakmai támogatása
  - adatvédelmi incidensek kivizsgálása, jelentése
  - a hatósággal való együttműködés

# KÖSZÖNÖM A FIGYELMET!

## Kérdések?

# Bevezetés a kiberbiztonságba - Biztonságtudatosság

Jelszavak kezelése

Bonifert Tamás

2023. 04. 13.

# Tartalom

## Jelszavakkal kapcsolatos tudnivalók

- Jelszavakkal, jelszó hash-ekkel kapcsolatos általános tudnivalók
- Biztonságos jelszótárolás
- Jelszó policyk
- Jelszófeltörési technikák
- Jelszómenedzser megoldások
- Alkalmazás hitelesítés

# Milyen minőségű jelszavak használatosak?

# 80%



# Jelszavakkal kapcsolatos megállapítások

- A különböző vizsgálatok eredményei alapján rossz minőségű jelszavak használatosak
- Oktatás szerepe -> jelszóképzési technikák ismertetése
- Jelszavakra vonatkozó szabályok körültekintő kialakítása
- Üzemeltető állomány felelőssége
  - Jelszavakkal kapcsolatos operációs rendszer szintű beállítások
  - Kiemelt jogosultságok körültekintő használata
  - Jelszó blacklistek létrehozása
  - A technikai fejlődés figyelembe vétele

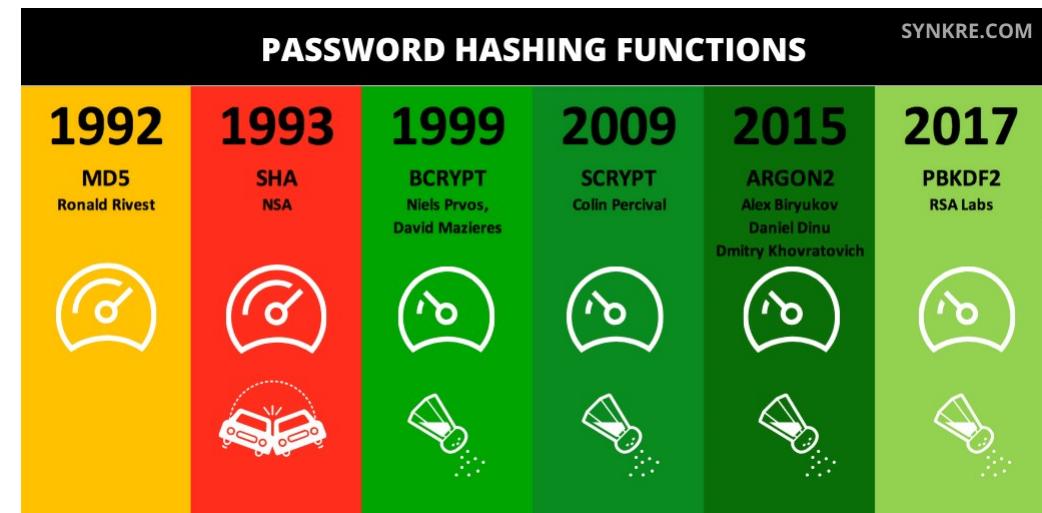
# Jelszótárolás elvi lehetőségei

- Clear text
- Titkosított jelszótárolás
- Jelszóhash

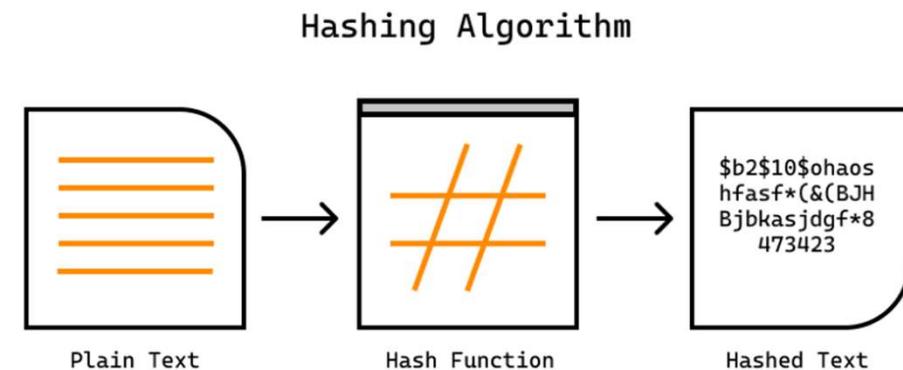


# Hash algoritmusok fajtái

- Jelszavak hashelésére nem alkalmas függvények
  - MD5
  - SHA-1, SHA-256, SHA-512 stb.
- Jelszavak hashelésére szolgáló függvények
  - Bcrypt, Scrypt
  - Argon2, PBKDF2

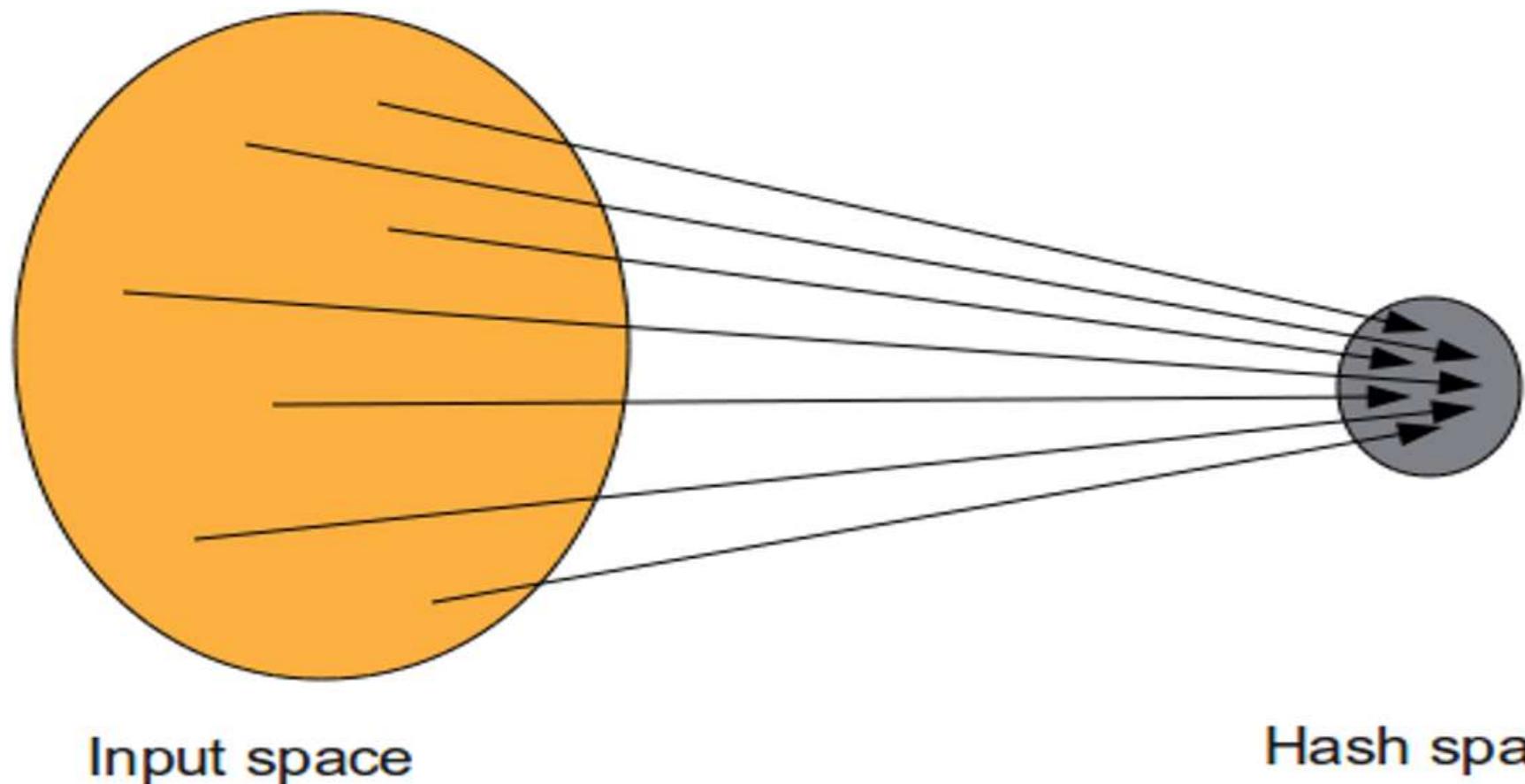


# Hash algoritmusok jellemzői



- Egyirányú kódolási rutin
- Adott bemenetből mindenkor ugyanaz a kimenet képződik
- A kimeneti adat egyértelműen utal a bemeneti adatra...
- ...de a kimeneti adatból nem állítható elő a bemeneti adat
- A bemeneti adat legkisebb változása teljesen más kimenetet eredményez

# Hash értékkészlet jellemzői

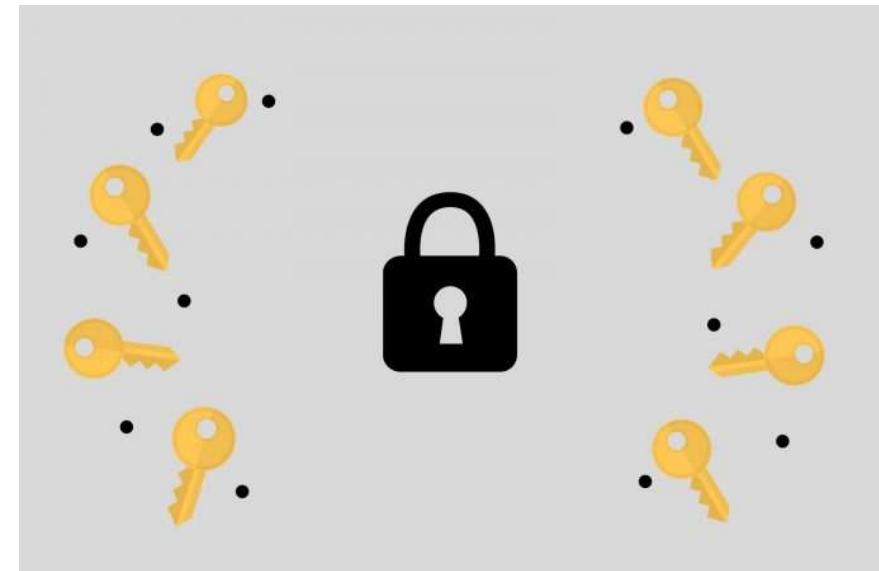


# Jelszó hash algoritmusok

- LM (Windows NT 1.0)
- NTLM v1 (Windows NT 3.1)
- NTLM v2 (Windows NT 4.0)
- KRB5TGS (Kerberos)
- B-crypt, S-crypt
- Argon2

}

Adaptív jelszóhash



# Jelszóképzés szempontjai

- Ideális jelszóhossz
- Hosszú vs. összetett jelszó: melyik preferáljuk?
- Jelszavakra vonatkozó szabályok körültekintő kialakítása
- Jelszócsere: az új jelszó ne hasonlítson az előző jelszóra!
- Divatos jelszóképzési technikák: valóban biztonságos?
  - **Budapest12 -> Bud@p\$st12**
- Feketelisták jelentősége
- Kódmondaton alapuló jelszavak
  - **Afm100%iv**

# Hosszú vs. összetett jelszó

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

# Eltúlzott biztonsági beállítások következményei

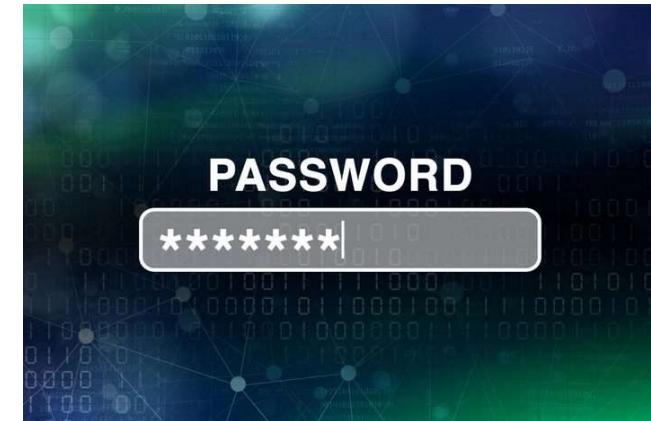
-Kérem, adja meg jelszavát!  
alma  
-Sajnálom, a jelszónak legalább 8 karakterből kell állnia.  
-reszelt alma  
-Sajnálom, a jelszónak tartalmaznia kell legalább egy számot.  
-50reszeltalma  
-Sajnálom, a jelszónak legalább egy nagybetűt kell tartalmaznia.  
-50KIBASZOTTreszeltalma  
-Sajnálom, a jelszóban nem követhetik egymást nagybetűk.  
-50Kibaszott,ReszeltAlma,FeldugvaAseggedbe!  
-Sajnálom, a jelszó nem tartalmazhat írásjeleket.  
-50KibaszottReszeltAlmaRohaggymegHaNemFogadodElEztSe  
-Sajnálom, a jelszó már foglalt.

# Biztonsági problémák a gyakorlatban

- Legacy rendszereknél alapértelmezett lehet az NTLM v1
- A jelszóhash-ek sok esetben megszerezhetők (hálózati forgalom, lokál gép)
- 8 karakteres jelszó egy közepes vga-val akár 350 milliárd (!) hash legenerálható
- ... azaz egy 8 karakter hosszúságú, bármilyen bonyolultságú jelszó 5-6 óra alatt törhető, ha megvan a hash

# Jelszóházirend beállítások

- Enforce password history: >24
- Maximum password age: >360
- Minimum password age: 1 day
- Minimum password lenght: >12
- Password must meet complexity: Enabled (?)
- Store password using reversible encryption: Disabled



# Password manager programok jellemzői

- Automatikus (biztonságos) jelszóképzés
- Jelszavak titkosított adatbázisban történő tárolása
- Mesterjelszóval történő (akár automatizált) hozzáférés a jelszavakhoz
- Lehet felhős vagy lokális tárolású megvalósítás is

# Követelmények

- Jelszó adatbázis és mesterjelszó erős algoritmussal történő titkosítása (AES-256 stb.)
- Gyártói támogatás (sérülékenység menedzsment)
- Biztonsági mentés lehetősége
- Kétfaktoros hitelesítés
- Felhős változat esetén:
  - Zero-knowledge architektúra
  - Local only encryption/decryption

# Ajánlott password manager alkalmazások

- 1Password
- KeePass
- Dashlane
- LastPass
- Syspass



- Különböző PAM megoldások (pl. Thycotic, Thalos)

# KÖSZÖNÖM A FIGYELMET!

## Kérdések?

# Közösségi média és felhőalapú adatmegosztó platformok - adatvezérelt gazdaság, felhasználói profilalkotás és nyomon követés, botok és trollok, internetes zaklatás, incidensek, esettanulmányok, OSINT.

Szabó Patrik László

2023. április 18.

# Gondolatébresztő kérdések

Melyek az ismertebb közösségi oldalak, felhőalapú adatmegosztó platformok?

Az említett platformokon megjelenő adatainkat mennyire elemzik ki a platform üzemeltetői?

Az említett platformokon megjelenő adatainkat mennyire elemzik ki a platform felhasználói?

A platformokon végrehajtott cselekvéseinket (például chat-elés valakivel) mennyire figyeli és elemzi az üzemeltető?

A platformokon végrehajtott cselekvéseinket (például chat-elés valakivel) mennyire figyeli és elemzik a platform felhasználói?

# Túl sok az adat...

Hol legyenek tárolva az adatok?

Hogyan legyenek tárolva az adatok?

Az adatok mely része legyen feldolgozva?

Az adatok hogyan legyenek feldolgozva?

Hogyan fogunk megfelelni az aktuális előírásoknak?

# Adatvezérelt gazdaság

„egov.hu: Az adatvezérelt működés nehezen kezelhető problémák elő állítja a vállalatokat.”

Gondoljuk át vállalatvezetői szemmel, hogy mennyire szükséges számunkra az emberek adatainak ismerete...

Adathasználati és elemzési stratégia készítése szükséges a nagy mennyiségű adat miatt a vállalatok számára.

Az adatmanipuláció egyre nagyobb veszélyt jelent!

# OSINT (Open Source Intelligence)

Nyílt forrású hírszerzésként is emlegetik.

A tévhitekkel ellentétben, az internet létrejötte előtt is létezett!

„Jó és rossz dolgokra is használható.”

A közösségi médiáknak **DPV1** koszönhetően napjainkban nagyon veszélyes „fegyver” tud lenni.

Ma már olyan AI-ok is léteznek melyek segítenek az OSINT-ba.

## 5. dia

---

**DPV1**

A média a médium többesszáma, teht helytelen a médiát tovább többesszámozni.

Dr. Póser Valéria; 2023. 02. 15.

# Felhasználói profilalkotás, nyomon követés

Az alkalmazások nagy része nem elégzik meg azzal, hogy a felhasználó adatait elkéri, hanem engedélyt kér a hely meghatározásához, mikrofon használatához stb...

Például a Youtube esetében észlelhetjük ezt a jelenséget.

Ha mint felhasználó szeretnénk egy másik felhasználóról profilt alkotni, nyomon követni akkor kiváló eszköz az OSINT

Túlzásokba esés esetén előfordulhat, hogy a profilalkotót zaklatással vádolják

# Botok és trollkodás



A trollkodás irányulhat felhasználó által rendszer felé vagy fordítva is.

