Kiberbiztonsági trendek és legjellemzőbb támadási formák

EIVOK

EIVOK Konferencia Délután
2019. November 28.

Zala Mihály
Associate Partner | Cybersecurity, Technology Risk and Technology Consulting Leader
Ernst & Young Tanácsadó Kft.

Building a better working world

Trendek az információbiztonság területén

TOP 5 üzleti kockázat

Miért alakulnak ki a biztonsági problémák egy szervezetnél?

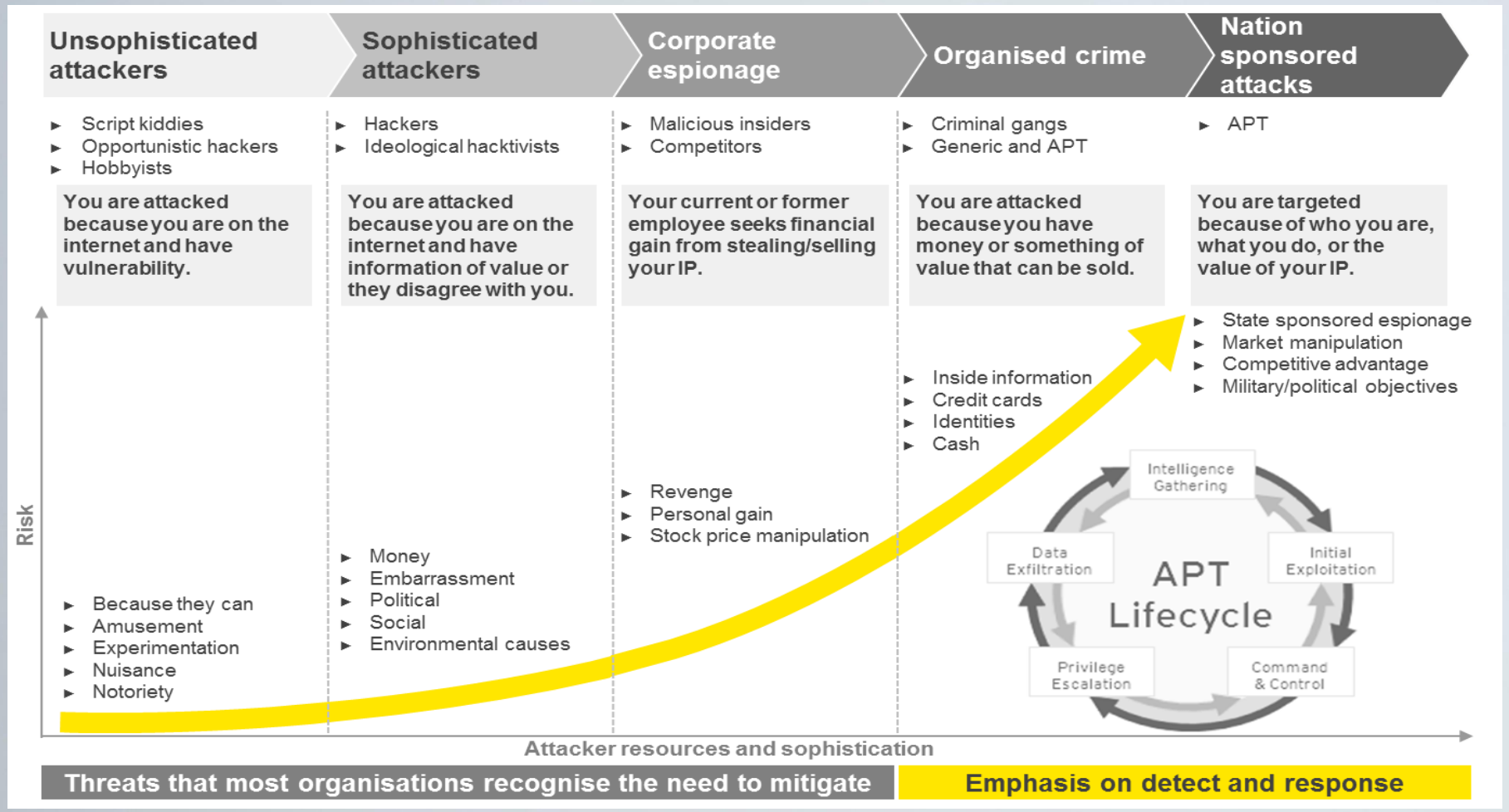
Top 5 risks for small enterprise companies (<€250mn annual revenues)

