# Bevezetés a kiberbiztonságba és biztonságtudatosság

## Kiberbiztonsági eszközök

Szarvák Anikó

2023. Tavasz

# Alapfogalmak

Biztonság

- Kockázat, fenyegetés, sérülékenység

Kontrollok:

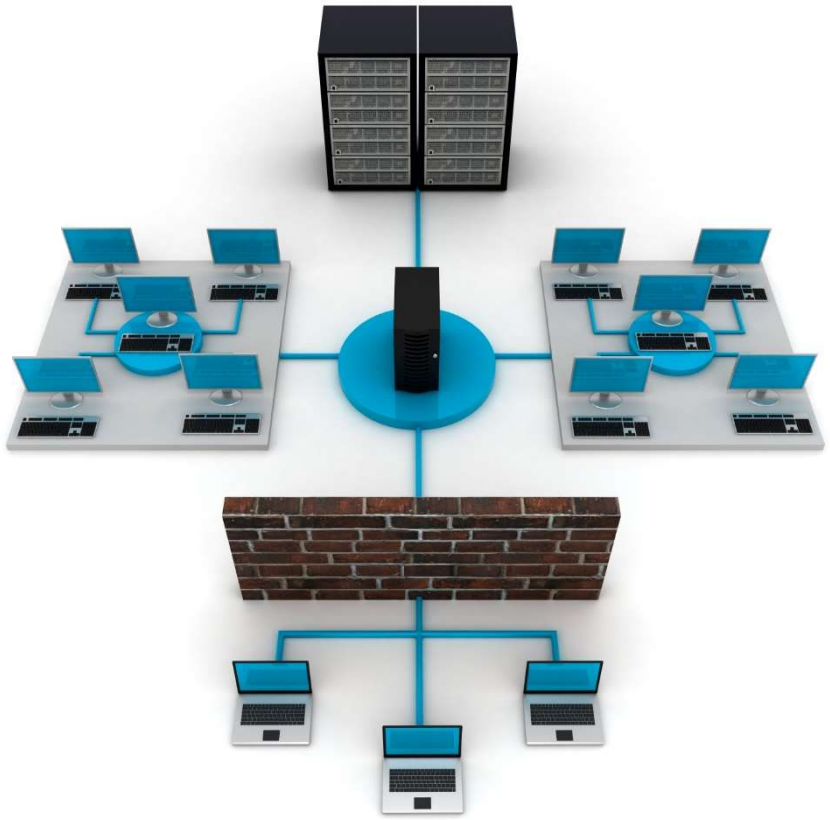
- Adminisztratív vs technikai
- Preventív, detektív, korrektív

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

# 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 Authentiation** |
| 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 Missconfiguration** |
| 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 |

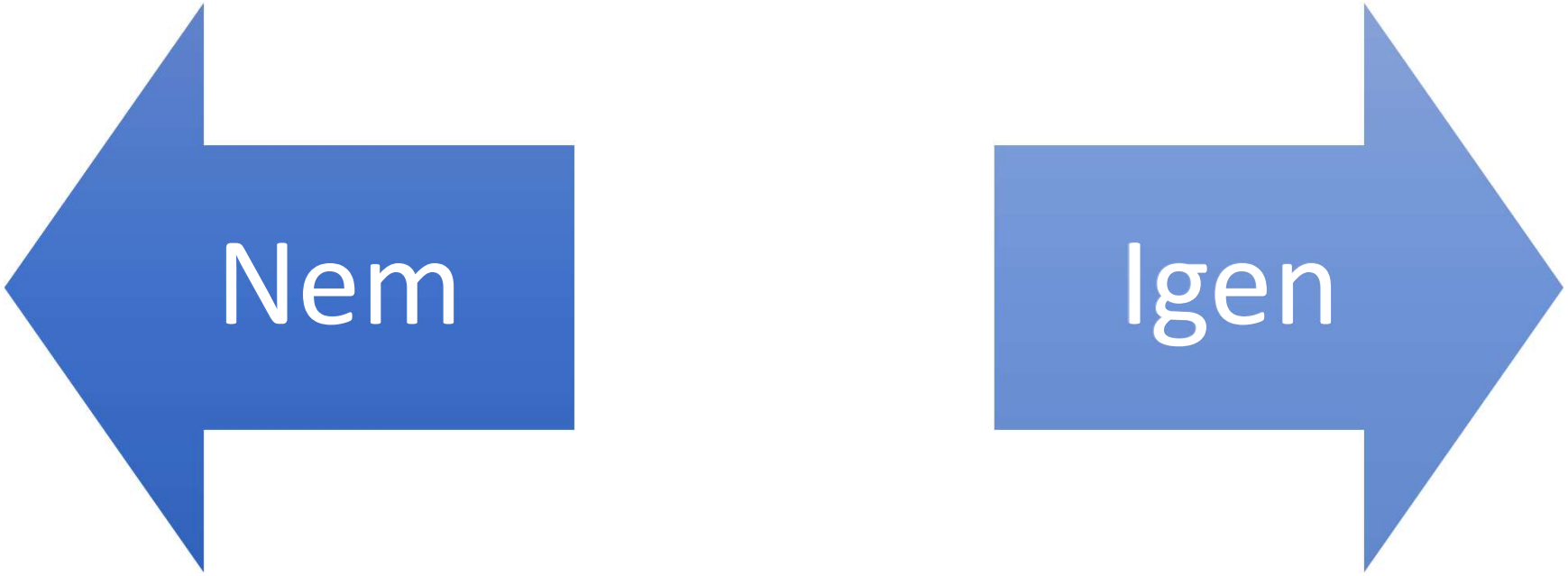
https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