Két felhasználó között történő trollkodás könnyen átmehet mentális károkozásba.

# Internetes zaklatás

Az interneten a legtöbb ember elfelejti, hogy:

- Akivel kommunikál, Ő egy érző ember
- A cselekedetei nyomon követhetőek
- A tetteinek következményei lehetnek

Az interneten a legtöbb ember bátor így olyan dolgokat tesz melyeket személyesen nem tenne. (Például másokat szavakkal bántalmaz.)

Vannak olyan robotok melyek ezt elősegítik.

Internet vs személyes kommunikáció:

<https://www.youtube.com/watch?v=6zUc-mpMGr>

# Internetes zaklatás

Nem tudhatjuk, hogy ki mit élt át korábban, miktől fél és mikre érzékeny viszont sokan a közösségi médiában megosztják bánatukat, életük negatív történésein ezzel fegyvert adva a támadóknak.

Újonnan a bűnszervezetek, az áldozataik becserkészését internetes zaklatással indítják.

Kisfilm: <https://www.youtube.com/watch?v=MDqxBGL738U>



ÓBUDAI EGYETEM  
NEUMANN JÁNOS INFORMATIKAI KAR

Mérnökinformatikus SOC elemző

# OSINT a gyakorlatban...

# Bevezetés a kiberbiztonságba és biztonság tudatosság

Zero Trust Architecture (ZTA)

Szarvák Anikó

2023. Tavasz

## NIST Special Publication 800-207

---

# Zero Trust Architecture

---

Scott Rose  
Oliver Borchert  
Stu Mitchell  
Sean Connelly

This publication is available free of charge from:  
<https://doi.org/10.6028/NIST.SP.800-207>

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf>

# Bevezetés

Egy tipikus vállalat infrastruktúrája egyre bonyolultabbá vált.

Egy vállalat több belső hálózatot, saját helyi infrastruktúrával rendelkező távoli irodát, távoli és/vagy mobil egyéneket, valamint felhőszolgáltatásokat üzemeltethet.

Ez az összetettség felülmúlta a határvédelem (perimeter) alapú hálózatbiztonság korábbi módszereit, mivel nincs egyetlen, könnyen azonosítható kerület a vállalat számára.

A határvédelem alapú hálózati biztonság sem bizonyult elégségesnek, mivel amint a támadók áttörik a kerületet, a további oldalirányú mozgás akadálytalan.

# Bevezetés (folyt.)

A ZT nem egyetlen architektúra, hanem a munkafolyamat, a rendszertervezés és a műveletek vezérelvei, amelyek segítségével javítható bármilyen alkalmazó biztonsági szintje, helyzete [FIPS199].

A ZTA-ra való átállás egy utazás, arról szól, hogy egy szervezet miként értékeli a kockázatokat küldetése során, és ez nem valósítható meg egyszerűen a technológia cseréjével. Ennek ellenére sok szervezet vállalati infrastruktúrájában már ma is megtalálhatók a ZTA elemei.

A szervezeteknek törekedniük kell a ZTA bizalmi elvek, a folyamatváltozások és a technológiai megoldások fokozatos bevezetésére, amelyek felhasználási esetenként védi a adatvagyonukat és üzleti funkcióikat.

A legtöbb vállalati infrastruktúra hibrid zéró bizalom/perem alapú üzemmódban fog működni, miközben továbbra is befektet az IT-korszerűsítési kezdeményezésekbe és javítja a szervezeti üzleti folyamatokat.

# Alapvetések

A ZT egy kiberbiztonsági paradigmája, amely az erőforrások védelmére összpontosít, és arra az előfeltevésre, hogy a bizalmat soha nem adják meg implicit módon, hanem folyamatosan értékelni kell.

A ZT architektúra a vállalati erőforrás- és adatbiztonság teljes körű megközelítése, amely magában foglalja az identitást (személyes és nem személyi entitások), a hitelesítő adatokat, a hozzáféréskezelést, a műveleteket, a végpontokat, a tárhely-környezeteket és az összekapcsoló infrastruktúrát.

Arra kell összpontosítani, hogy az erőforrásokat azokra korlátozzák, akiknek csak a küldetés végrehajtásához szükséges minimális jogosultságokat (például olvasási, írási, törlési) kell hozzáférniük és megadniuk.

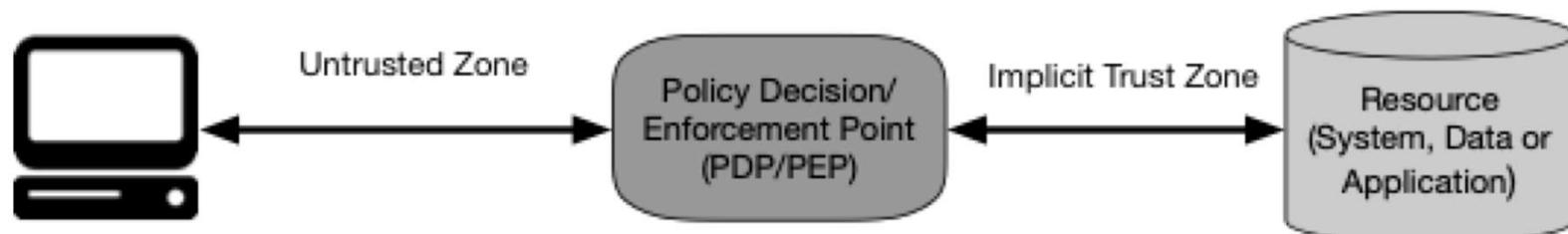


Figure 1: Zero Trust Access

# ZTA tételek (folyt.)

## 1. minden adatforrás és számítástechnikai szolgáltatás erőforrásnak minősül.

Egy hálózat több eszközösztályból is állhat.

A hálózatnak lehetnek kis helyigényű eszközei is, amelyek adatokat küldenek aggregátoroknak/tárolóknak, szoftvert szolgáltatásként (SaaS), utasításokat küldő rendszereket működtetőknek és egyéb funkciókat.

A vállalat dönthet úgy is, hogy a személyes tulajdonú eszközöket erőforrásként minősíti, ha hozzáfér a vállalati tulajdonú erőforrásokhoz.

## ZTA tételek (folyt.)

**2. A hálózat helyétől függetlenül minden kommunikáció biztonságos. A hálózati hely önmagában nem jelent bizalmat.**

A vállalati tulajdonú hálózati infrastruktúrán (például egy régebbi hálózaton belül) elhelyezkedő eszközökből származó hozzáférési kérelmeknek ugyanazoknak a biztonsági követelményeknek kell megfelelniük, mint a hozzáférési kérelmeknek és a kommunikációnak bármely más, nem vállalati tulajdonú hálózatról. Más szavakkal, a megbízhatóságot nem szabad automatikusan megadni attól függően, hogy az eszköz a vállalati hálózati infrastruktúrán van.

Minden kommunikációt az elérhető legbiztonságosabb módon kell végrehajtani, védeni kell a bizalmasságot és az integritást, és biztosítani kell a forrás hitelesítését.

# ZTA tételek (folyt.)

## 3. Az egyes vállalati erőforrásokhoz való hozzáférés munkamenetenkénti alapon történik.

A kérelmezőbe vetett bizalmat a rendszer a hozzáférés megadása előtt értékeli.

A hozzáférést a feladat elvégzéséhez szükséges legkevesebb jogosultsággal kell biztosítani. Ez csak azt jelenti, hogy „valamikor mostanában” az adott tranzakcióhoz, és nem fordulhat elő közvetlenül a munkamenet kezdeményezése vagy az erőforrással való tranzakció végrehajtása előtt.

Az egyik erőforrás hitelesítése és engedélyezése azonban nem ad automatikusan hozzáférést egy másik erőforráshoz.

## ZTA tételek (folyt.)

**4. Az erőforrásokhoz való hozzáférést dinamikus házirend határozza meg – beleértve az ügyfélazonosság, az alkalmazás/szolgáltatás és a kérelmező eszköz megfigyelhető állapotát –, és más viselkedési és környezeti jellemzőket is tartalmazhat.**

A szervezet az erőforrások védelmét azáltal védi, hogy meghatározza, milyen erőforrásokkal rendelkezik, kik a tagjai (vagy képesek-e hitelesíteni az egyesített közösségből származó felhasználókat), és milyen erőforrásokhoz van szükségük a tagoknak.

Az erőforrás-hozzáférési és műveleti engedélyek házirendjei az erőforrás/adat érzékenységétől függően változhatnak.

A legkisebb jogosultság elvét alkalmazzák a láthatóság és a hozzáférhetőség korlátozására.

## ZTA tételek (folyt.)

**5. A vállalat felügyeli és méri az összes tulajdonában lévő és kapcsolódó eszköz integritását és biztonsági helyzetét.**

Egyetlen vagyontárgy sem eredendően megbízható.

A vállalat az erőforráskérés értékelésekor értékeli az eszköz biztonsági helyzetét.

A ZTA-t megvalósító vállalkozásnak létre kell hoznia egy folyamatos diagnosztikai és mérséklő (CDM) vagy hasonló rendszert az eszközök és alkalmazások állapotának figyelésére, és szükség esetén javításokat/javításokat kell alkalmaznia.

Ehhez is szükség van egy robustus megfigyelési és jelentési rendszerre, amely alkalmas adatokat szolgáltat a vállalati erőforrások jelenlegi állapotáról.

# ZTA tételek (folyt.)

**6. minden erőforrás-hitelesítés és engedélyezés dinamikus, és a hozzáférés engedélyezése előtt szigorúan betartandó.**

Ez a hozzáférés megszerzésének, a fenyegetések vizsgálatának és értékelésének, az alkalmazkodásnak és a folyamatos kommunikációba vetett bizalom folyamatos újraértékelésének állandó ciklusa.

A ZTA-t megvalósító vállalattól elvárható, hogy rendelkezzen Identity, Credential és Access Management (ICAM) és eszközkezelési rendszerekkel.

Ez magában foglalja a többtényezős hitelesítés (MFA) használatát egyes vagy az összes vállalati erőforráshoz való hozzáféréshez.

## ZTA tételek (folyt.)

**7. A vállalkozás a lehető legtöbb információt összegyűjti az eszközök aktuális állapotáról, a hálózati infrastruktúráról és a kommunikációról, és ezt felhasználja biztonsági helyzetének javítására.**

A vállalatnak adatokat kell gyűjtenie az eszközök biztonsági helyzetéről, a hálózati forgalomról és a hozzáférési kérelmekről, fel kell dolgozna ezeket az adatokat, és minden megszerzett betekintést fel kell használnia a szabályzat létrehozásának és betartatásának javítására.

Ezek az adatok felhasználhatók arra is, hogy kontextust biztosítsanak az alanyok hozzáférési kérelmeihez.

# ZTA Hálózati nézete

## 1. A teljes vállalati magánhálózat nem tekinthető implicit bizalmi zónának.

Az eszközöknek mindenkor úgy kell viselkedniük, mintha támadó lenne jelen a vállalati hálózaton, és a kommunikációt a lehető legbiztonságosabb módon kell végezni (lásd a fenti 2. tételeit).

Ez olyan műveletekkel jár, mint az összes kapcsolat hitelesítése és az összes forgalom titkosítása.

## ZTA Hálózati nézete (folyt.)

**2. Előfordulhat, hogy a hálózaton lévő eszközök nem lehetnek a vállalat tulajdonában és nem konfigurálhatók.**

A látogatók és/vagy a szerződéses szolgáltatások tartalmazhatnak nem vállalati tulajdonú eszközöket, amelyeknek hálózati hozzáférésre van szükségük szerepük ellátásához.

Ebbe beletartoznak a „hozd saját eszközöd” (BYOD) házirendek, amelyek lehetővé teszik a vállalati alanyok számára, hogy nem vállalati tulajdonú eszközöket használjanak a vállalati erőforrásokhoz.

# ZTA Hálózati nézete (folyt.)

## 3. Egyetlen erőforrás sem eleve megbízható.

Minden eszköz biztonsági helyzetét PEP segítségével ki kell értékelni, mielőtt egy vállalati tulajdonú erőforráshoz adnak egy kérelmet.

Ennek az értékelésnek folyamatosnak kell lennie mindaddig, amíg az ülés tart.

A vállalati tulajdonú eszközök tartalmazhatnak olyan melléktermékeket, amelyek lehetővé teszik a hitelesítést, és magasabb megbízhatósági szintet biztosítanak, mint a nem vállalati tulajdonú eszközökről érkező kérés.

Az alany hitelesítő adatai önmagukban nem elegendők az eszköz hitelesítéséhez egy vállalati erőforráshoz.

# ZTA Hálózati nézete (folyt.)

## 4. Nem minden vállalati erőforrás található a vállalati infrastruktúrán.

Az erőforrások közé tartoznak a távoli vállalati témák, valamint a felhőszolgáltatások.

Előfordulhat, hogy a vállalati tulajdonú vagy kezelt eszközöknek a helyi (azaz nem vállalati) hálózatot kell használniuk az alapvető csatlakozásokhoz és hálózati szolgáltatásokhoz (például DNS-feloldáshoz).

## ZTA Hálózati nézete (folyt.)

**5. A távoli vállalati alanyok és eszközök nem bízhatnak teljes mértékben a helyi hálózati kapcsolatukban.**

A távoli személyeknek feltételezniük kell, hogy a helyi (azaz nem vállalati tulajdonú) hálózat ellenséges.

Az eszközöknek feltételezniük kell, hogy az összes forgalmat figyelik és potenciálisan módosítják.

Minden csatlakozási kérelmet hitelesíteni és engedélyeztetni kell, és minden kommunikációt a lehető legbiztonságosabb módon kell végrehajtani (azaz biztosítani kell a bizalmas kezelést, az integritás védelmét és a forráshitelesítést).

# ZTA Hálózati nézete (folyt.)

**6. A vállalati és nem vállalati infrastruktúra között mozgó eszközöknek és munkafolyamatoknak következetes biztonsági politikával és helyzettel kell rendelkezniük.**

Az eszközöknek és a munkaterheléseknek meg kell őrizniük biztonsági helyzetüket, amikor a vállalati tulajdonú infrastruktúrába vagy onnan költöznek.

Ez magában foglalja azokat az eszközöket, amelyek a vállalati hálózatokból nem vállalati hálózatokba lépnek át (azaz távoli felhasználók).

Ez magában foglalja a helyszíni adatközpontokból a nem vállalati felhőpéldányokba migráló munkaterheléseket is.

# Házi rend motor (PE)

Ez a komponens felelős a végső döntésért, hogy hozzáférést biztosítanak-e egy adott téma erőforrásához.

A PE vállalati szabályzatot, valamint külső forrásokból (pl. CDM-rendszerekből, alább ismertetett fenyegetés-felderítő szolgáltatásokból) származó bemenetet használ egy megbízhatósági algoritmus bemeneteként az erőforráshoz való hozzáférés megadására, megtagadására vagy visszavonására.

A PE párosítva van a házi rend-rendszer-gazda összetevővel.

A házi rend-motor hozza meg és naplózza a döntést (jóváhagyva vagy elutasítva), a házi rend-adminisztrátor pedig végrehajtja a döntést.

# Házi rend-adminisztrátor (PA)

Ez az összetevő felelős az alany és az erőforrás közötti kommunikációs útvonal létrehozásáért és/vagy leállításáért (a megfelelő PEP-ekhez küldött parancsokon keresztül).

Ez létrehozna minden munkamenet-specifikus hitelesítési és hitelesítési tokent vagy hitelesítő adatot, amelyet az ügyfél a vállalati erőforrás eléréséhez használ.

Szorosan kötődik a PE-hez, és annak döntésére támaszkodik, hogy végül engedélyezi vagy megtagadja a munkamenetet.

- Ha a munkamenet engedélyezett, és a kérés hitelesített, a PA konfigurálja a PEP-t, hogy lehetővé tegye a munkamenet elindítását.
- Ha a munkamenetet megtagadják (vagy egy korábbi jóváhagyást ellensúlyoznak), a PA jelzi a PEP-nek a kapcsolat leállítását.

Egyes megvalósítások a PE-t és a PA-t egyetlen szolgáltatásként kezelhetik; itt fel van osztva annak két logikai komponens.

