www.pwc.com

A hatékony incidens kezelés alapjai

Hétpecsét Egyesület

2017. május 17.

pwc

Az előadóról

Szarvák Anikó

- Információbiztonsági szakértő
- CISSP, CHFI, CEH
- A. Menedzser @ PwC
- Társ alapító @ WITSEC
- Elnökségi tag @ ISC2 Hungary
- PhD hallgató @ OE BDI

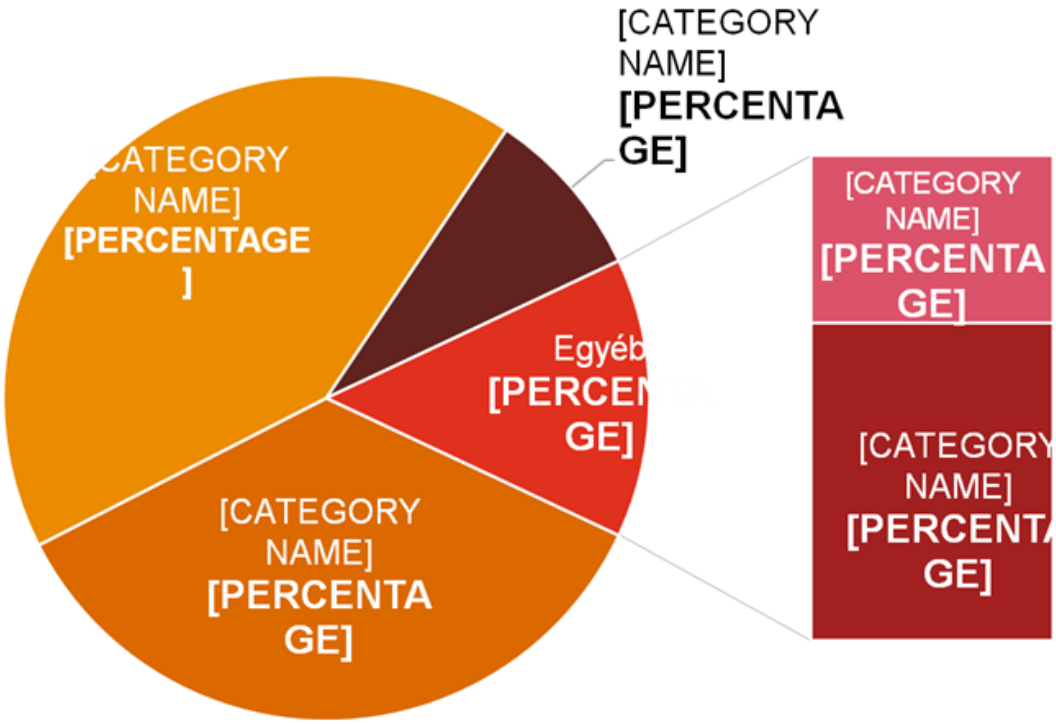
„A vállalati kockázatkezelésnek olyan szilárd kereteket kell biztosítania, amelyeket a védekező taktikák mellett lehetővé teszik a proaktív módon történő értékteremtést is.”

Major Andrea

Vállalati Kockázatkezelés @ PwC:

- Adatvédelemhez kapcsolódó kockázatkezelés (GDPR)
- IT és folyamati megfelelőség
- IT biztonsági szolgáltatások, biztonságtudatosság
- Megfelelőségi vizsgálatok, kockázatelemzés
- Felhő szolgáltatások folyamatai és biztonsága
- ERP rendszerek vizsgálata
- Belső ellenőrzés
- GRC

Vezetői félelem-index (?)



Csökkentik-e a bizalmat az iparágában az üzleti információkat vagy kritikus rendszereket érintő kibertámadások?