Rank		Percent	2018 rank	Trend
1	**Cyber incidents (e.g. cyber crime, IT failure/outage, data breaches, fines and penalties)**	**32%**	2 (30%)	▲
2	Changes in legislation and regulation (e.g. trade wars and tariffs, economic sanctions, protectionism, Brexit, Euro-zone disintegration)	**30%**	5 (22%)	▲
3	Natural catastrophes (e.g. storm, flood, earthquake)	**27%**	3 (28%)	=
4	Market developments (e.g. volatility, intensified competition/new entrants, M&A, market stagnation, market fluctuation)	**27%**	4 (27%)	=
5	Business interruption (incl. supply chain disruption)	**26%**	1 (33%)	▼

Source: Allianz Risk Barometer 2019
https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2019.pdf

Trendek az információbiztonság területén

Kibertámadások evolúciója



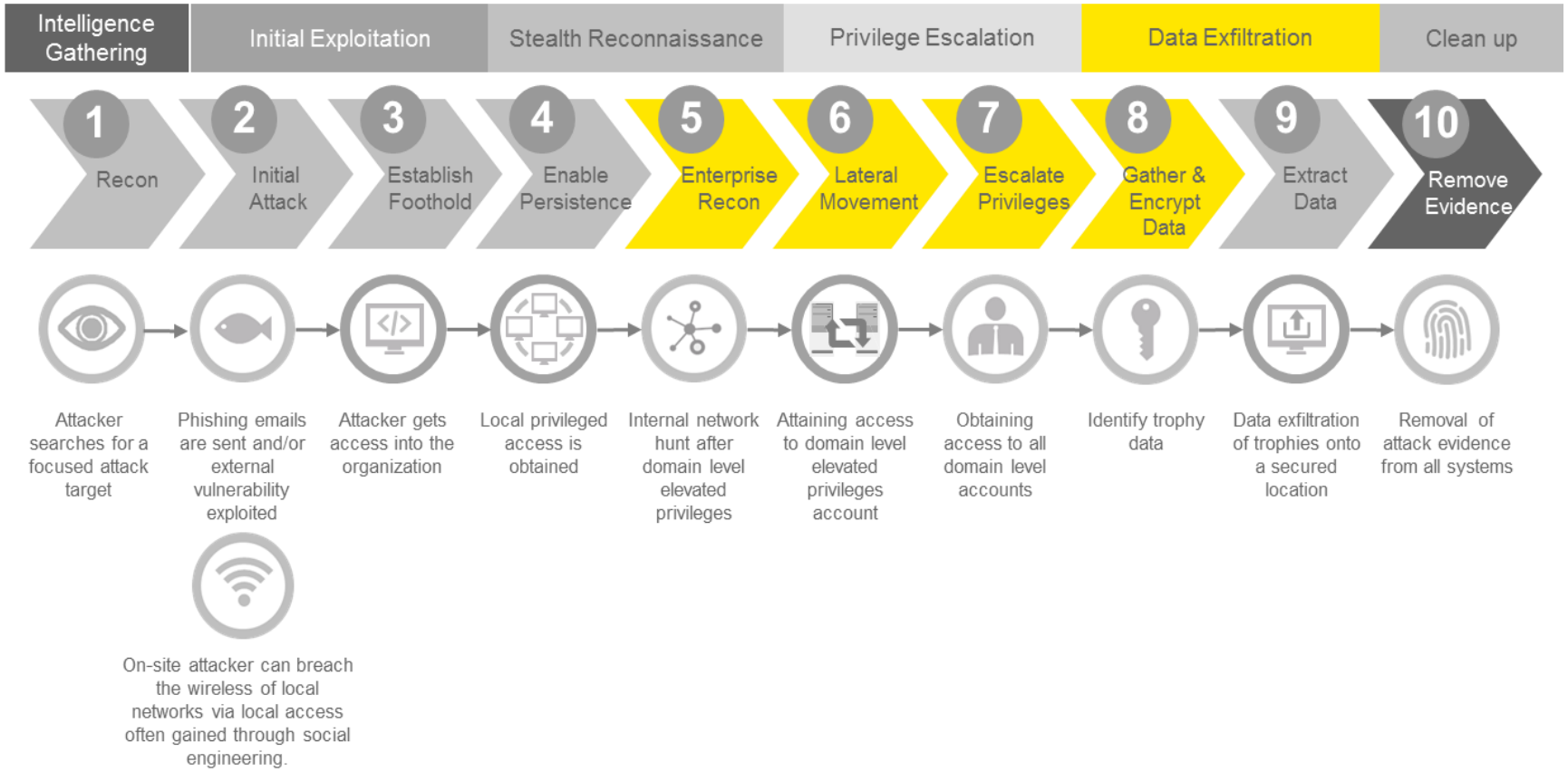
Trendek az információbiztonság területén