# Irányelv-végrehajtási pont (PEP)

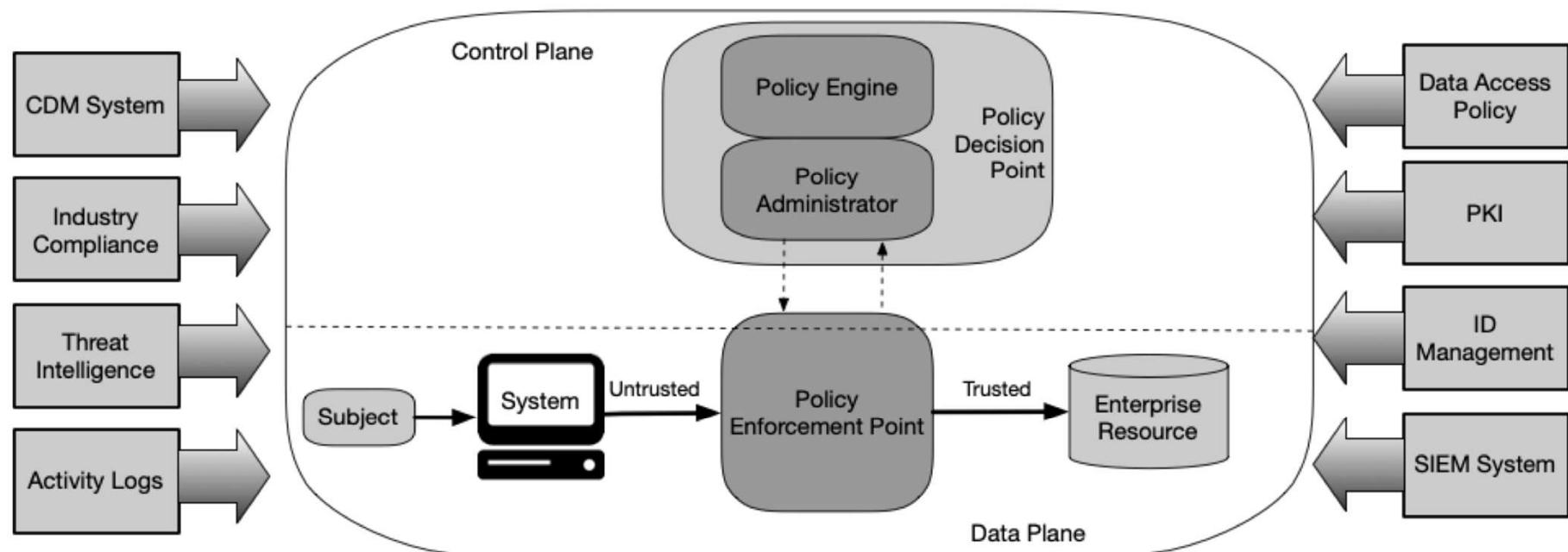
Ez a rendszer felelős az alany és a vállalati erőforrás közötti kapcsolatok engedélyezéséért, figyeléséért és esetlegesen megszüntetéséért.

A PEP kommunikál a PA-val a kérelmek továbbítása és/vagy az irányelv-frissítések fogadása érdekében.

Ez egyetlen logikai komponens a ZTA-ban, de két különböző összetevőre bontható: a kliens (pl. ügynök a laptopon) és az erőforrás oldal (pl. a hozzáférést vezérlő erőforrás előtti átjáró komponens) vagy egyetlen portálkomponens, amely működik mint a kommunikációs utak kapuőre.

A PEP-n túl található a vállalati erőforrást kiszolgáló bizalmi zóna.

# ZTA elemei



**Figure 2: Core Zero Trust Logical Components**

# Folyamatos diagnosztikai és kockázatcsökkentő (CDM) rendszer

Ez információkat gyűjt a vállalati eszköz aktuális állapotáról, és frissítéseket hajt végre a konfigurációs és szoftverösszetevőkre.

A vállalati CDM-rendszer információkat nyújt a házirend-motor számára a hozzáférési kérelmet benyújtó eszközről, például arról, hogy fut-e a megfelelő javított operációs rendszer (OS), a vállalati jóváhagyott szoftverösszetevők integritása vagy a nem jóváhagyott összetevők jelenléte és hogy az eszköznek van-e ismert sebezhetősége.

A CDM-rendserek felelősek a házirendek egy részhalmazának azonosításáért és esetleges érvényesítéséért is a vállalati infrastruktúrán aktív, nem vállalati eszközökön.

# Iparági megfelelőségi rendszer

Ez biztosítja, hogy a vállalkozás továbbra is megfeleljen minden olyan szabályozási rendszernek, amely alá eshet (pl. FISMA, egészségügyi vagy pénzügyi ágazat információbiztonsági követelményei).

Ez magában foglalja az összes szabályzatot, amelyet a vállalat a megfelelés biztosítására dolgoz ki.

# Fenyegetés-információs hírfolyam(ok)

Belső vagy külső forrásokból származó információkat biztosít, amelyek segítik a házirend-motort a hozzáférési döntések meghozatalában.

Ezek több szolgáltatás is lehetnek, amelyek belső és/vagy több külső forrásból vesznek adatokat, és információkat szolgáltatnak az újonnan felfedezett támadásokról vagy sebezhetőségekről.

Ez magában foglalja a szoftverben újonnan felfedezett hibákat, az újonnan azonosított rosszindulatú programokat és az egyéb eszközök elleni jelentett támadásokat is, amelyekhez a házirend-motor meg akarja tagadni a hozzáférést a vállalati eszközöktől.

# Hálózati és rendszertevékenységi naplók

Ez a vállalati rendszer összesíti az eszköznaplókat, a hálózati forgalmat, az erőforrás-hozzáférési műveleteket és egyéb eseményeket, amelyek valós idejű (vagy közel valós idejű) visszajelzést adnak a vállalati információs rendszerek biztonsági helyzetéről.

# Adathozzáférési szabályzatok

Ezek a vállalati erőforrásokhoz való hozzáférésre vonatkozó attribútumok, szabályok és szabályzatok.

Ez a szabálykészlet kódolható (a felügyeleti felületen keresztül) vagy dinamikusan generálható a házirend-motor által.

Ezek a házirendek jelentik az erőforrásokhoz való hozzáférés engedélyezésének kiindulópontját, mivel alapvető hozzáférési jogosultságokat biztosítanak a vállalati fiókokhoz és alkalmazásokhoz/szolgáltatásokhoz.

Ezeknek a politikáknak a szervezet meghatározott küldetési szerepein és igényein kell alapulniuk.

# Vállalati nyilvános kulcsú infrastruktúra (PKI)

Ez a rendszer felelős a vállalat által erőforrásoknak, alanyoknak, szolgáltatásoknak és alkalmazásoknak kiadott tanúsítványok létrehozásáért és naplózásáért.

Ez magában foglalja a globális tanúsító hatóság ökoszisztemáját és a szövetségi PKI-t is,<sup>4</sup> amely lehet integrálva a vállalati PKI-vel, de lehet, hogy nem.

Ez egy olyan PKI is lehet, amely nem X.509-tanúsítványokra épül.

# Azonosítókezelő rendszer

Ez felelős a vállalati felhasználói fiókok és identitásrekordok létrehozásáért, tárolásáért és kezeléséért (pl. könnyű címtárelérési protokoll (LDAP) szerver).

Ez a rendszer tartalmazza a szükséges tárgyinformációkat (pl. név, e-mail cím, tanúsítványok) és egyéb vállalati jellemzőket, például szerepkört, hozzáférési attribútumokat és hozzárendelt eszközöket.

Ez a rendszer gyakran más rendszereket (például PKI-t) használ a felhasználói fiókokhoz társított műtermékekhez.

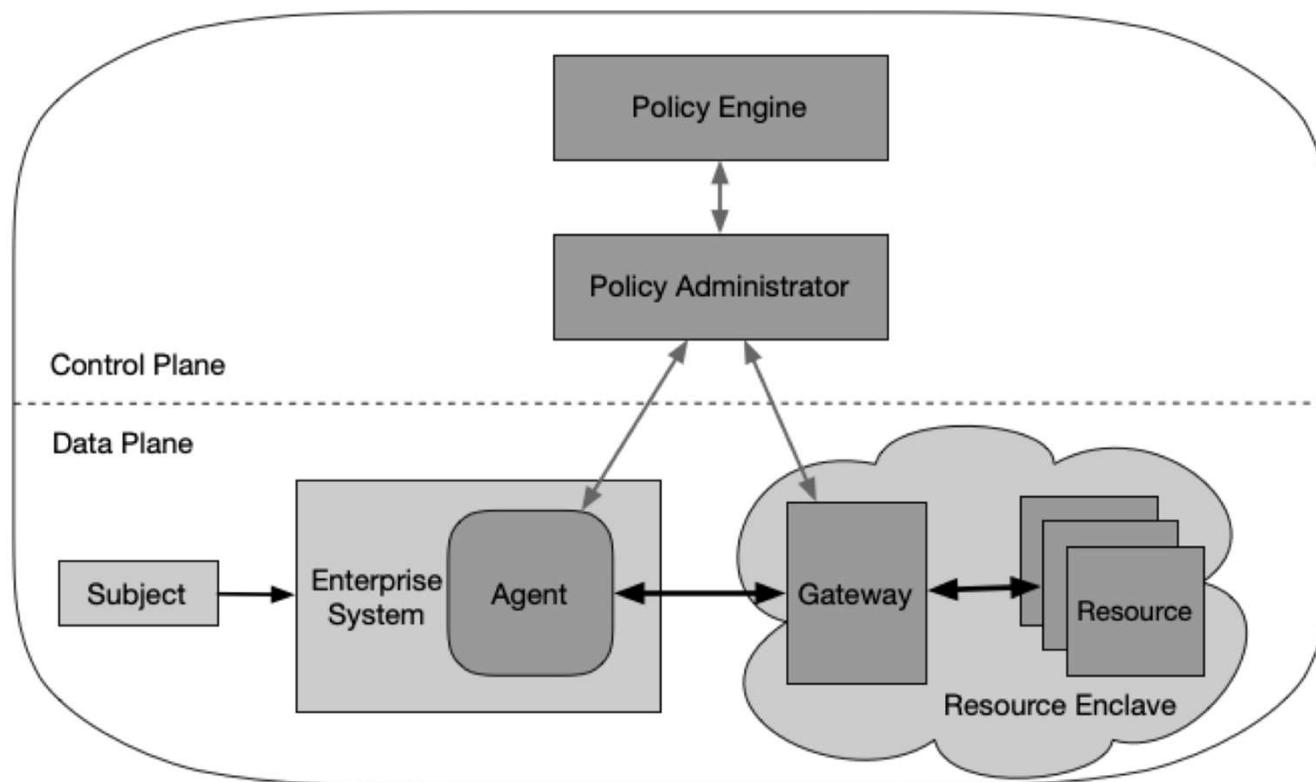
Ez a rendszer egy nagyobb szövetségi közösség része lehet, és nem vállalati alkalmazottakat vagy nem vállalati eszközökre mutató hivatkozásokat tartalmazhat az együttműködés érdekében.

# Biztonsági információ- és eseménykezelő (SIEM) rendszer

Ez biztonsági központú információkat gyűjt a későbbi elemzéshez.

Ezeket az adatokat azután a házirendek finomítására és a vállalati eszközök elleni lehetséges támadásokra való figyelmeztetésre használják.

# Példa ZTA



**Figure 4: Enclave Gateway Model**

# Bevezetés a kiberbiztonságba és biztonság tudatosság

Digitális identitás

Szarvák Anikó

2023. Tavasz

# Jogosultság kezelési módszerek, megoldások

- Access Control List – ACL,
  - Discretionary Access Control – DAC,
  - Mandatory Access Control – MAC,
  - Role Based Access Control – RBAC,
  - Attribute Based Access Control – ABAC,
  - Bell-LaPadula modell
  - Clark-Wilson modell
- + Megvalósítások.

# ACL

A számítógépes biztonságban a hozzáférés-vezérlési lista (ACL) a rendszererőforráshoz (objektumhoz) társított engedélyek listája.

Az ACL meghatározza, hogy mely felhasználók vagy rendszerfolyamatok kapnak hozzáférést az objektumokhoz, valamint hogy milyen műveletek engedélyezettek az adott objektumokon.

A tipikus ACL minden bejegyzése meghatároz egy tárgyat és egy műveletet. Például, ha egy fájlobjektum rendelkezik ACL-lel, amely tartalmazza

# DAC

A számítógépes biztonságban a diszkrecionális hozzáférés-szabályozás (DAC) egyfajta hozzáférés-szabályozás, amelyet a Trusted Computer System Evaluation Criteria (TCSEC) határoz meg, amely eszközként korlátozza az objektumokhoz való hozzáférést az alanyok és/vagy csoportok identitása alapján tartoznak.

Az ellenőrzések diszkrecionálisak abban az értelemben, hogy egy bizonyos hozzáférési engedéllyel rendelkező alany képes ezt az engedélyt (talán közvetetten) átadni bármely más alanynak (hacsak nem korlátozza a kötelező hozzáférés-szabályozás).

# MAC

A számítógépes biztonságban a kötelező hozzáférés-szabályozás (**MAC**) a hozzáférés-szabályozás egy olyan típusát jelenti, amellyel az operációs rendszer vagy az adatbázis korlátozza az alany vagy a kezdeményező azon képességét, hogy hozzáférjen egy objektumhoz vagy célhoz, vagy általában valamilyen műveletet hajtson végre azokon.

Az operációs rendszerek esetében az alany általában egy folyamat vagy szál; Az objektumok olyan konstrukciók, mint a fájlok, könyvtárak, TCP/UDP portok, megosztott memória szegmensek, IO-eszközök stb.

**Az alanyok és objektumok mindegyike rendelkezik biztonsági attribútumokkal.**

# RBAC

A számítógépes rendszerek biztonsága, a szerepkör-alapú hozzáférés-vezérlés (RBAC) vagy a szerepalapú biztonság egy olyan megközelítés, amely a rendszerhez való hozzáférést az engedélyezett felhasználókra korlátozza.

Ez egy megközelítés a kötelező hozzáférés-vezérlés (MAC) vagy a diszkrecionális hozzáférés-vezérlés (DAC) megvalósítására.

A szerepkör alapú hozzáférés-vezérlés egy házirend-semleges hozzáférés-vezérlési mechanizmus, amely szerepkörök és jogosultságok köré épül.

# ABAC

Az attribútum-alapú hozzáférés-vezérlés (ABAC), más néven IAM szabályzatalapú hozzáférés-vezérlés, egy hozzáférés-vezérlési paradigmát határoz meg, amelyben az alany jogosultságát egy műveletkészlet végrehajtására az alanyhoz, objektumhoz, kért műveletekhez társított attribútumok kiértékelése határozza meg, és bizonyos esetekben a környezeti jellemzők is.

Az ABAC egy olyan hozzáférés-vezérlési házirendek megvalósítási módja, amely nagymértékben adaptálható, és az attribútumok széles skálájával testreszabható, így alkalmas elosztott vagy gyorsan változó környezetben való használatra.

# Bell-Lapadula modell

A Bell–LaPadula Modell (BLP) egy állapot-gép-modell, amelyet kormányzati és katonai alkalmazások hozzáférés-szabályozásának kikényszerítésére használnak.

David Elliott Bell és Leonard J. LaPadula fejlesztette ki Roger R. Schell határozott útmutatása nyomán az US Védelmi Minisztérium (DoD) többszintű biztonsági (MLS) szabályozására.

A modell a számítógépes biztonsági politika formális állapot-átmeneti modellje, amely olyan hozzáférés-szabályozási követelményeket ír le, amelyek biztonsági címkéket használnak az objektumokon és engedélyeket az alanyok számára.

A biztonsági címkék a legérzékenyebbtől (pl. "Szigorúan titkos"), egészen a legkevésbé érzékenyekig (pl. "Nem minősített" vagy "Nyilvános") terjedhetnek.

A Bell–LaPadula modell egy olyan modell példája, ahol nincs egyértelmű különbség a védelem és a biztonság között.

# Clark-Wilson modell

A Clark-Wilson integritási modell alapot biztosít egy számítástechnikai rendszer integritási szabályzatának meghatározásához és elemzéséhez.

A modell elsősorban az információs integritás fogalmának formalizálására irányul. Az információk integritását azáltal tartják fenn, hogy megakadályozzák a rendszerben lévő adatelemek sérülését hiba vagy rosszindulatú ok esetén.

Az integritási szabályzat leírja, hogy a rendszerben lévő adatelemekeket hogyan kell érvényben tartani a rendszer egyik állapotától a másikig, és meghatározza a rendszerben lévő különféle állapotok követelményeit.

A modell biztonsági címkeket használ, hogy hozzáférést biztosítson az objektumokhoz átalakítási eljárásokon és egy korlátosított interfész modellen keresztül.

# Megoldások

- LDAP
- Kerberos
- AD
- SAML
- OpenID

# LDAP

Az LDAP a Lightweight Directory Access Protocol rövidítése. Ez a protokoll directory szolgáltatások elérését szabályozza.

LDAP RFC: <https://ldap.com/ldap-related-rfcs/>

Az LDAP-protokollnak számos megvalósítása van, mint például:

- OpenLDAP,
- Apple Open Directory,
- Microsoft Active Directory.

# AD

Az Active Directory, röviden AD a Microsoft egyes hálózati szolgáltatásainak gyűjtőneve, ezek:

- X.500-alapú, LDAPv3 protokollal lekérdezhető, elsősorban Microsoft Windows-környezetben használatos címtárszolgáltatás;
- Kerberos protokoll-alapú autentikáció;
- DNS-alapú névszolgáltatás és egyéb hálózati információk.

## AD (folyt.)

Egy Active Directory-címtár legmagasabb szintje az erdő (forest), ami egy vagy több bizalmi kapcsolatokkal (trust) összekötött tartományt (domain) magába foglaló egy vagy több fa (tree) összessége. A tartományokat DNS-beli névterük azonosítja. A címtár objektumait a Directory Information Tree (címtárinformációs fa, DIT) adatbázisa tárolja, ami három partícióra bomlik, ezek:

- az objektumok tulajdonságait leíró sémapartíció (schema partition),
- az erdő szerkezetét (tartományokat, fákat, helyeket) leíró konfigurációs partíció(configuration partition) és
- a tartomány objektumait tartalmazó tartományi partíció (domain partition). Ezekben kívül létezhetnek alkalmazáspartíciók (application partition) is.

# Kerberos

A Kerberos egy számítógépes hálózati hitelesítési protokoll, amely egy nem biztonságos hálózaton keresztül úgy teszi lehetővé a csomópontok közötti kommunikációt, hogy biztonságos módon igazolják személyazonosságukat egymás felé.