Forrás: CEO felmérés, 2017, PwC

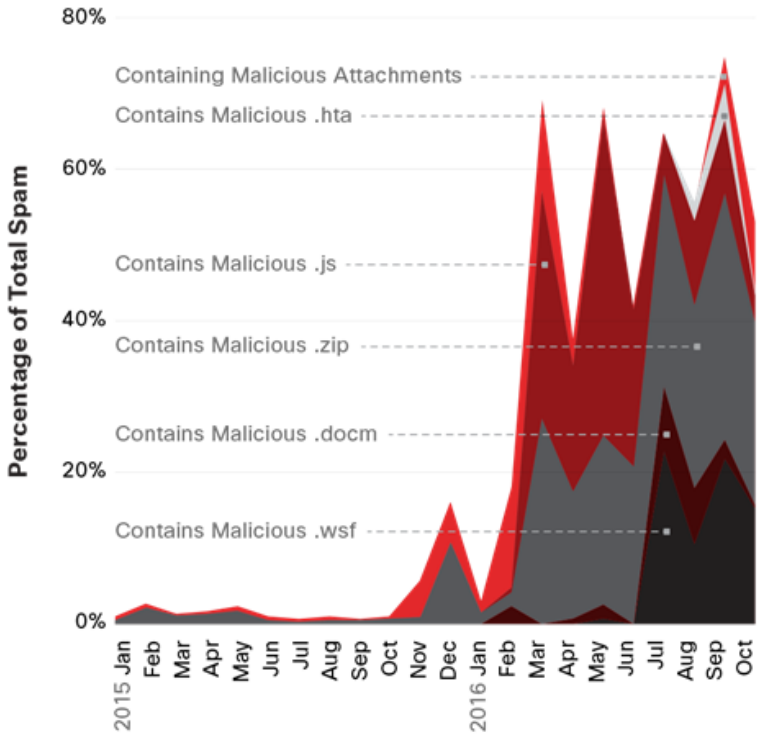
Változó környezet

A spam a fogadók által **nem kért**, elektronikusan, például e-mailen keresztül tömegesen küldött **hirdetés**, felhívás vagy lánclevél.

/https://hu.wikipedia.org/wiki/Spam/

Figure 17 Percentage of Total Spam Containing Malicious Attachments

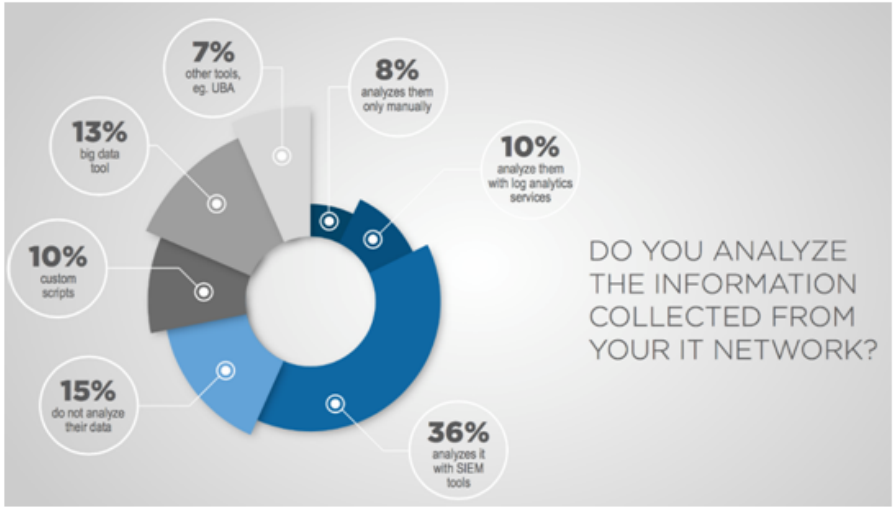
Source: Cisco Security Research



For more info visit: **www.cisco.com/go/acr2017**

cisco

Események figyelése



79%
Valószínűleg nem veszi észre visszaélést felhasználói hozzáféréssel!

15%-a nem vizsgálja a keletkezett eseményeket...

Forrás: https://andrea.blogs.balabit.com/files/2015/11/Balabit_CSI_Survey_Infographic_Final.pdf

Incidens – garantálva

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

Forrás: http://www.owasp.org

Az incidens – a mumus?

Esemény vagy incidens?