# APT

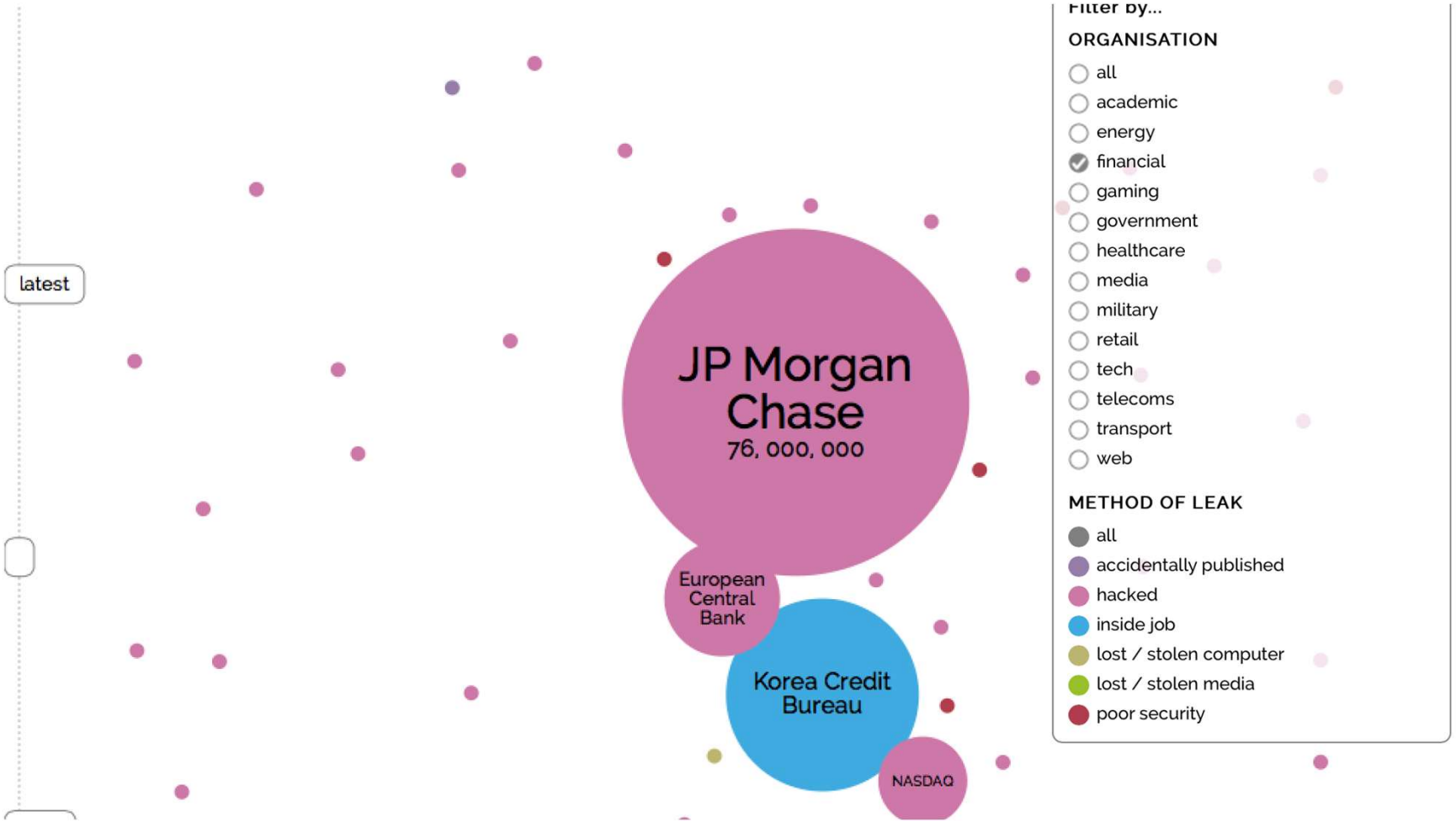
1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command and Control
7. Action