Tervezőinek elsődleges célja egy kliens-szerver modell volt, amely kölcsönös hitelesítést nyújt mind a kliens, mind a szerver számára, hogy egymás személyazonosságát megállapíthassák.

A Kerberos protokoll üzenetei védve vannak a lehallgatások és az ismétlődő támadások ellen (replay attacks). A Kerberos a szimmetrikus kulcsú titkosításon alapszik, amelyhez egy „megbízható harmadik fél” szükséges: opcionálisan, a hitelesítés egyes fázisaiban – az aszimmetrikus kulcsú titkosítást felhasználva – publikus kulcsú titkosítást is választhatunk.

(A Kerberos a Massachusetts Institute of Technology (MIT) által kiadott és alkalmazott protokoll, amely egy ingyenes szoftvercsomag is egyben. A Kerberos alapértelmezettként a 88-as portot használja.)

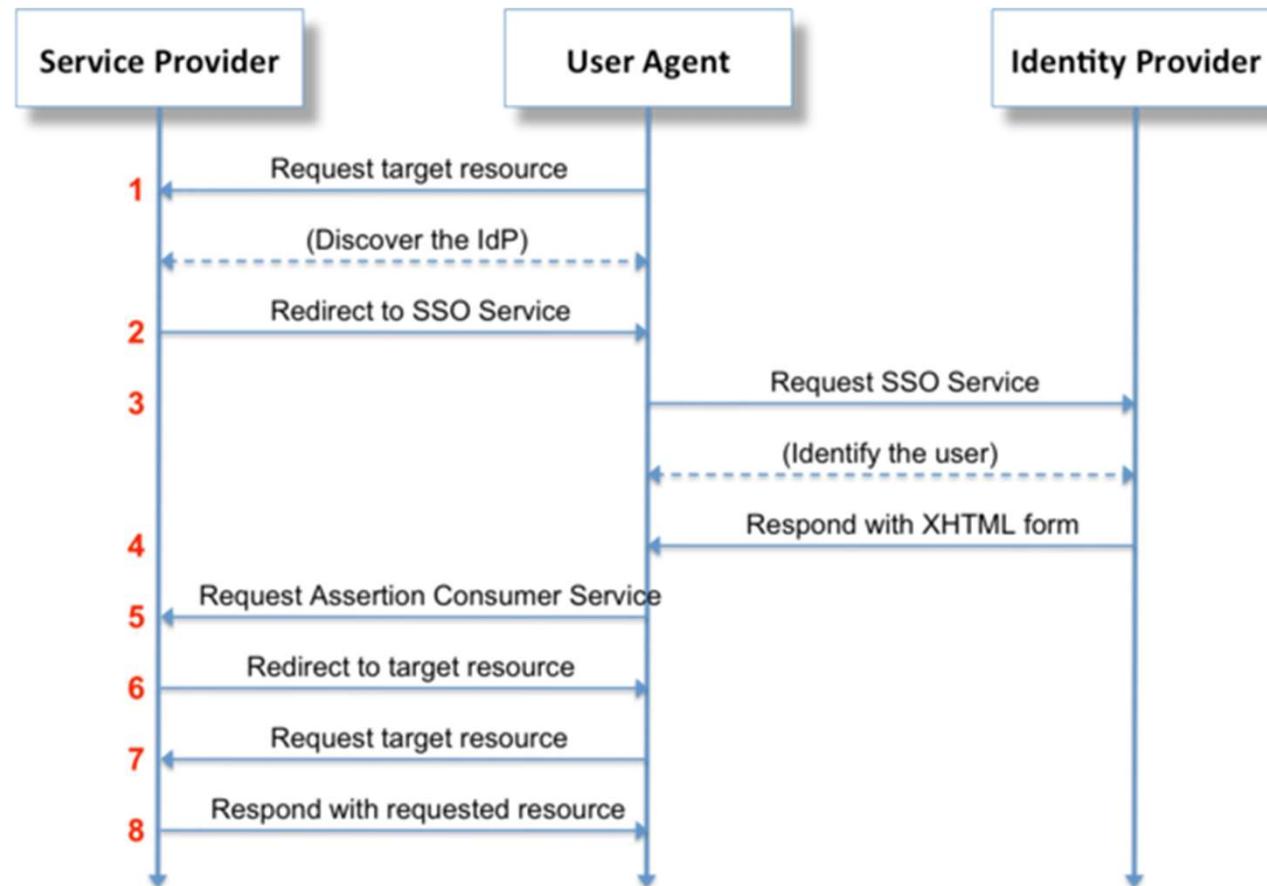
# SAML

A SAML a Security Assertion Markup Language rövidítése.

Ez egy XML-alapú nyílt szabvány az identitásadatok átvitelére két fél között: egy identitásszolgáltató (IdP) és egy szolgáltató (SP) között.

Identity Provider – Hitelesítést hajt végre, és átadja a felhasználó identitását és jogosultsági szintjét a szolgáltatónak.

# Single Sign On – SAML



<https://commons.wikimedia.org/wiki/File:Saml2-browser-sso-redirect-post.png>

# OpenID

Az OpenID egy nyílt szabványú és decentralizált hitelesítési protokoll, amelyet a non-profit OpenID Foundation támogat.

Lehetővé teszi a felhasználók hitelesítését együttműködő webhelyek (úgynevezett támaszkodó felek, vagy RP) által harmadik féltől származó identitásszolgáltató (IDP) szolgáltatással, így nincs szükség arra, hogy saját, ad hoc bejelentkezési rendszert biztosítsanak.

Lehetővé teszi a felhasználók számára, hogy bejelentkezzen több, nem kapcsolódó webhelyre anélkül, hogy mindenekhez külön azonosítóval és jelszóval kellene rendelkeznie.

A felhasználók egy OpenID identitásszolgáltató kiválasztásával hoznak létre fiókokat, majd ezekkel a fiókokkal bejelentkezhetnek bármely olyan webhelyre, amely elfogadja az OpenID hitelesítést.

Számos nagy szervezet ad ki vagy fogad el OpenID-t a webhelyén.

[https://openid.net/specs/openid-authentication-2\\_0.html](https://openid.net/specs/openid-authentication-2_0.html)

# Bevezetés a kiberbiztonságba és biztonságtudatosság

## Kiberbiztonsági eszközök

Szarvák Anikó

2023. Tavasz

# Alapfogalmak

## Biztonság

- Kockázat, fenyegetés, sérülékenység

## Kontrollok:

- Adminisztratív vs technikai
- Preventív, detektív, korrektív

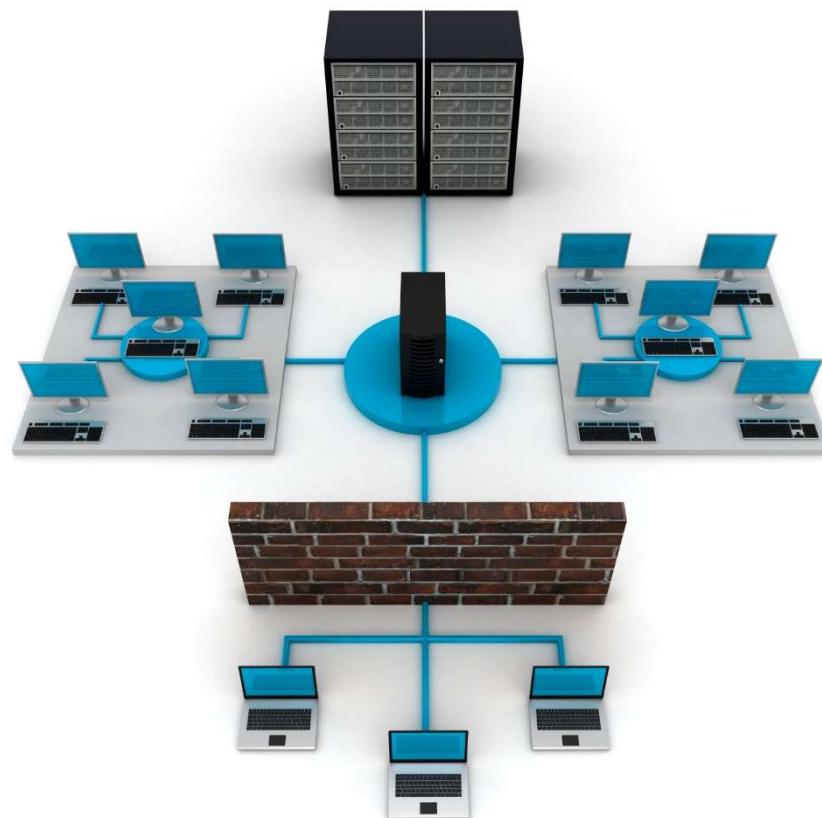
## Biztonsági alkalmazások

- FW, IDS/IPS, UTM, DLP, UBA, STB, HBR

## Biztonsági esemény, DF, IR, SOC

# Informatikai rendszer

= információs rendszer?



# Adminisztratív kontrollok



# Technikai kontrollok



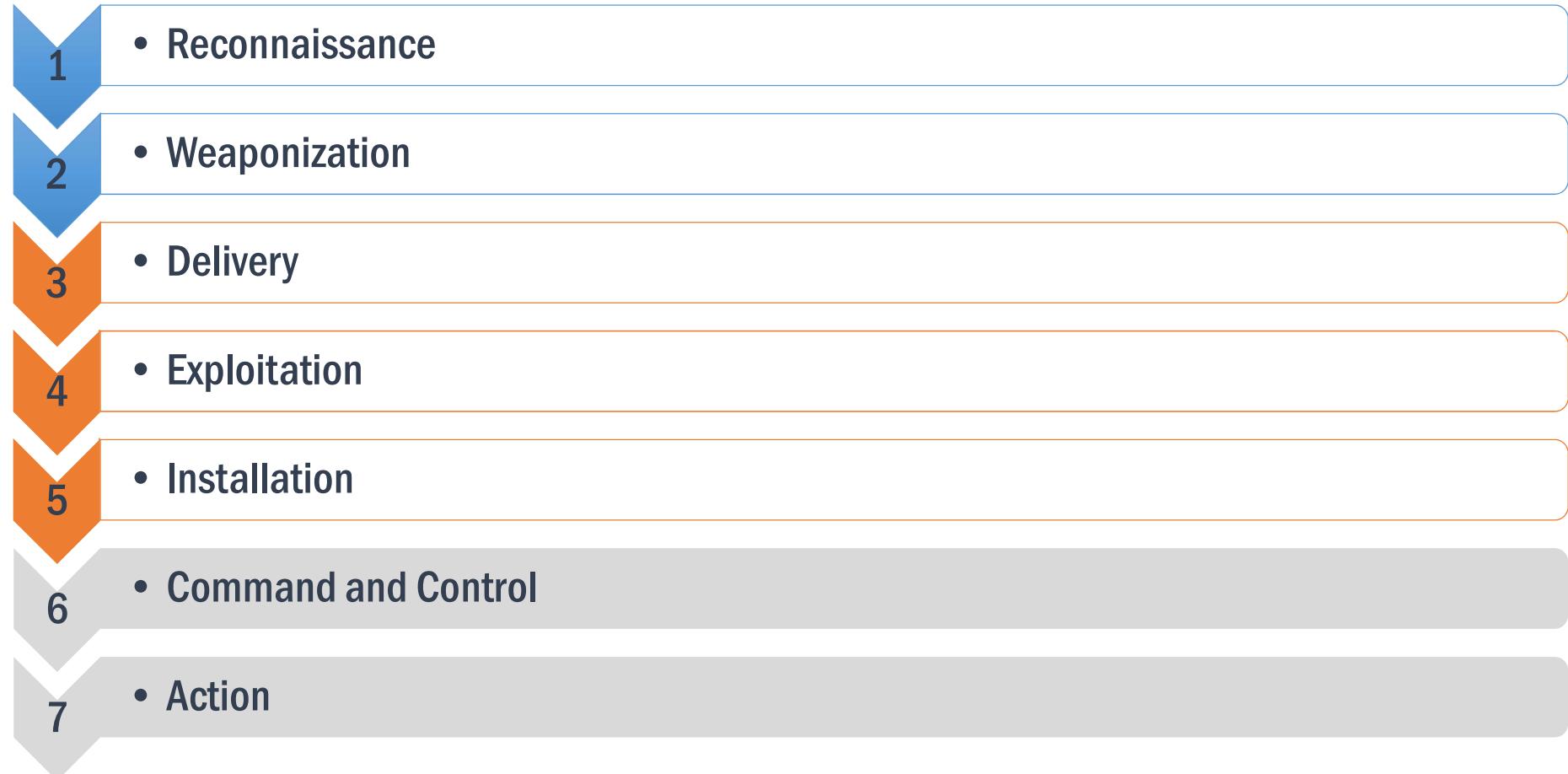
Layer	Application/Example	Central Device/ Protocols	DOD4 Model
<b>Application (7)</b>  Serves as the window for users and application processes to access the network services.	<b>End User layer</b> Program that opens what was sent or creates what is to be sent  Resource sharing • Remote file access • Remote printer access • Directory services • Network management	<b>User Applications</b>  SMTP	
<b>Presentation (6)</b>  Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	<b>Syntax layer</b> encrypt & decrypt (if needed)  Character code translation • Data conversion • Data compression • Data encryption • Character Set Translation	JPEG/ASCII EBDIC/TIFF/GIF PICT	Process
<b>Session (5)</b>  Allows session establishment between processes running on different stations.	<b>Synch &amp; send to ports</b> (logical ports)  Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.	<b>Logical Ports</b>  RPC/SQL/NFS NetBIOS names	
<b>Transport (4)</b>  Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	<b>TCP</b> Host to Host, Flow Control  Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	F I L T E R P A C K E T Routers IP/IPX/ICMP	Host to Host
<b>Network (3)</b>  Controls the operations of the subnet, deciding which physical path the data takes.	<b>Packets</b> ("letter", contains IP address)  Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		Internet
<b>Data Link (2)</b>  Provides error-free transfer of data frames from one node to another over the Physical layer.	<b>Frames</b> ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end)  Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control	Switch Bridge WAP PPP/SLIP	Can be used on all layers
<b>Physical (1)</b>  Concerned with the transmission and reception of the unstructured raw bit stream	<b>Physical structure</b> Cables, hubs, etc.  Data Encoding • Physical medium attachment • Physical layer addressing	Hub	Network

# OWASP

	2007	2010	2013	2017
1	Cross Site Scripting (XSS)	Injection	Injection	Injection
2	Injection	Cross Site Scripting (XSS)	Broken Authentication and Session Management	Broken Authentication
3	Malicious File Execution	Broken Authentication and Session Management	Cross Site Scripting (XSS)	Sensitive Data Exposure
4	Insecure Direct Object Reference	Insecure Direct Object References	Insecure Direct Object References	XML External Entities
5	Cross Site Request Forgery (CSRF)	Cross Site Request Forgery (CSRF)	Security missconfiguration	Broken Access Control
6	Information Leakage and Improper Error Handling	Security missconfiguration	Sensitive Data Exposure	Security Misconfiguration
7	Broken Authentication and Session Management	Insecure Cryptographic Storage	Missing Function Level Access Control	Cross-Site Scripting (XSS)
8	Insecure Cryptographic Storage	Failure to Restrict URL Access	Cross Site Request Forgery (CSRF)	Insecure Deserialization
9	Insecure Communication	Insufficient Transport Layer Protection	Using Components with Known Vulnerabilities	Using components with known vulnerabilities
10	Failure to Restrict URL Access	Unvalidated Redirects and Forwards	Unvalidated Redirects and Forwards	Insufficient Logging and Monitoring

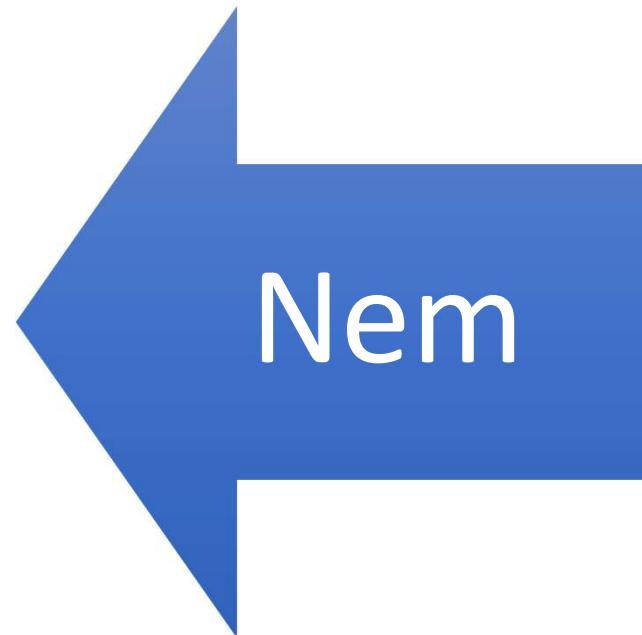
[https://www.owasp.org/images/7/72/OWASP\\_Top\\_10-2017\\_%28en%29.pdf.pdf](https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf)