Támadók és motivációik

Type of Hacker	Definition	Motivation Includes:
Script Kiddies	A hacker that does not possess technical expertise and relies on pre-developed scripts and programs to perform attacks.	• Thrill of the Challenge • Malicious Intent • Financial Gain
Thrill-Seeker	A hacker that break into systems/network for entertainment value (non-malicious intent)	• Thrill of the Challenge • Admiration of fellow hackers
Insider Hacker	An employee/consultant that performs security exploits within their firm's system/network utilizing organizational knowledge. Typically this type of hacker is a disgruntled/departing employee, contractor or whistleblower.	• Revenge • Exposing firm weaknesses • Deception/fraud
Hacktivists	A socially or politically motivated hacker with the intention of fulfilling a social or political agenda.	• Promotion of political or social beliefs • Website and Social Media Defacement
Cyberterrorists	A hacker with threatening objectives such as harming people or destroying critical systems and/or information.	• Invoke Terror/Fear/Panic • Disruption • Cause chaos
Cyber Warriors/State Sponsored	A hacker that works for a specific governments to serve their military/economic objectives via cyberspace. These hackers have limitless time and funding to target civilians, corporations, and enemies of the state.	• Promote governmental beliefs • Damage economies • Invoke Terror/Fear/Panic • Exert Dominance • Cause chaos

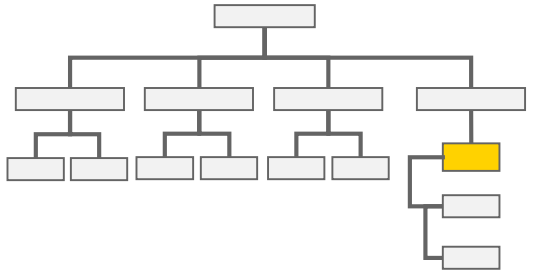
Hogyan visznek véghez a támadók egy kibertámadást?

Támadások lefolytatása



Milyen problémákkal küzd általában az IT biztonsági terület?

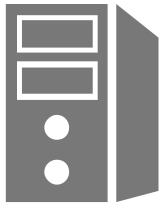
Szervezeti hierarchia



Költségvetés

Szakértői csapat

Korszerű rendszerek



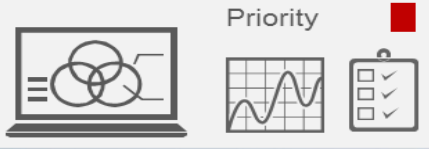
Belső szabályozások

Külső szabályzói megfelelések

Milyen problémákkal küzd az IT biztonsági terület technikai szinten?