# Betörés

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

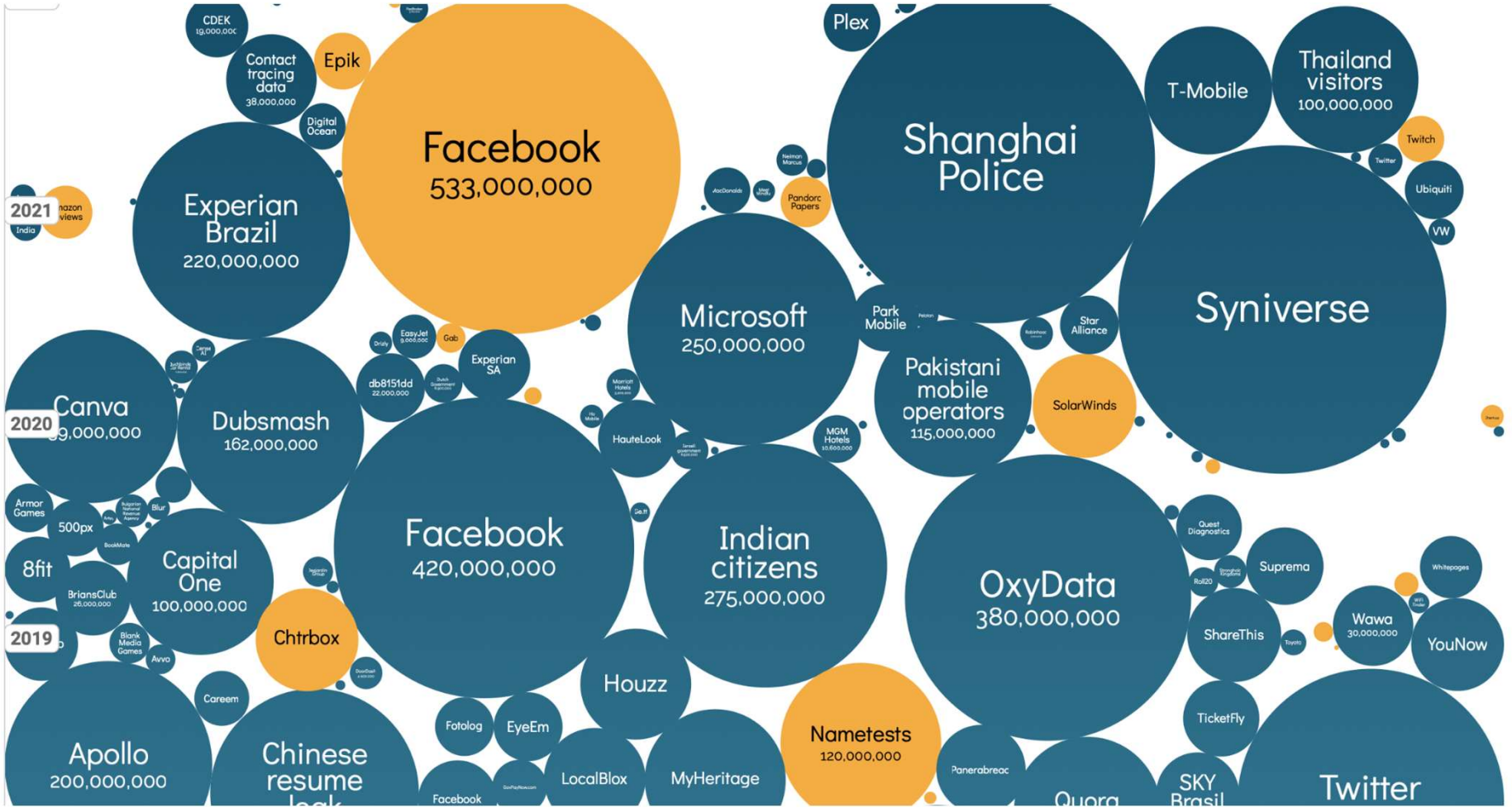