# APT

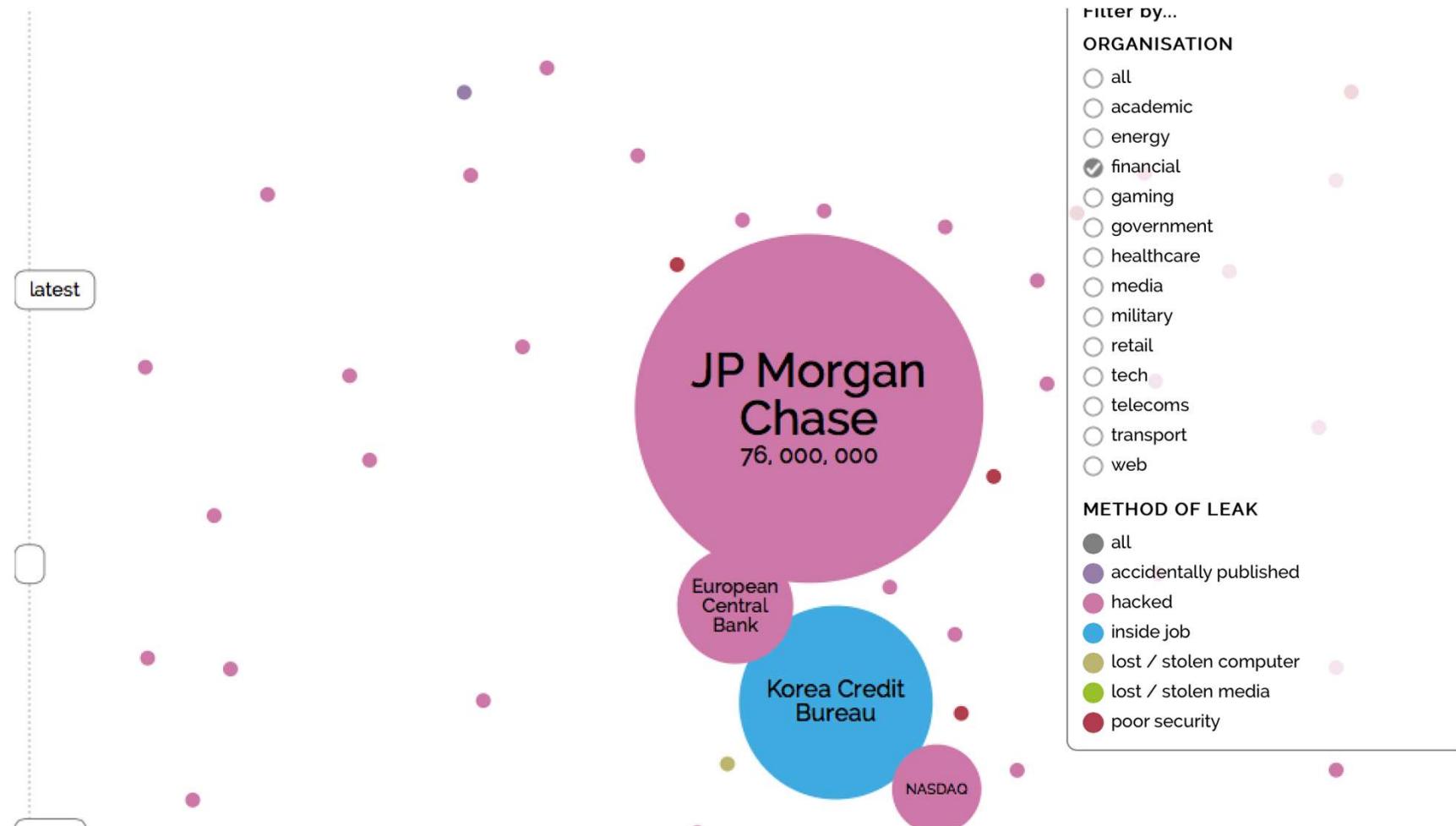


# Betörés

Nem az a kérdés, történik-e betörés. A kérdés az, mikor?!



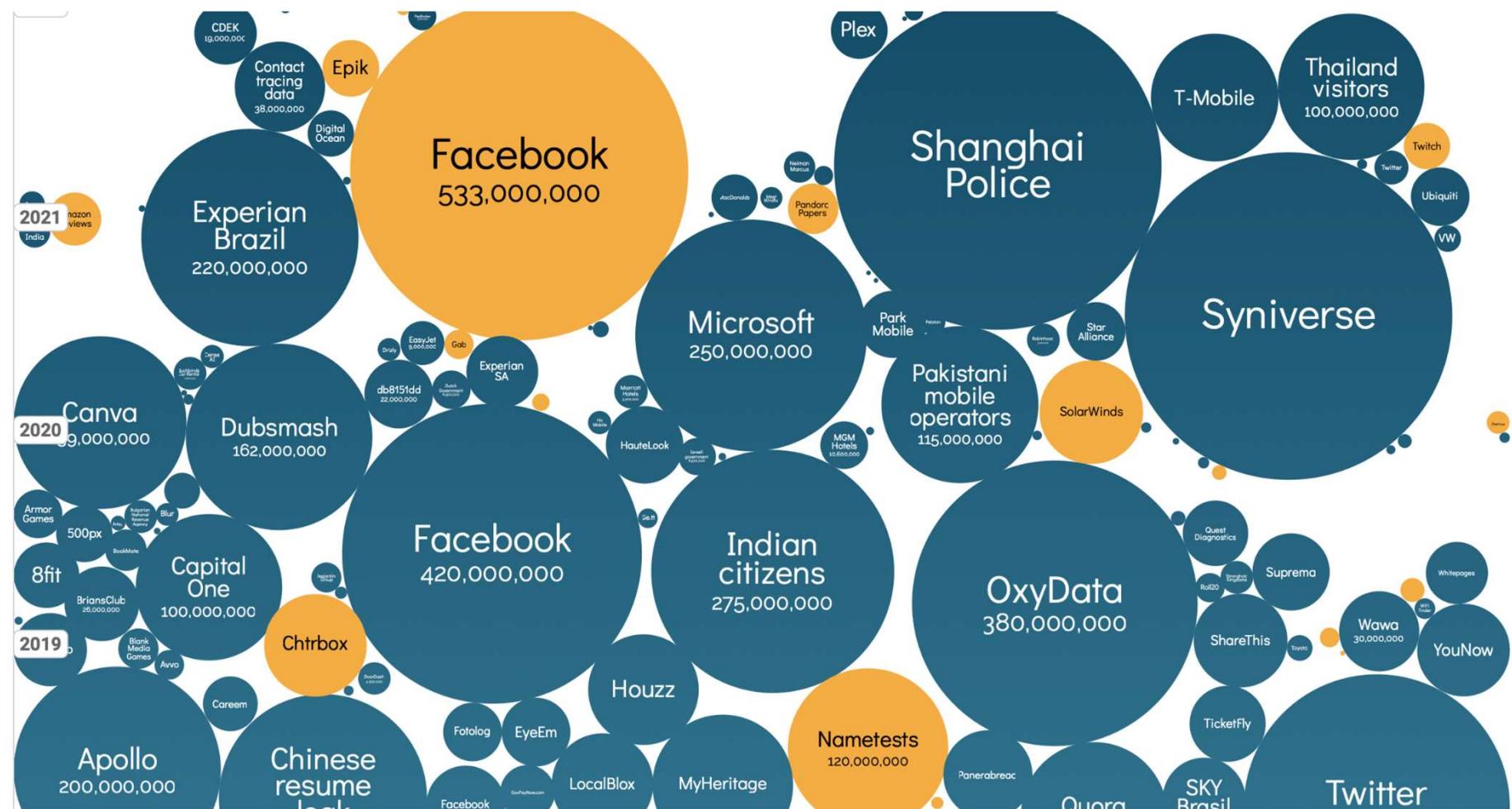
# World biggest databreaches 2015 / finance

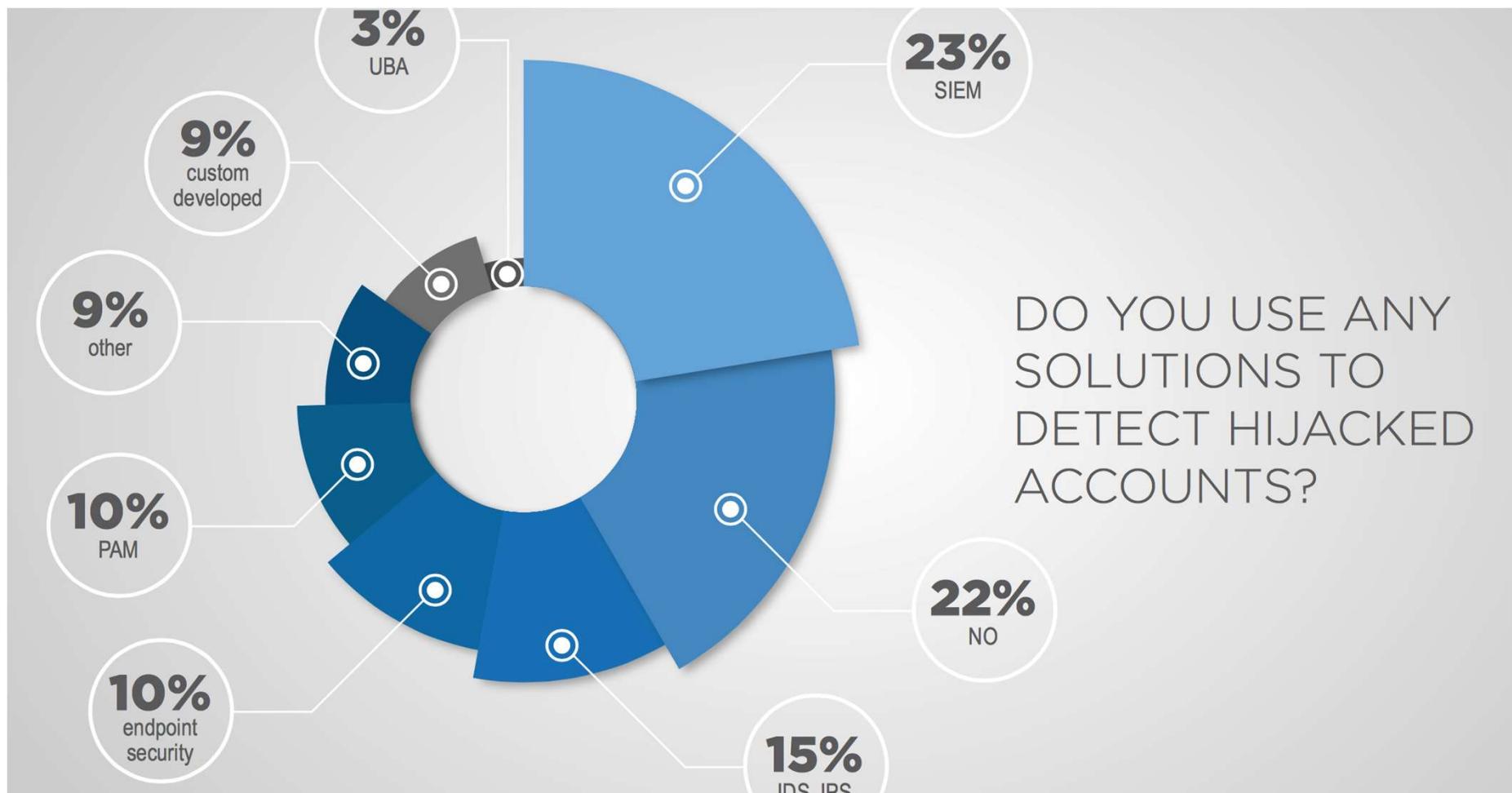


# World biggest databreaches latest / finance

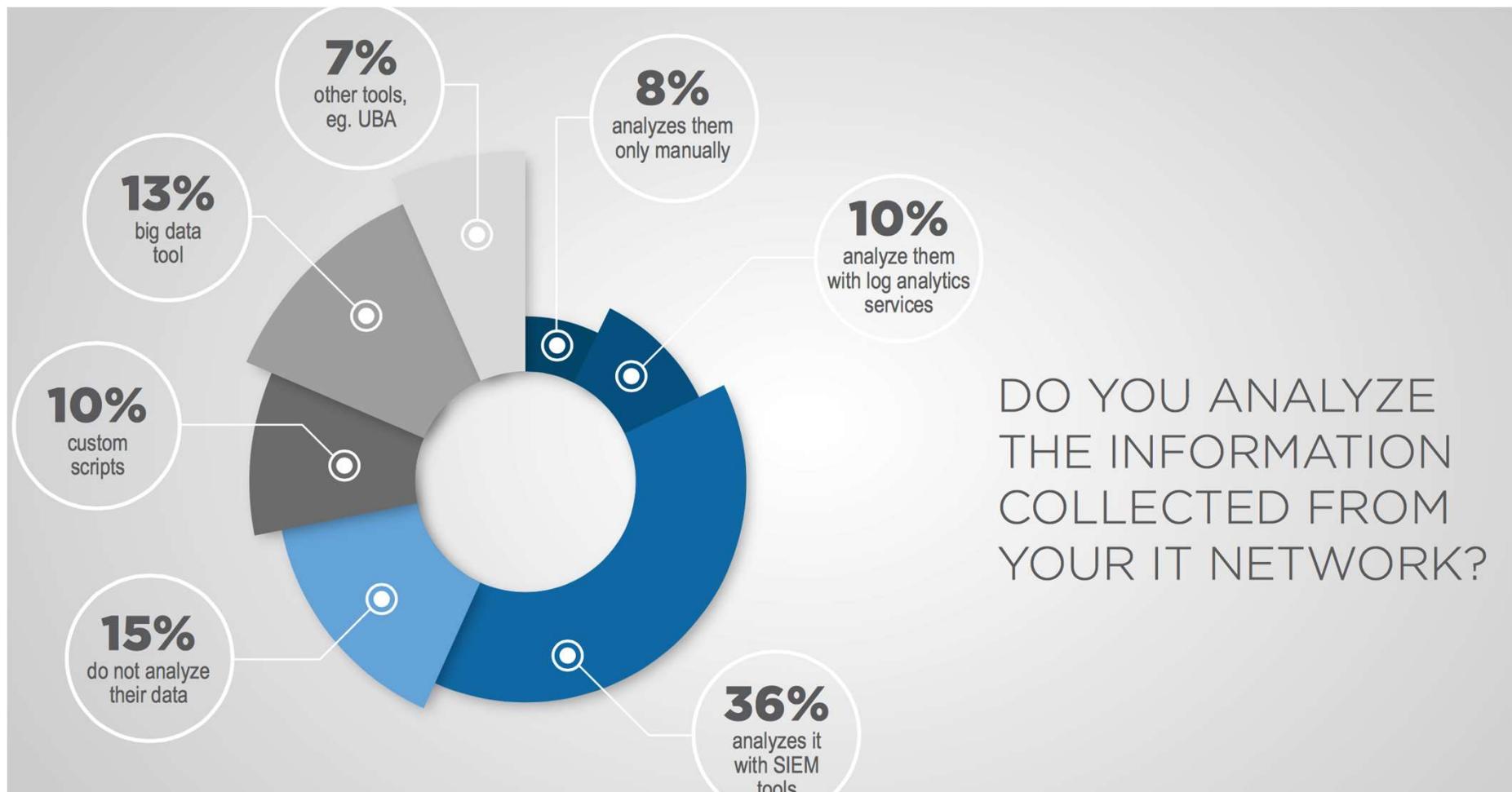


# World biggest databreaches – latest





[https://andrea.blogs.balabit.com/files/2015/11/Balabit\\_CSI\\_Survey\\_Infographic\\_Final.pdf](https://andrea.blogs.balabit.com/files/2015/11/Balabit_CSI_Survey_Infographic_Final.pdf)



[https://andrea.blogs.balabit.com/files/2015/11/Balabit\\_CSI\\_Survey\\_Infographic\\_Final.pdf](https://andrea.blogs.balabit.com/files/2015/11/Balabit_CSI_Survey_Infographic_Final.pdf)

# Schneier on Security



Blog Newsletter Books Essays News Schedule Crypto About Me

[← Petition the U.S. Government to Force the TSA to Follow the Law](#)

[All-or-Nothing Access Control for Mobile Phones](#)

**Dropped USB Sticks in Parking Lot as Actual Attack Vector**

For years, it's been a clever trick to [drop USB sticks in parking lots](#) of unsuspecting businesses, and track how many people plug them into computers. I have long argued that the problem isn't that people are plugging the sticks in, but that the computers trust them enough to run software off of them.

This is the [first time](#) I've heard of criminals trying this trick.

Tags: [cybercrime](#), [flash drives](#), [malware](#), [social engineering](#)

Posted on July 12, 2012 at 9:47 AM • 31 Comments

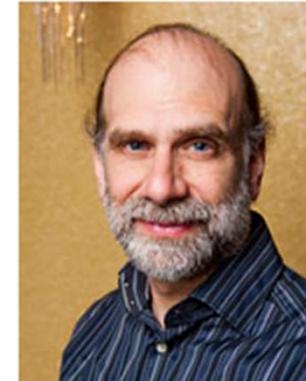
**Search**  
Powered by DuckDuckGo

**Go**

blog  essays  whole site

**Subscribe**

**About Bruce Schneier**



## Stories

[Home](#) • [News](#) • [Stories](#) • [2015](#) • [January](#) • [Ransomware on the Rise](#)

Nyelv kiválasztása

 [Get FBI Updates](#)

### Latest Ransomware Threat

A fairly new ransomware variant has been making the rounds lately. Called CryptoWall (and CryptoWall 2.0, its newer version), this virus encrypts files on a computer's hard drive and any external or shared drives to which the computer has access. It directs the user to a personalized victim ransom page that contains the initial ransom amount (anywhere from \$200 to \$5,000), detailed instructions about how to purchase Bitcoins, and typically a countdown clock to notify victims how much time they have before the ransom doubles. Victims are infected with CryptoWall by clicking on links in malicious e-mails that appear to be from legitimate businesses and through compromised advertisements on popular websites. According to the U.S. CERT, these infections can be devastating and recovery can be a difficult process that may require the services of a reputable data recovery specialist.