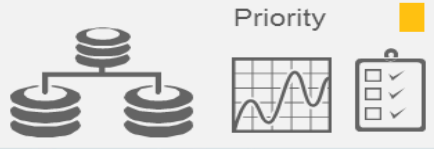
Leggyakoribb hiányosságok

1. Lejárt támogatású OS

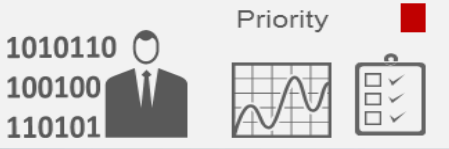


2. Frissítések hiánya

3. Hálózati szeparáció



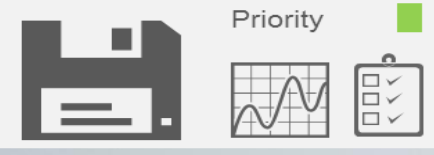
4. IT biztonsági tudatosság



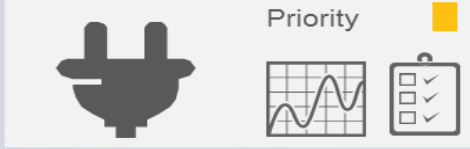
5. Végponti védelem

6. Szabályozási rendszer

7. Mentési rendszerek

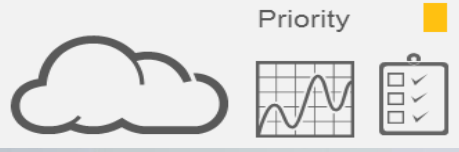


8. BCP/DRP



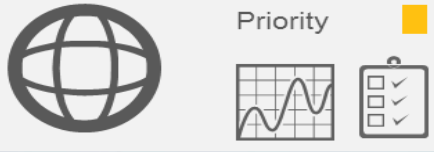
9. Adathordozók védelme

10. Felhő adatbiztonság



11. Titkosítás

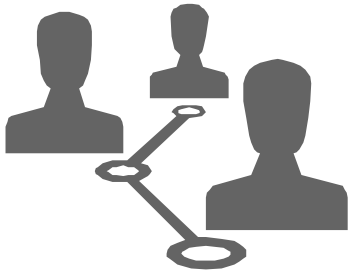
12. Webes alkalmazások



Motivációs tényezők a támadó, védekező és vizsgálati oldalon

A helyi üzemeltetés miért nem tárja fel a problémát?