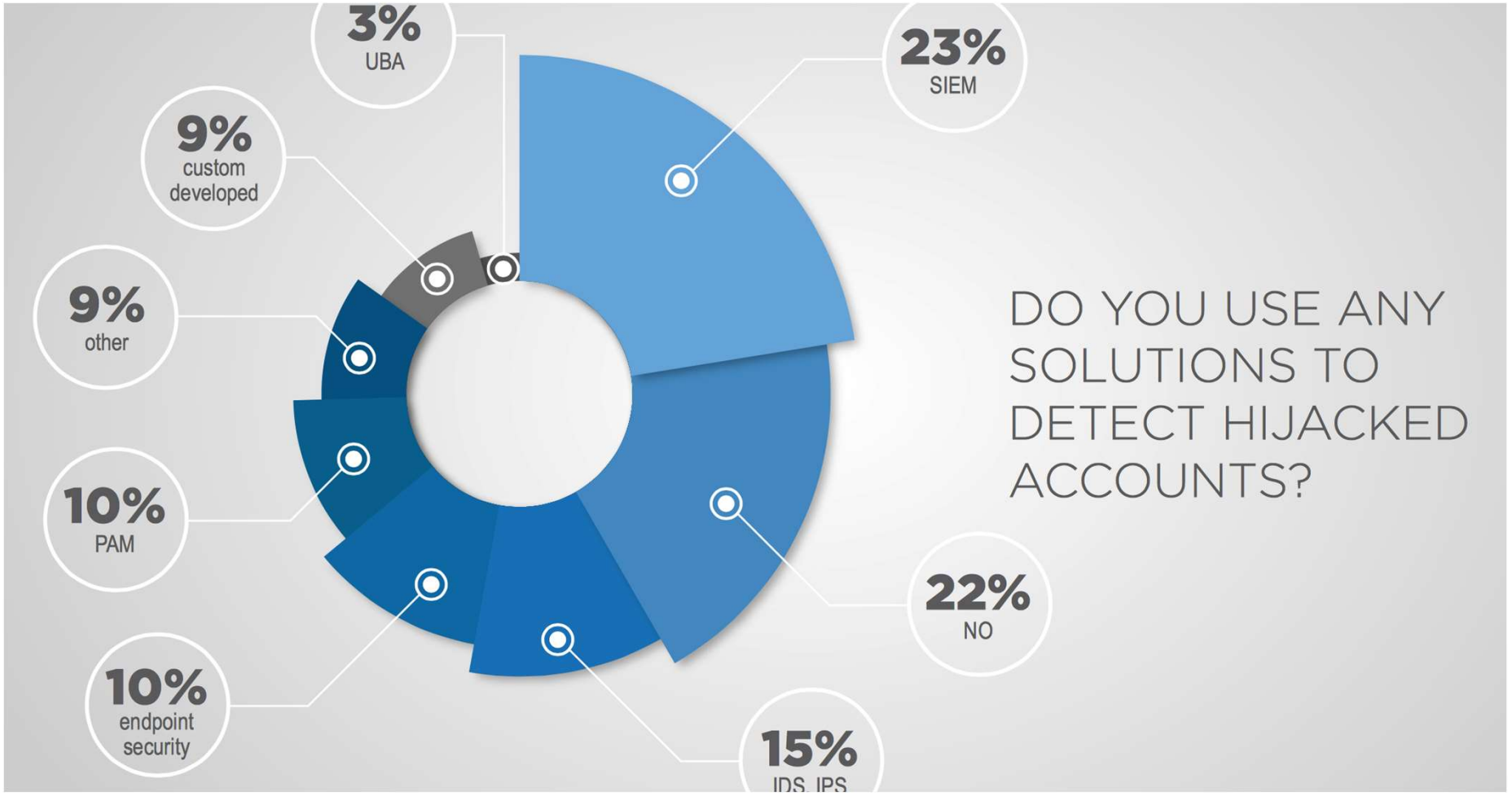
# World biggest databreaches 2015 / finance