Törvényi elvárások – emelkedik a tét

GDPR:

- Kötelezővé teszi a személyes adatok védelmének kidolgozását már a tervezési szakaszban (pl. informatikai fejlesztések)
- Személyes adatokra vonatkozóan hatáselemzést ír elő
- **Bejelentési kötelezettséget vezet be** a személyes adatokkal történő visszaélés esetére

NIS Irányelv:

- Hálózati és határvédelmi biztonsági intézkedések bevezetését írja elő
- **Megköveteli az események észlelését és jelentését**
- Kitér a kritikus infrastruktúra védelmi követelményeire

Az incidensek kommunikációja

GDPR - Áldozatok

GDPR - Hatóság

NIS - Hatóság

Az esemény – **Incidens** – körülményeiről tájékoztatást kell adni:

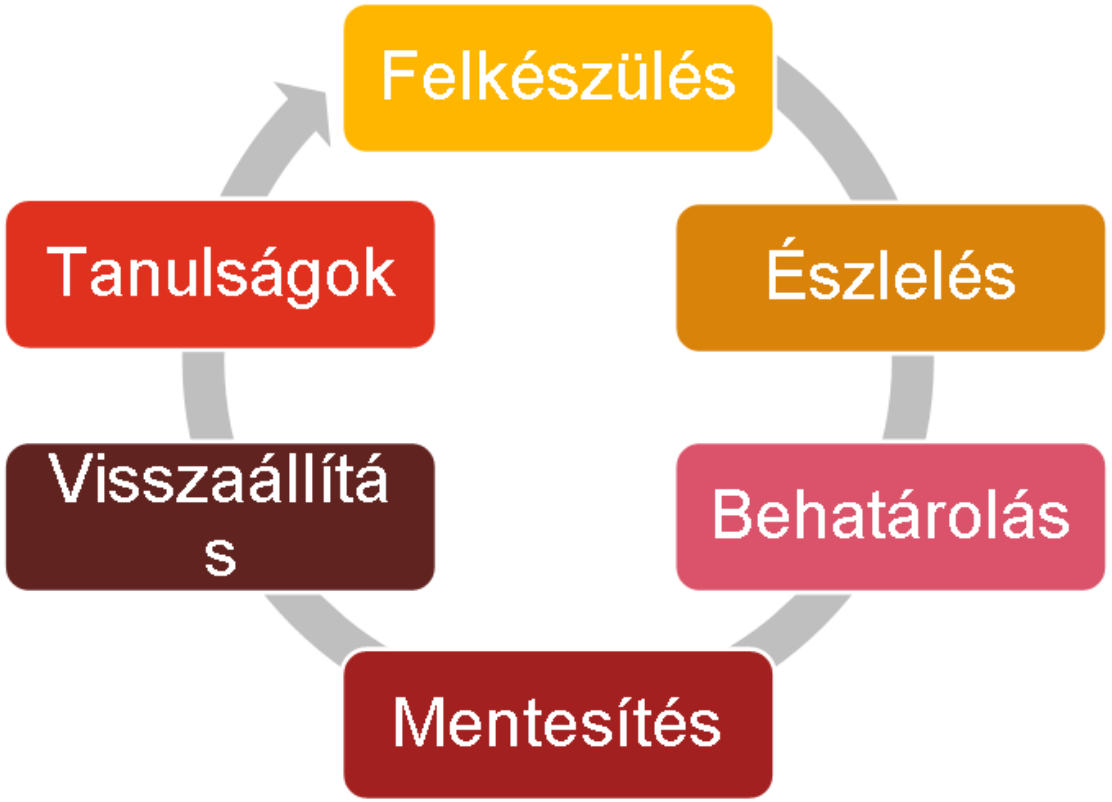
Mi történt?

Mikor történt?

Kik / mi az érintett?

Milyen ellenlépés történt az incidens okozta károk enyhítésére?

Az incidens kezelés folyamata



Eddigi lépések az incidensek kezelésében

Infrastruktúra:

- Vírusvédelem
- Log gyűjtés és elemzés
- Munkamenet monitorozás
- Központi felhasználó- és jelszómenedzsment
- Központi eszköz menedzsment
- …

Hálózat:

- VPN
- Tűzfal / NG / WAF
- IDS / IPS
- Proxy
- …

Kiegészítő technikák:

- Támadási felület minimalizálás
- Bejövő és kimenő adatok ellenőrzése
- Titkosított és azonosított adatkapcsolatok
- Pentest, kód audit
- Hardening
- …

Eddigi lépések az incidensek kezelésében (Folyamatok)

Folyamatok:

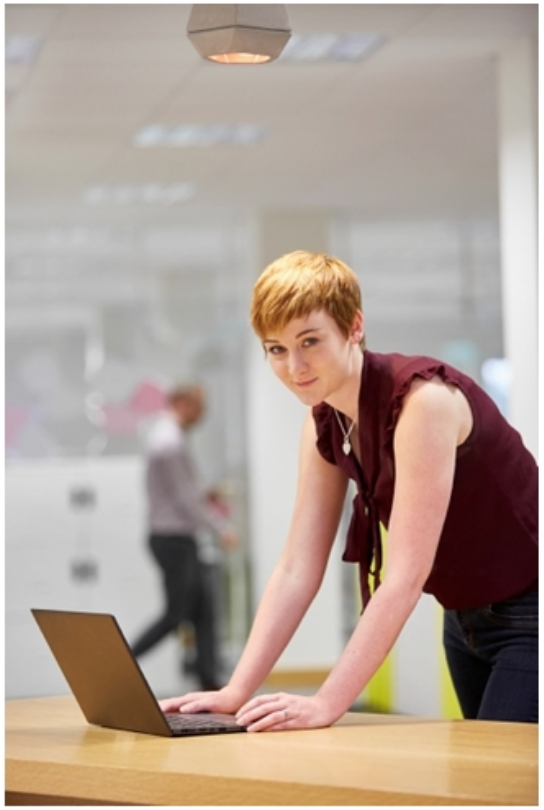
- Adatvagyon leltár, eszköz leltár
- Rendszeres információbiztonsági kockázatelemzés
- Informatikai eszköz életciklus menedzsment
- Jogosultság kezelés
  - Kiemelt jogosultságok kezelése
- Változáskezelési folyamat / Change management
- Sérülékenység-menedzsment
- Incidens menedzsment (!)
- Biztonságtudatossági képzés (!)

SOC

Különböző típusú események egyidejű feldolgozása.

- **Bigdata**
- Threat Intelligence
- Central controll

Biztonságtudatosság



Tudatosság egy képesség, amely közvetlenül tudása és észlelése, érzése és átélése egy eseménynek.

Tágabban értelmezve **állapot** vagy **minőség**, valaminek a **tudatában** lenni.

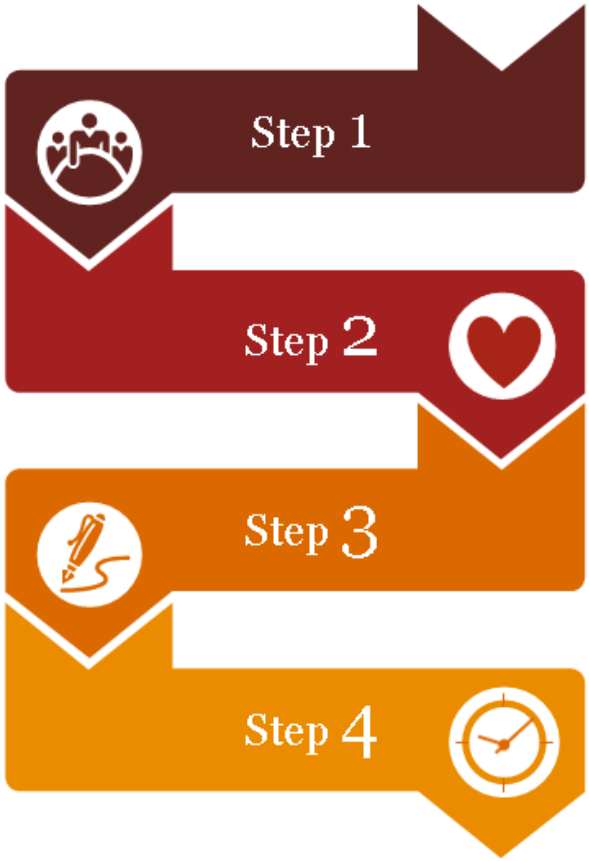
A tudatosság relatív **fogalom**.

„tudni, mi történik”

Biztonságtudatosság != Szabályzatok ismerete

https://en.wikipedia.org/wiki/Awareness

A biztonságtudatosság gyakorlati elemei



Érthetően, „konyhanyelven” kell kommunikálni.

„Érintetté” kell tenni.

Gyakorlati teszteket kell bevetni, az elmélet nem elég.

Legalább fél évente – vagy sűrűbben – ismételni kell.

Köszönöm a figyelmet!

Szarvák Anikó

A. Manager
PwC Magyarország

aniko.szarvak@hu.pwc.com