Fejlesztők, üzemeltetők



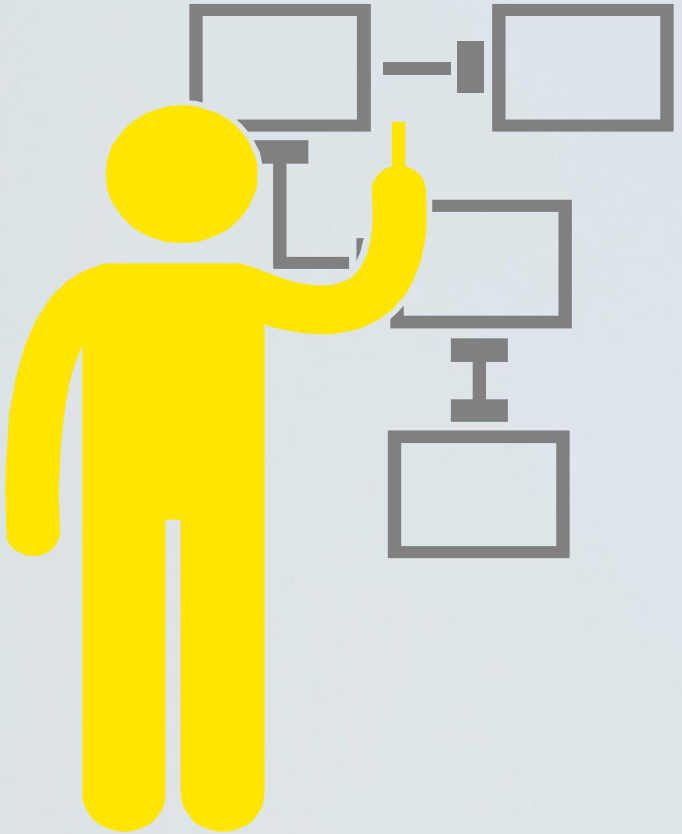
Vizsgálatot végzők

Támadók

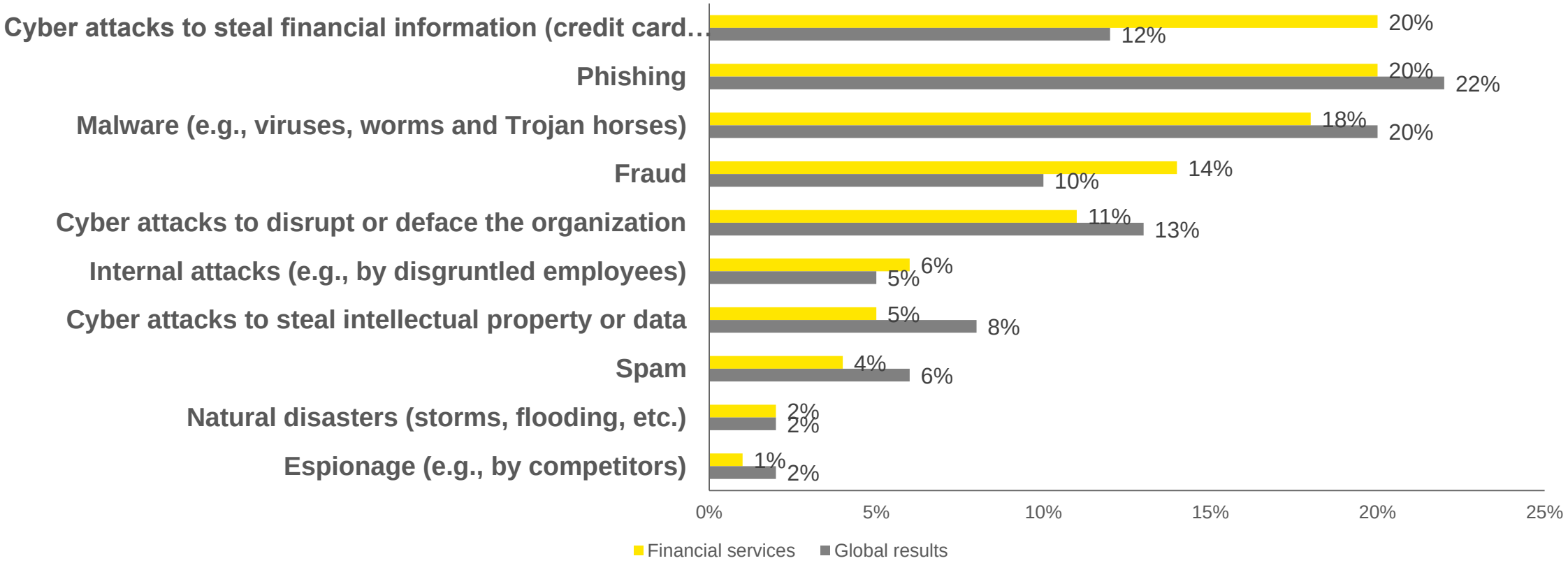
Felkészültség, sikeres támadások (GISS 2018)

A sikeres támadások **99%**-át ismert, ám ki nem javított sebezhetőségek tették lehetővé