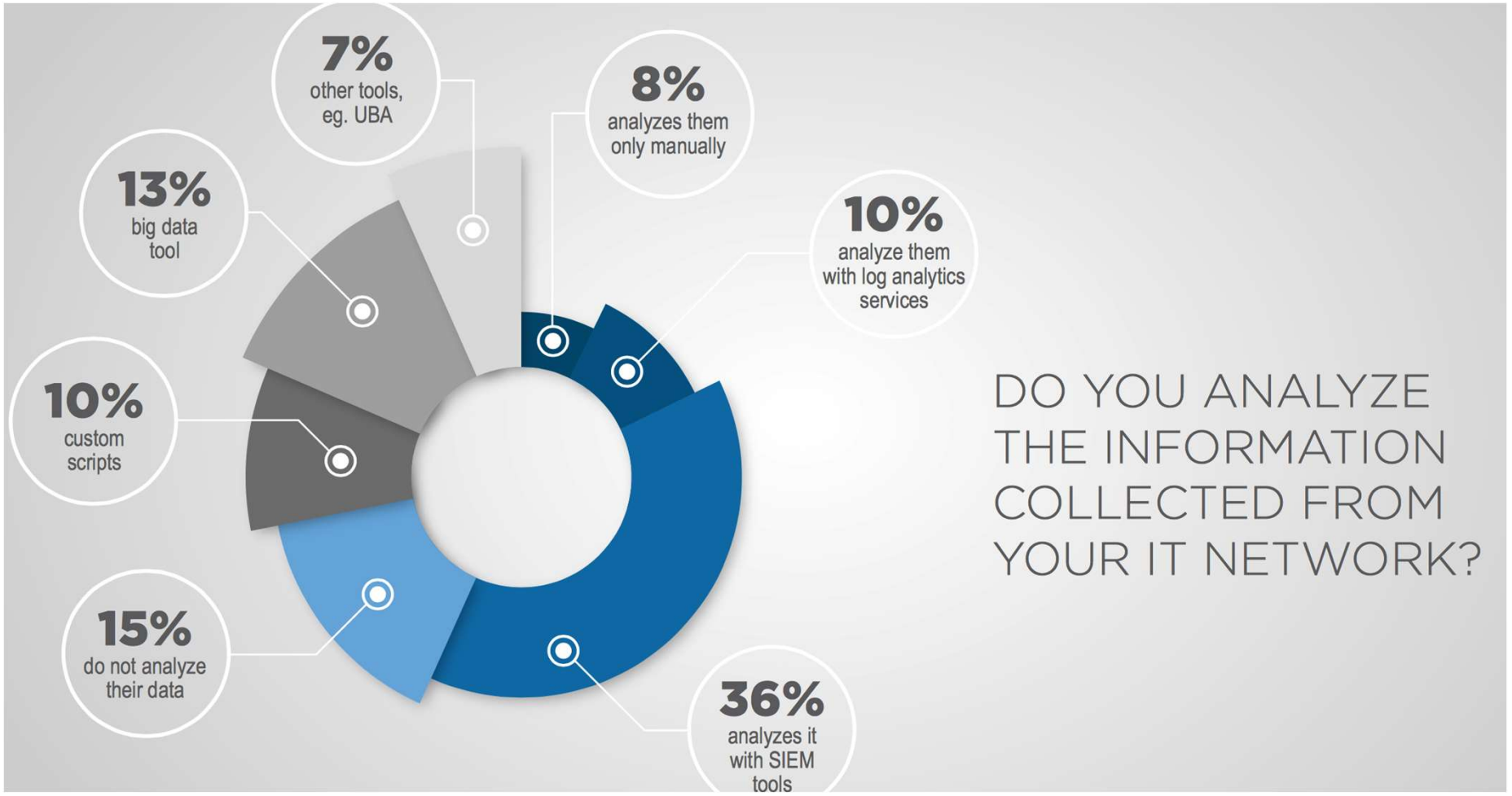
# World biggest databreaches latest / finance