For more information on ransomware in general, visit the U.S. CERT website.

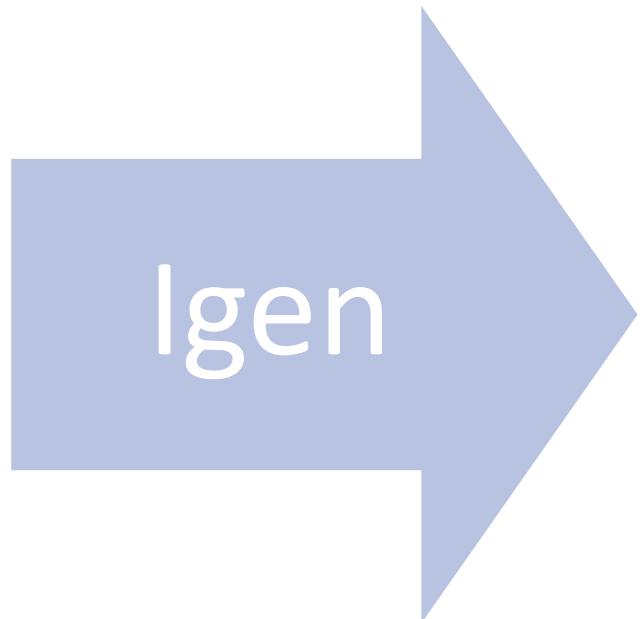
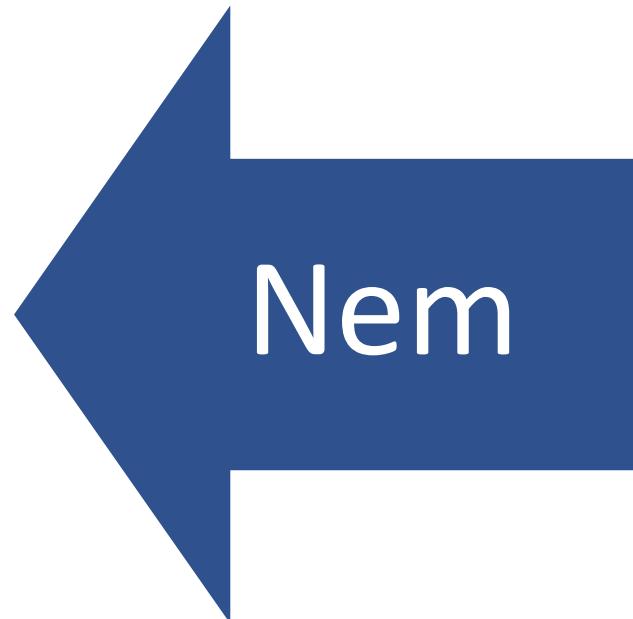
### Protect Your Computer from Ransomware

- Make sure you have updated antivirus software on your computer.
- Enable automated patches for your operating system and web browser.
- Have strong passwords, and don't use the same passwords for everything.
- Use a pop-up blocker.
- Only download software—especially free software—from sites you know and trust (malware can also come in downloadable games, file-sharing programs, and customized toolbars).
- Don't open attachments in unsolicited e-mails, even if they come from people in your contact list, and never click on a URL contained in an unsolicited e-mail, even if you think it looks safe. Instead, close out the e-mail and go to the organization's website directly.
- Use the same precautions on your mobile phone as you would on your computer when using the Internet.
- To prevent the loss of essential files due to a ransomware infection, it's recommended that individuals and businesses always conduct regular system back-ups and store the backed-up data offline.

<http://www.fbi.gov/news/stories/2015/january/ransomware-on-the-rise/ransomware-on-the-rise>

# Észlelés

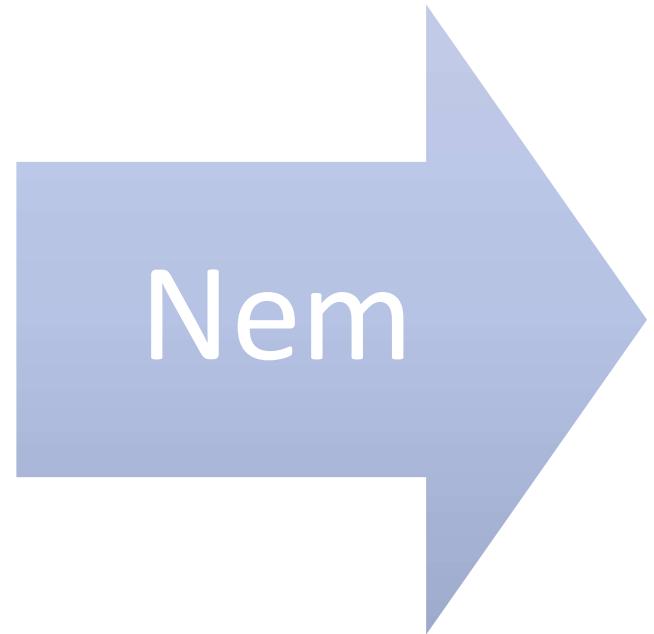
Biztonsági incidens, ha a rendszergazda nem tud bejelentkezni?



# Visszaállítás

Hátsó bejáratot hoztak létre, mert felülírták az “sshd”-t a szerveren.

Elég a “backdoor” hozzáférés tiltása?



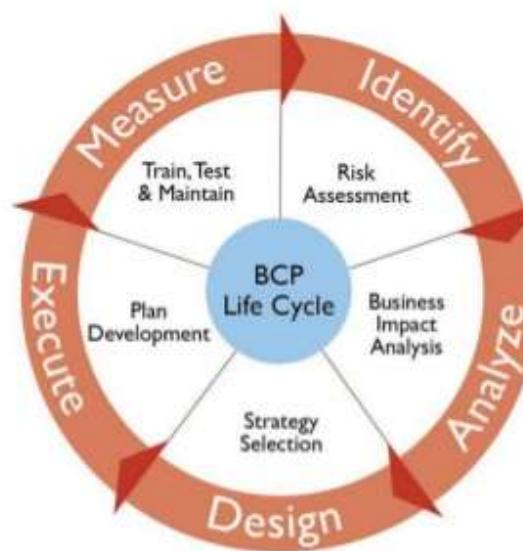
# Bevezetés a kiberbiztonságba - Biztonság tudatosság

Üzletmenet-folytonosság tervezése

Bonifert Tamás

2023. 05. 18.

# Mi az üzletmenet-folytonosság tervezés?

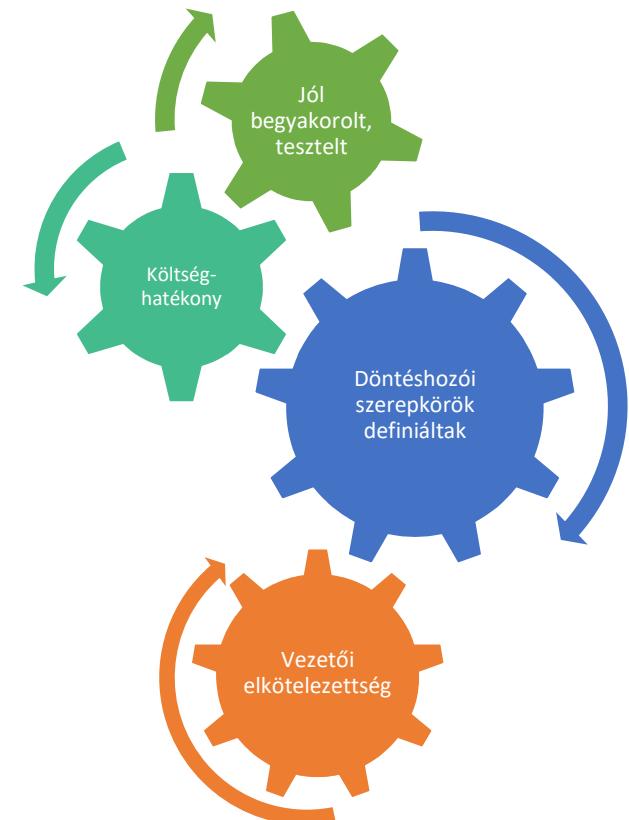


Forrás: ISO 22301, Stay in Business

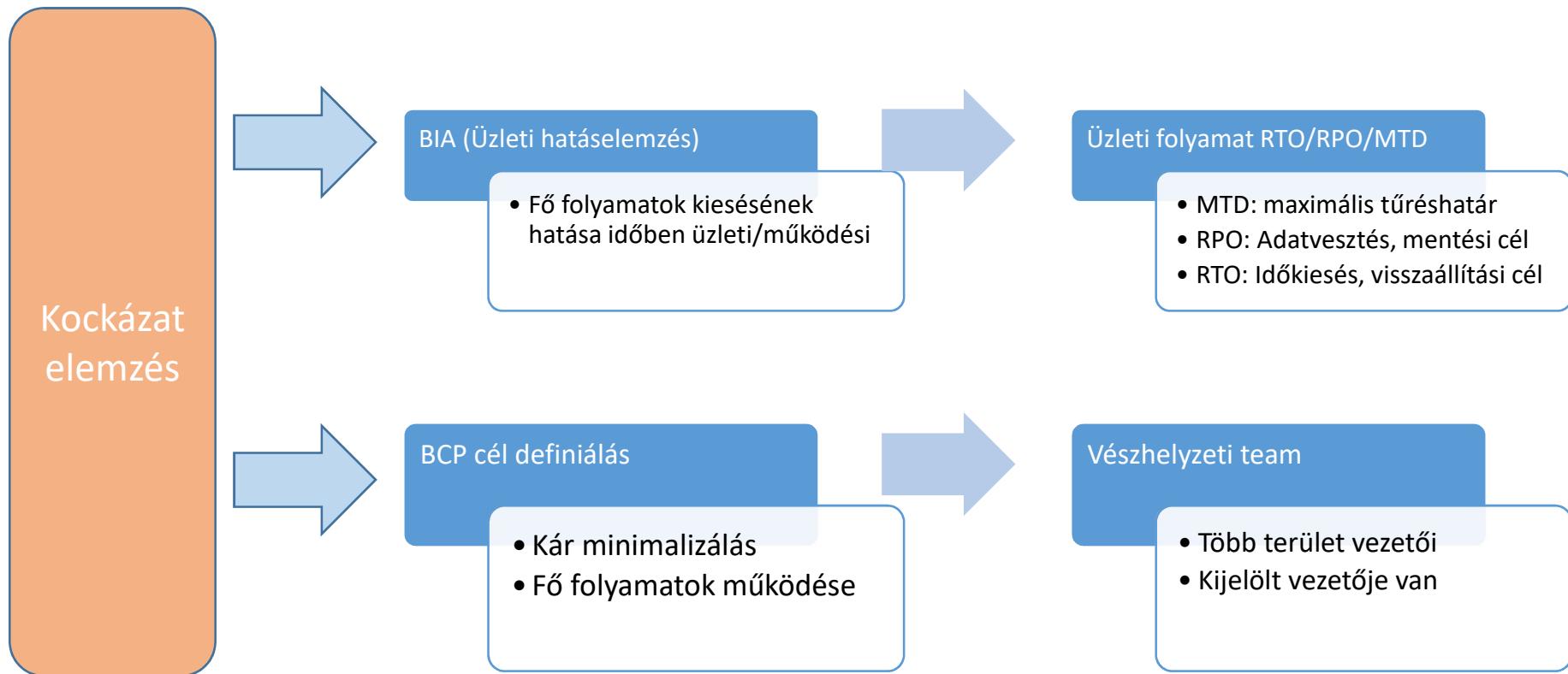
- Az a folyamat, melynek során a szervezet felkészül az üzleti folyamatok kiesés utáni visszaállítására, kár minimalizálással
- Kockázat menedzsment képezi az alapját: mire kell felkészülni?
- Az üzleti területek bevonása alapvető: az üzleti terület határozza meg a kiesések hatását, és az elfogadható kiesési időt: BIA
- Tartalmaz alternatív üzleti folyamatokat, illetve a támogató IT rendszer előkészítését, és visszaállítási lépéseit
- Folyamatos működtetést, tesztelést, karbantartást, és képzést igényel
- BCDR: a rendszer leállás utáni visszaállítása (DRP), és az üzleti folyamatok folyamatossága (BCP) egy egységet képez

# BCDR sikerkritériumok

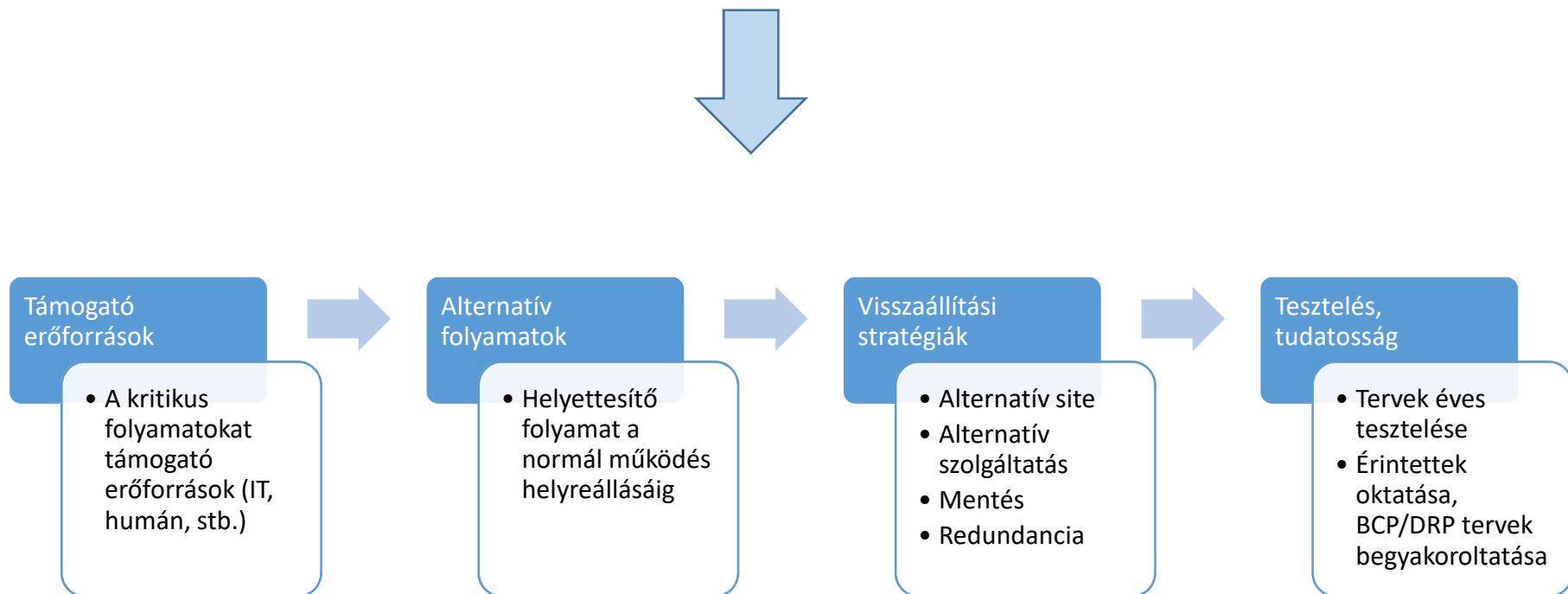
- minden érintett tudja, hogy mi a dolga leállás esetén: jól begyakorolt, letesztelt BCP/DRP tervezet
- Költséghatékony: minél gyorsabban kell visszaállítani egy folyamatot, annál drágább a DRP stratégia -> üzleti hatáselemzés
- Definiált döntéshozói szerepkörök: katasztrófahelyzet esetén létfontosságú a fejetlenség elkerülése. Világos döntésekre van szükség, melyhez dedikált szerepkörökre van szükség.
- Vezetői elkötelezettség és jóváhagyás



# BCDR folyamata



# BCDR folyamata



# Üzleti hatáselemzés (BIA) és a BCDR kapcsolata



1. Az üzleti terület meghatározza a kritikus folyamatokat és kiesésük hatását
2. Az üzleti terület meghatározza a kritikus adatköröket és az adatvesztési toleranciát
3. Az IT terület a kritikus folyamatokhoz meghatározza a támogató IT erőforrásokat
4. A BIA eredménye
  - a kritikus folyamatok MTD értékei
  - Erőforrások, IT rendszerek felé támasztott RTO értékek
  - a kritikus adatok RPO értékei, mentési stratégia

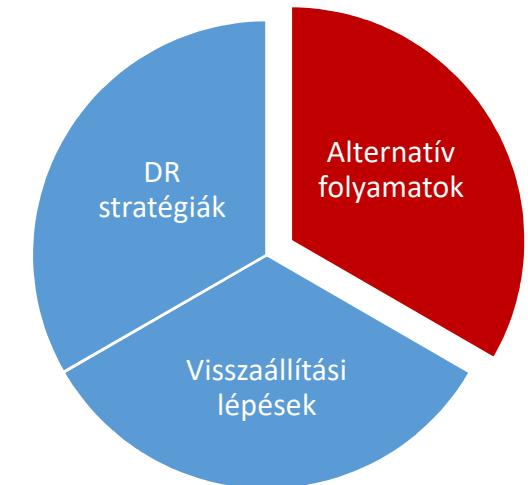
# Üzleti hatáselemzés (BIA)