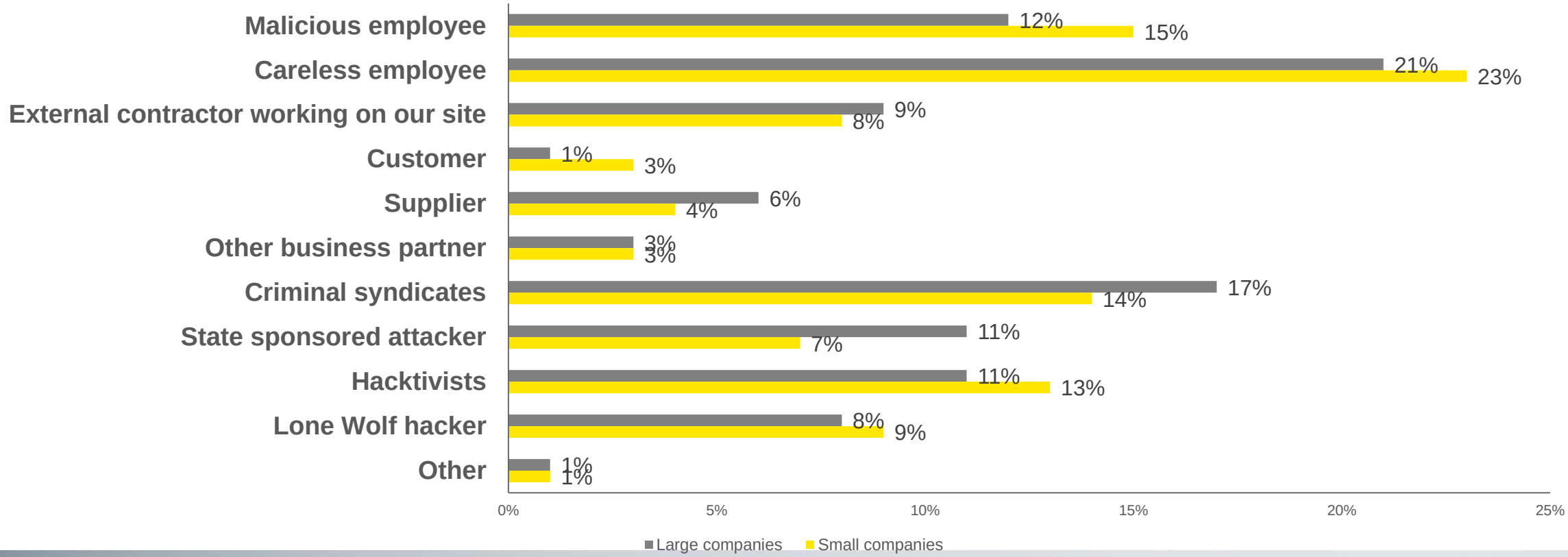
A válaszadók **75%** szerint cégük nem rendelkezik megfelelően fejlett módszerekkel a sérülékenységek azonosításához



Mely fenyegetettségek növelték legjobban szervezete kockázatát az elmúlt 12 hónapban? (GISS 2019)



Kit gondol egy esetleges kibertámadás legvalószínűbb forrásának? (GISS 2019)



Mit kockáztatunk (GISS 2019)

A legnagyobb kiber fenyegetettségek szervezetek számára

1. Phishing (22%)
2. Malware (20%)
3. Kibertámadás (leállás) (13%)
4. Kibertámadás (pénz) (12%)
5. Fraud (10%)
6. Kibertámadás (szellemi tulajdon ellopása) (8%)
7. Spam (6%)
8. Belső támadás(5%)
9. Természeti katasztrófa (2%)
10. Ipari kémkedés (2%)

A megkérdezett szervezetek

17% legjobban az ügyféladatok elvesztésétől fél

22% szerint a legnagyobb fenyegetettség a phising

2% szerint a legnagyobb fenyegetettség az ipari kémkedés

Legértékesebb információk kiberbűnözők számára

1. Ügyfél információ (17%)
2. Pénzügyi információ (12%)
3. Stratégiai tervek (12%)
4. Döntéshozói információ (11%)
5. Ügyfél jelszavak (11%)
6. R&D információ (9%)
7. M&A információ (8%)
8. Szellemi tulajdon(6%)
9. Be nem jegyzett szellemi tulajdon (5%)
10 Beszállítói információ (5%)