# 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

# 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

Like Tweet +1

**Search**

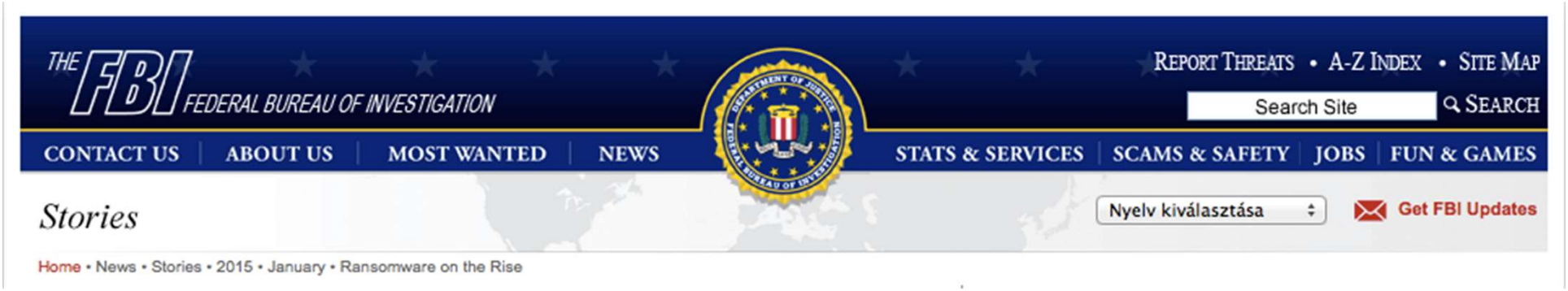
*Powered by DuckDuckGo*

Go

blog essays whole site

**Subscribe**

**About Bruce Schneier**




**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.**

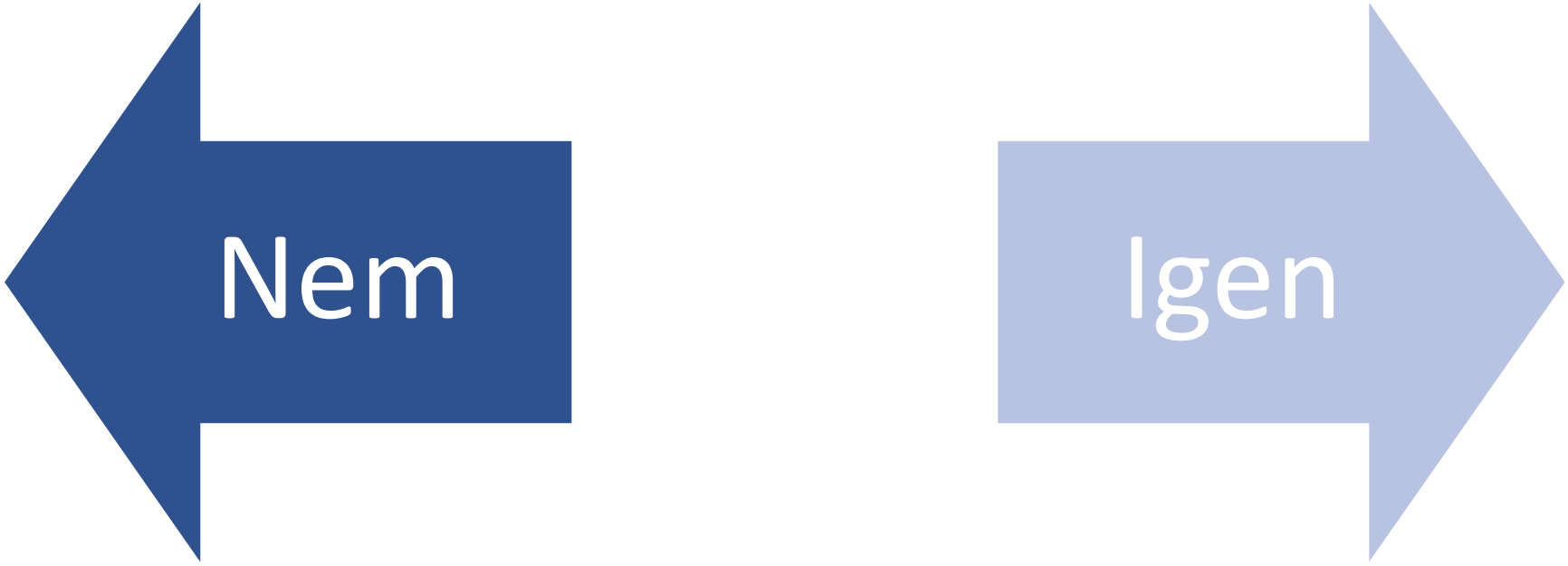
**Protect Your Computer from Ransomware**

- 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?