- Tisztán üzleti elemzés, nem műszaki
- Célja, hogy meghatározza a leállás által okozott kárt
- minden üzleti folyamathoz meghatározza az MTD értéket
- Meghatározza, hogy az MTD-n túli leállás naponta, hetente mekkora kárt okoz
- A hatás lehet kvalitatív (hírnév), vagy kvantitatív (anyagi)
- Interjús módszerrel végezzük egy területi vezető és egy szakértő dolgozó bevonásával
- Tartsuk szem előtt, hogy minél kisebb az MTD, annál drágább lesz a DRP stratégia

NEM ELEMZI A LEÁLLÁS OKÁT, CSAK AZ OKOZOTT KÁRT AZ IDŐ FÜGGVÉNYÉBEN

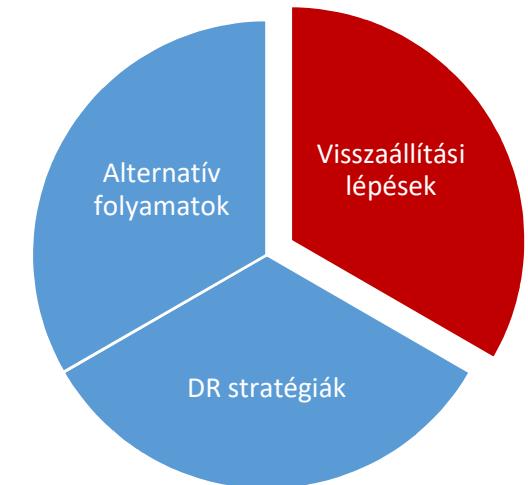
# Alternatív folyamatok (BCP)

- Üzletmenet-folytonossági tervezés része
- Proaktívabb megközelítés, mint a DRP
- Alternatív folyamatokat fejleszt ki arra az esetre, ha az IT rendszer leáll
- Biztosítja, hogy a kritikus folyamatok a leállás alatt is működjenek (pl. papíros könyvelés)
- Holisztikusabb megközelítés, vállalat fókuszú
- Rendszeres tesztelése, gyakorlása szükséges, hogy jól begyakorolt legyen, és naprakészen illeszkedjen az eredeti folyamathoz



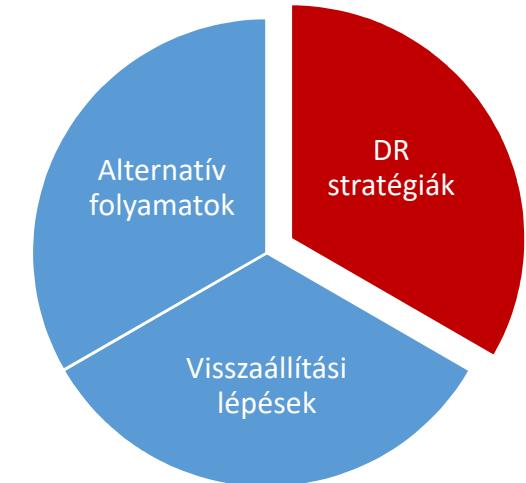
# Visszaállítási lépések (DRP)

- Katasztrófa-elhárítási tervezés része
- Reaktív megközelítés, az incidens megtörténtére indulnak a lépések
- Célja, hogy az IT rendszert a meghatározott idő alatt vissza lehessen állítani eredeti működési szintre.
- Technológiai fókuszú megközelítés
- Rendszeres tesztelése, gyakorlása szükséges, hogy előjöjjenek az IT rendszerek hibái, a DRP előkészületek hiányosságai



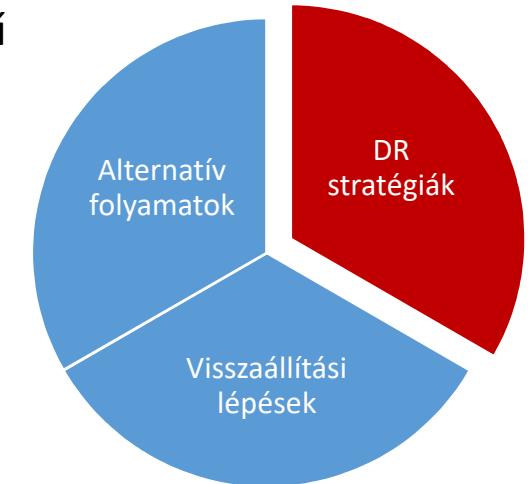
# DR stratégiák

- Alternatív site: minél jobban előkészített, annál drágább
  - Tükör site: minden rendszer és tranzakciós teljesen azonos az eredeti telephellyel
  - Hot site: Azonos hardver és szoftver környezet az eredeti telephellyel
  - Warm site: Speciális hardverek nem állnak rendelkezésre, csak minimális
  - Cold site: Csak a kábelezés, és a hely áll rendelkezésre
- Alternatív szolgáltatói szerződés: ilyen például egy másodlagos internet szolgáltató
- Alternatív adatközpont: a szervezet saját maga üzemeltet georedundáns szervertermet
- Redundáns szerverek: A szerverek cluster párokban dolgoznak, és az egyik kiesése esetén a másik átveszi a feladatát

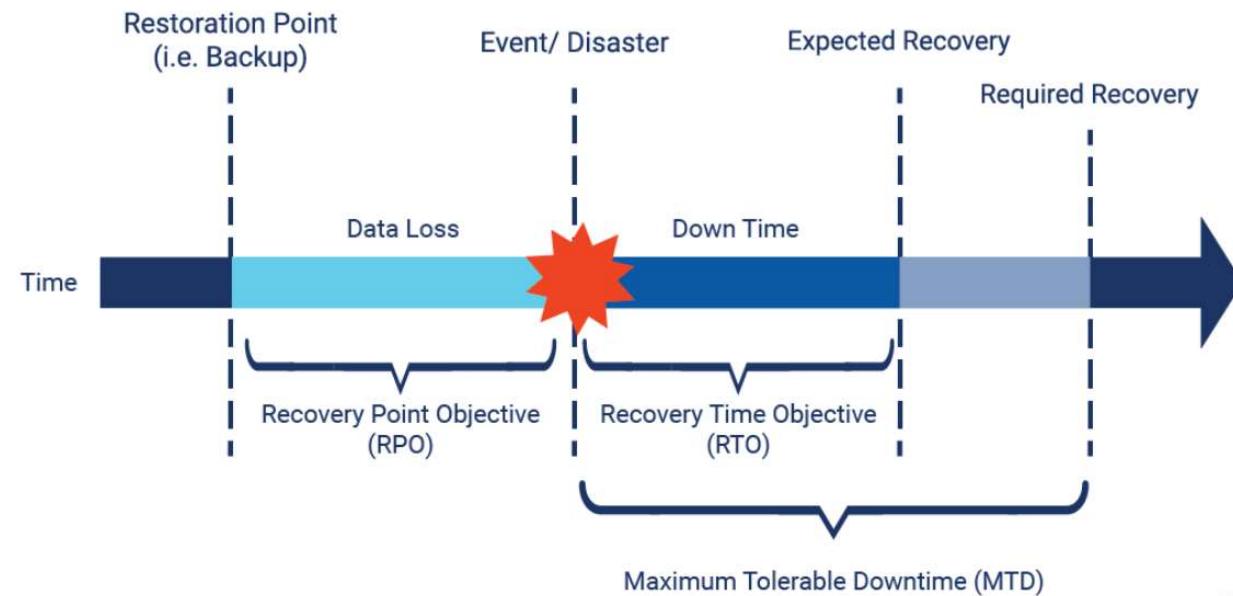


# DR stratégiák

- Mentés: az adatokat menteni kell, és a mentéseket célszerű földrajzilag elkülönített helyen tárolni, védeni. Típusai:
  - Teljes mentés: minden adatot mentünk. Leginkább tárhely igényes
  - Inkrementális mentés: minden változás után a módosult részt mentjük. A visszaállításhoz az utolsó teljes, és az összes inkrementális mentés kell.
  - Differenciális mentés: minden változás után a módosult részt mentjük. A visszaállításhoz az utolsó teljes, és az utolsó differenciális mentés kell.
  - Folyamatos mentés: minden adatváltozást azonnal mentünk.

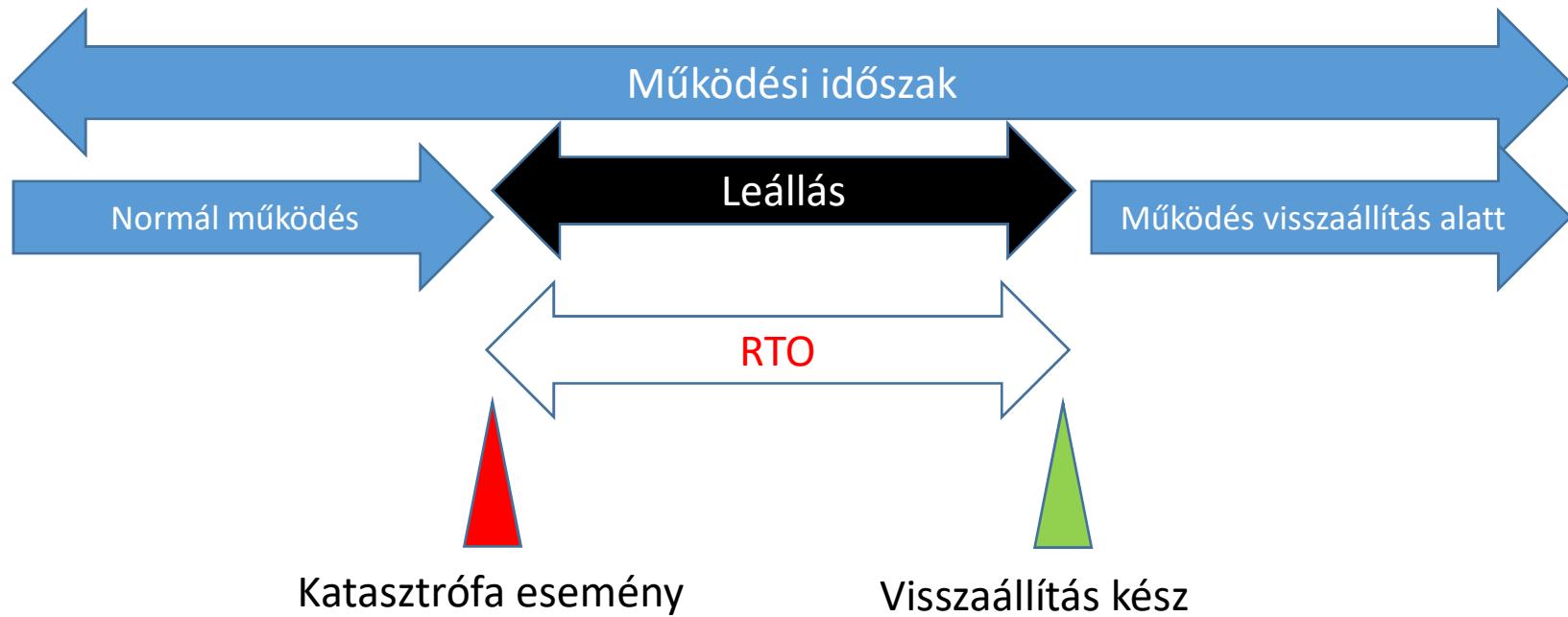


# DRP mérőszámok



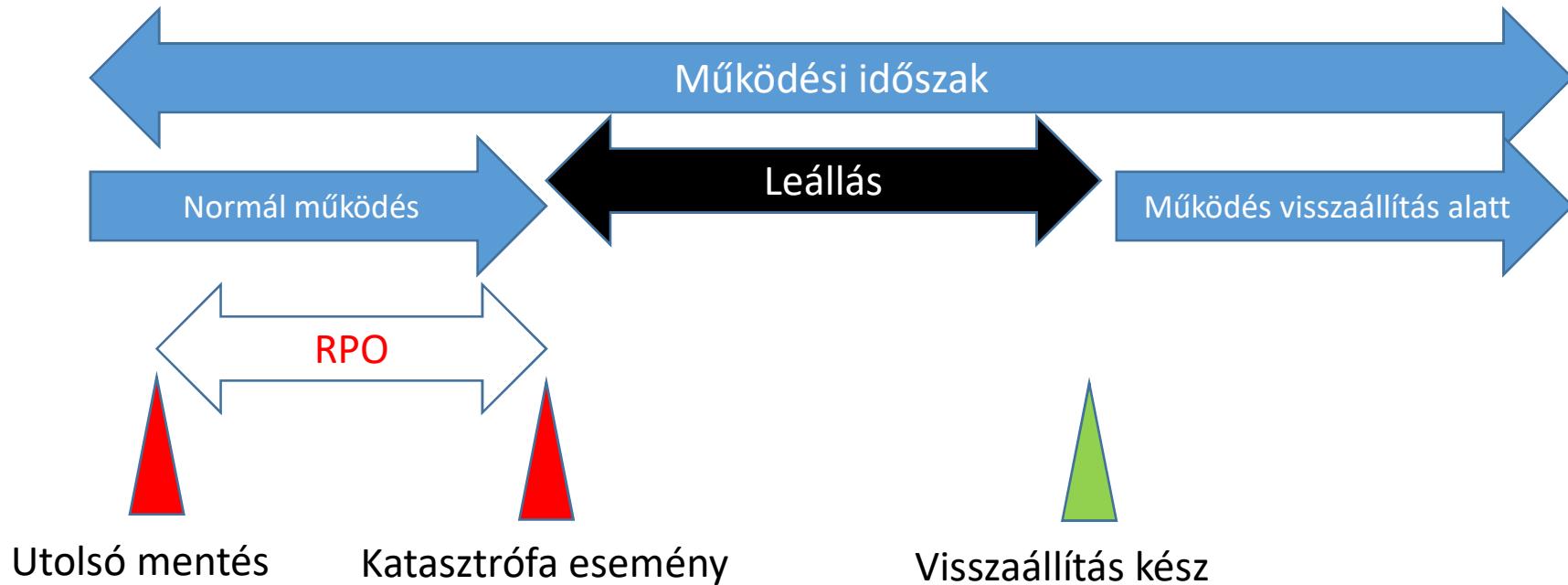
- **Recovery Point Objective (RPO):** Adatvesztés tolerancia. A katasztrófától visszafelé a maximum időtartam, mely adatainak elvesztése visszafordíthatatlan kárt okoz.
- **Recovery Time Objective (RTO):** A rendszer tervezett visszaállítási időtartama, hogy ne érje el az MTD-t, azaz a maximális elviselhető leállást.
- **Maximum Tolerable Downtime (MTD):** Maximum leállási idő, amit a folyamat képes tolerálni

# Recovery Time Objective



- RTO: az az időtartam, melyet az üzlet az IT szolgáltatás teljes elérhetetlensége esetén elvisel. Ez az idő áll rendelkezésre ahhoz, hogy a DRP megoldás visszaállítsa a működést.
- Az üzlet határozza meg, nem pedig a DRP megoldás.
- Úgy kell meghatározni, hogy a DRP megoldás ne legyen költségesebb, mint a kiesés

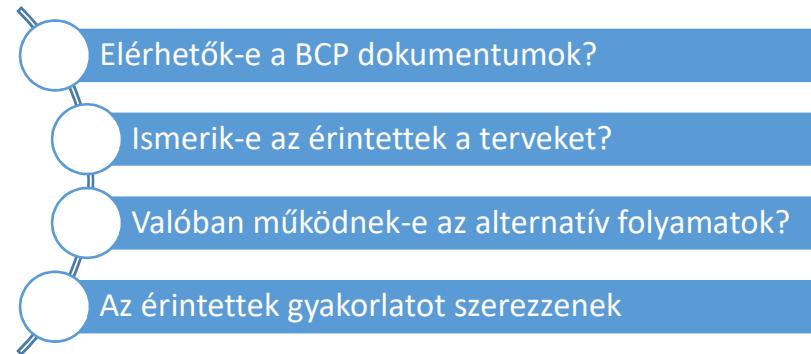
# Recovery Point Objective



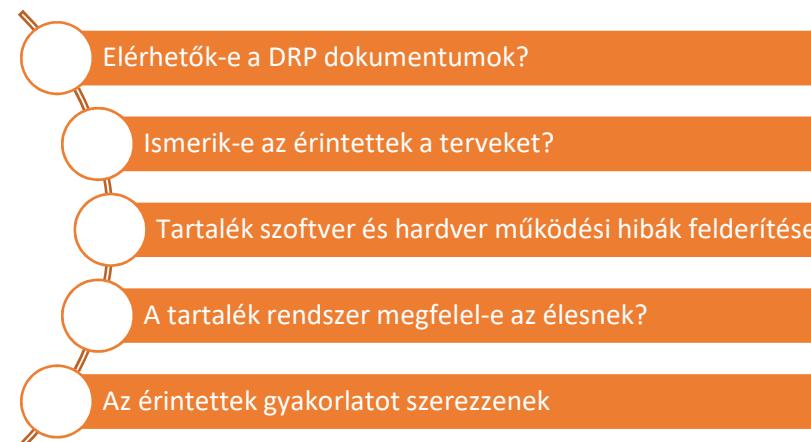
- RPO: A katasztrófától visszafelé a maximum időtartam, mely adatainak elvesztése visszafordíthatatlan kárt okoz. Gyakorlatilag az utolsó mentés időpontját adja meg.
- Az üzlet határozza meg, nem pedig a DRP megoldás.
- Úgy kell meghatározni, hogy a DRP megoldás ne legyen költségesebb, mint a kiesés (pl. tárhely költség)

# BCDR tesztelés

Miért teszteljük a BCP terveket?



Miért teszteljük a DRP terveket?



# BCDR tesztelés típusai

## Asztali gyakorlat

- Az asztali gyakorlat (tabletop testing) egy elméleti teszt, melynek során brainstorming jelleggel a résztvevők végig beszélnek, hogy kinek mi a szerepe és feladata egy leállás esetén.

## BCP/DRP terv átvizsgálás

- A terv átvizsgálás során szintén elméleti síkon a résztvevők részletesen átnézik a terv lépéseit, és végig gondolják annak megvalósíthatóságát.

## Checklist teszt

- A checklist alapú teszt a legegyszerűbb. Ennek során az érintettek kapnak egy listát a felkészülési feladatokról, a kontaktokról, szerepkörök ről. A teszt során ezt a listát kell ellenőrizni.

## Szimulációs teszt

- Akár BCP, akár DRP tesztről van szó, a szimulációs teszt során egy rész folyamat/rendszer leállását szimulálják, és erre hajtják végre a tervet. A leállás kontrollált és behatárolt.

## Párhuzamos teszt

- A párhuzamos teszt során kipróbálják, hogy a tartalék rendszerek teljes kapacitással ki tudják-e szolgálni a folyamatokat. A teszt során az éles rendszerek párhuzamosan üzemelnek.

## Real/teljes teszt

- A real, vagy teljes teszt során az éles rendszert valóban leállítják, és kipróbálják, hogy a tartalék rendszer el tudja-e látni a feladatát.

# KÖSZÖNÖM A FIGYELMET!

## Kérdések?

# Bevezetés a kiberbiztonságba - Biztonságtudatosság

## Social Engineering

Bonifert Tamás

2023. 05. 25.

# Tartalom

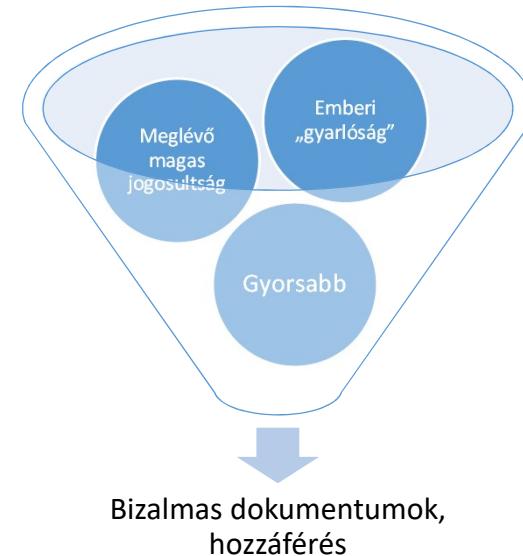
## Social engineering típusú támadások

- Fogalom
- Social Engineering támadások típusainak ismertetése
- Védekezés, biztonsági kontrollok

# Social Engineering támadás

„A leggyengébb láncszem a felhasználó”

- A támadó nem, vagy nem csak technikai módszerekkel ér el eredményt
- Nem a rendszereket, hanem az embert, a felhasználót támadja
- Pszichológiai módszerek: bizalom megszerzése, manipuláció, megtévesztés
- Az emberek önként tesznek meg lépéseket



# Social Engineering támadás

## ADATHALÁSZAT (PHISHING)

- Személyes, vagy bizalmas adat megszerzésének kísérlete megtévesztés által
- A támadó megbízható félnek, vagy jól ismert szervnek adja ki magát
- Leggyakoribb módja az e-mail phishing, de létezik telefonos, web portálos, vagy social media változata is
- Legtöbbször weboldal meglátogatására, vagy csatolmány megnyitására kér fel

### Tömeges phishing e-mail

- Legitim szervezetre hasonlító küldő domain és dizájn
- A címzett nem nevezített, bárkinek szólhat
- Sokszor kötődik sok embert érintő eseményekhez (pl. Covid teszt)

### Spear phishing (Célzott phishing)

- Célcsoportot, vagy egyetlen célszemélyt céloz meg
- Precízen megszerkesztett, személy specifikus információkat tartalmazó e-mail-ek
- OSINT kutatásnak kell megelőznie

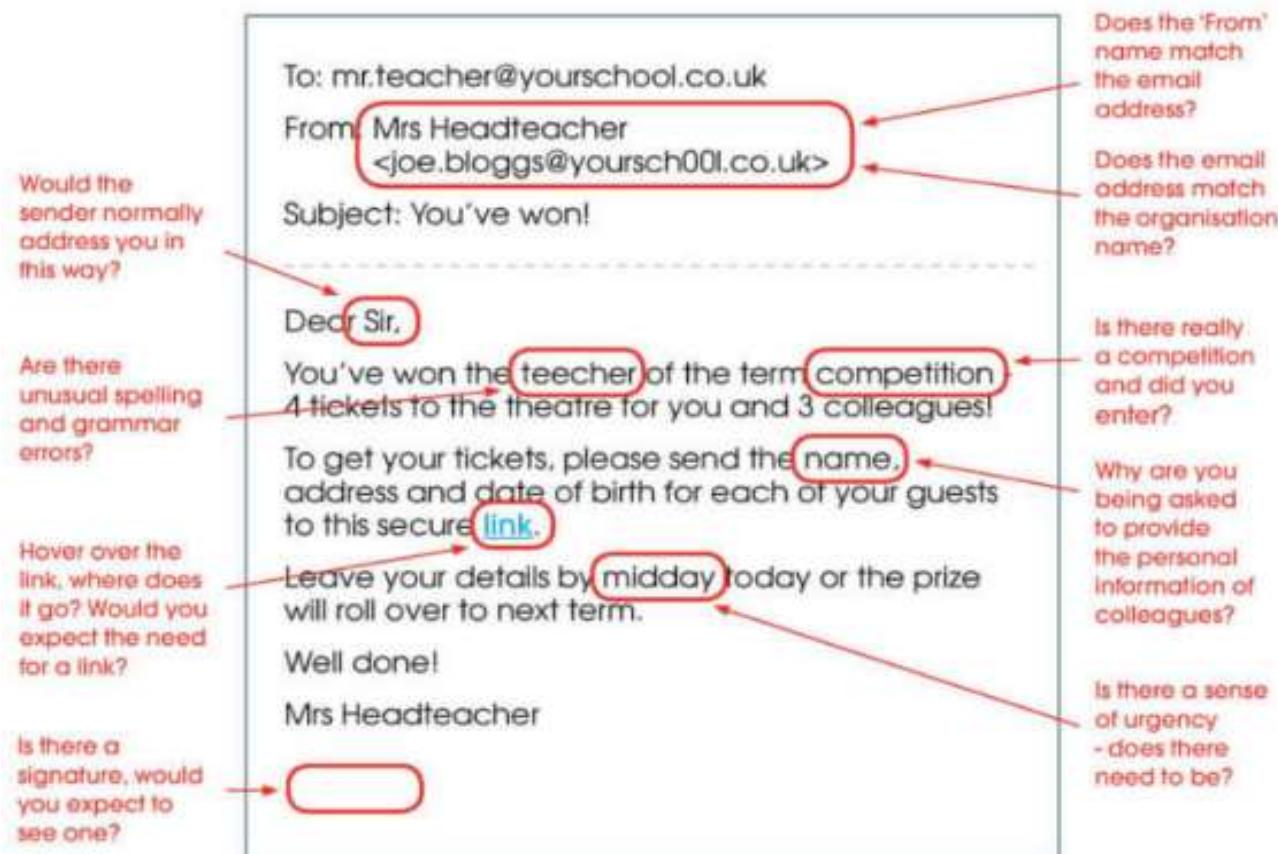
# Social Engineering támadás

## PHISING E-MAIL FELISMERÉSE

- Bár egyre szofisztikáltabbak az adathalász levelek, sok gyanús pontjuk lehet:
  - E-mail cím nem azonos a küldő szervezet nevével
  - Szokatlan, túl általános, vagy nem létező megszólítás
  - Személyes információ megadására, vagy egy oldal meglátogatására buzdít
  - Nyelvtani hibák (fordító program hiba)
  - Gyanús link, mely az egeret fölé helyezve más helyre mutat
  - Sürgetést tartalmaz
  - Semmi köze a címzettnek a levél tárgyához, tartalmához
- Technikai szinten
  - E-mail eredetiségek teszteken nem megy át: SPF,DKIM,DMARC

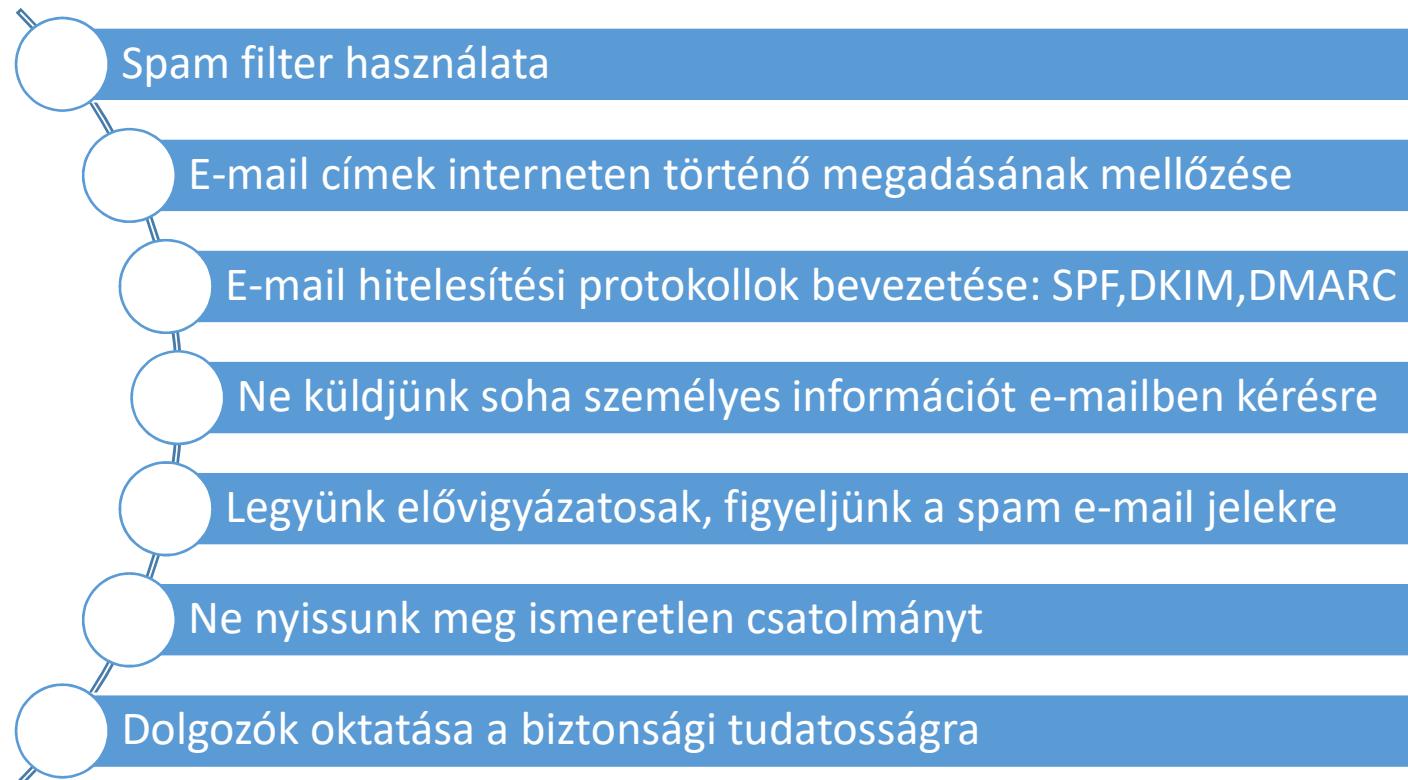
# Social Engineering támadás

## PHISING E-MAIL FELISMERÉSE



# Social Engineering támadás

## PHISING E-MAIL ELLENI VÉDEKEZÉS



# Social Engineering támadás

## PHISING E-MAIL ELLENI VÉDEKEZÉS

### SENDER POLICY FRAMEWORK (SPF)

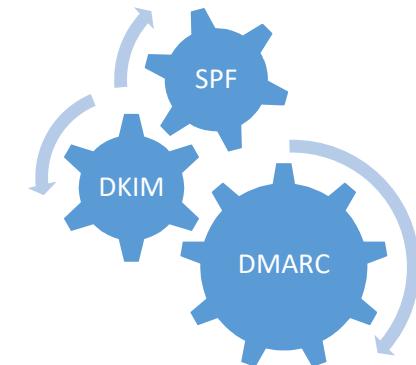
- DNS bejegyzés, ami azokat az IP címeket tartalmazza, melyek az adott domain névében levelet küldhetnek
- Ha a küldő IP nincs a megadott domain névhez regisztrálva, a spam folderbe kerül a mail

### DOMAINKEYS IDENTIFIED MAIL (DKIM)

- Digitális aláírás alapú e-mail szerver hitelesítés

### DOMAIN-BASED MESSAGE AUTHENTICATION, REPORTING & CONFORMANCE (DMARC)

- Ez a szabály mondja meg, hogy ha egy e-mail üzenet nem hiteles, mi történjen vele
- Lehetséges átengedés, spam/karentén folderbe tétele, vagy visszautasítás



# Social Engineering támadás

## CSALIZÁS (BAITING)

- Ajándék, vagy nyeremény reményén alapuló támadás
- Online és Offline típusa van
- Az ajándék malware-t tartalmaz, mely adatlopást hajt végre
- Az emberi kíváncsiságon, és az ajándék felett érzett örömön alapul



### Online baiting

- Visszautasíthatatlan ajánlatok
- Ingyenes zene, film, szoftver stb.
- Pénznyerénnel történő kecsegétek
- A nyeremény helyett malware töltődik le a linkről

### Offline baiting

- Ajándék, vagy elhagyott pendrive
- A pendrive malware-t tartalmaz
- A Social Engineering pendrive-ok kártékony kódjainak elkészítésére konkrét megoldások léteznek ingyenesen

# Social Engineering támadás

## BAITING USB PENDRIVE KÉSZÍTÉSE

- Az ajándék, vagy elszórt pendrive-ra ártó kódot telepít a támadó
- A kódnak automatikusan kell indulnia
- Mivel a kód a belső hálózatban fog futni, könnyen okoz kárt
- Metasploit framework ingyenes és egyszerű megoldás



## SOCIAL ENGINEERING TOOLKIT

Select from the menu:

- 1) Spear-Phishing Attack Vectors
- 2) Website Attack Vectors
- 3) Infectious Media Generator**
- 4) Create a Payload and Listener
- 5) Mass Mailer Attack
- 6) Arduino-Based Attack Vector
- 7) Wireless Access Point Attack Vector
- 8) QRCode Generator Attack Vector
- 9) Powershell Attack Vectors
- 10) SMS Spoofing Attack Vector
- 11) Third Party Modules



- AUTORUN.INF
- REVERSE SHELL
- SAJÁT PROGRAM

# Social Engineering támadás

## FIZIKAI HOZZÁFÉRÉS SZERZÉSE MEGTÉVESZTÉSSEL

- Számos információt szerezhet a támadó az épületbe bejutással
- Veszélyesebb, mint a távoli Social Engineering: fizikailag el lehet kapni a támadót
- Lehetőséget ad Dumpster diving, Shoulder surfing tevékenységre például
- Lényege, hogy a támadó valakit megszemélyesít: pl. karbantartó, ügyfél, új alkalmazott, így bejuthat az épületbe



# Social Engineering támadás

## KUKABÚVÁRKODÁS (DUMPSTER DIVING)

- **Információgyűjtési módszer további social engineering támadáshoz**
- **Fizikai hozzáférés szükséges az épülethez, pl. vendég státusz**
- **Számos információt rejthet egy kuka, pl. telefonszámok, nevek, hosztnevek, akár jelszavak**

### Dumpster diving

This entails combing through someone else's trash to find treasures—or in the tech world, discarded sensitive information that could be used in an illegal manner. Information that should be securely discarded includes, but is not limited to:



# Social Engineering támadás

## FIZIKAI HOZZÁFÉRÉS SZERZÉSE MEGTÉVESZTÉSSEL

- Információgyűjtési módszer további social engineering támadáshoz
- Egy dolgozó képernyőjéről információ lelesése
- Fizikai hozzáférés szükséges az épülethez, pl. vendég státusz
- Bizalmasabb légkör megteremtését feltételezi

Invoice

VISA | MasterCard | JCB | AMERICAN EXPRESS

Card number  
1234 5678 9012 3456

Name on card  
Ex. John Website

Expiry date  
01 / 19

Security code  
\*\*\*

Choose your username  
imoncloud9

Choose a password  
m0nKee11

Show my password

When checkbox is clicked,  
password is unmasked



# Social Engineering támadás

## Esettanulmányok

# KÖSZÖNÖM A FIGYELMET!

## Kérdések?