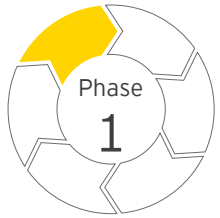
Védekezési lehetőségek

Plan and prepare

Identify particularly likely or especially damaging scenarios in order to focus initial effort on higher risk areas

IR should include plans for development, team creation and training, and establish supporting technologies

Regularly test plan/team (cyber incident simulation)



Identification

Detect and identify an incident Triage, categorize and classify an incident, and decide on immediate containment measures

Establish war room, assemble IR team, perform a detailed assessment and formulate specific plan of action

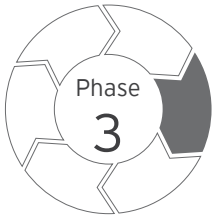
Confirm roles and responsibilities and establish reporting lines and frequency

Containment

Determine the steps to be taken in order to contain the damage or risk posed by the incident

Document the containment plan and, if possible, test technical containment controls

Deploy the containment controls and monitor for effectiveness or adverse impacts



Investigation

Identify sources of potential evidence and preserve or collect them, as required

Process and analyze evidence relevant to the incident, and determine the root cause of the incident

Report and undertake follow-on activities to support litigation, insurance and regulatory responses

Remediation

Develop and implement a plan to remediate the cause of the incident and return the organization to a stable state

Document the plans and controls and, if possible, test technical remediation methods

Deploy remediation controls and rebuild systems

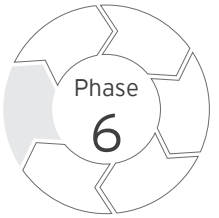
Monitor for re-occurrence and adverse impacts

Lessons learned

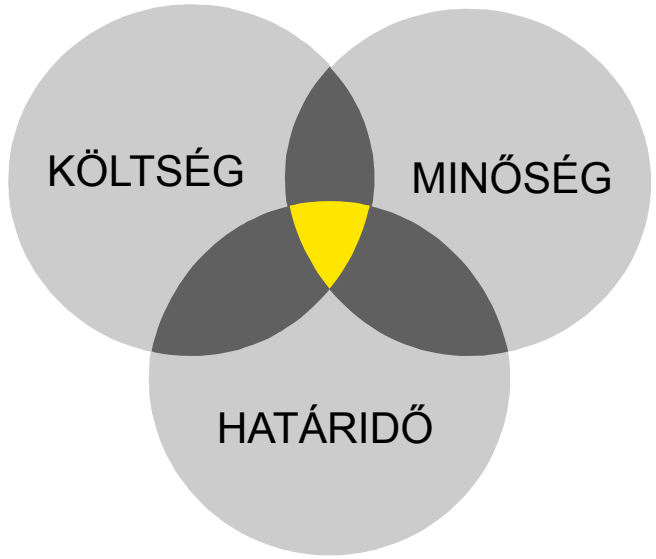
Finalize IR documentation and hold closeout lessons learned meeting

Provide feedback to team members and update IR plan with improvements

Make long-term security improvements to help reduce the impact of similar incidents in future



A fejlesztési problémák az informatikai projektekben jelen vannak



- a fejlesztés a tervezettnél drágábban készül el
- a fejlesztés a tervezettnél hosszabb idő alatt készül el
- a fejlesztés nem az igényeknek megfelelően készül el
- a fejlesztés eredményterméke rossz minőségű, nehezen karbantartható lesz
- a fejlesztés eredménytermékének használata anyagi kárhoz vezet
- a fejlesztés eredményterméke átadásra sem kerül

Mire érdemes figyelni az IT biztonság mellett?

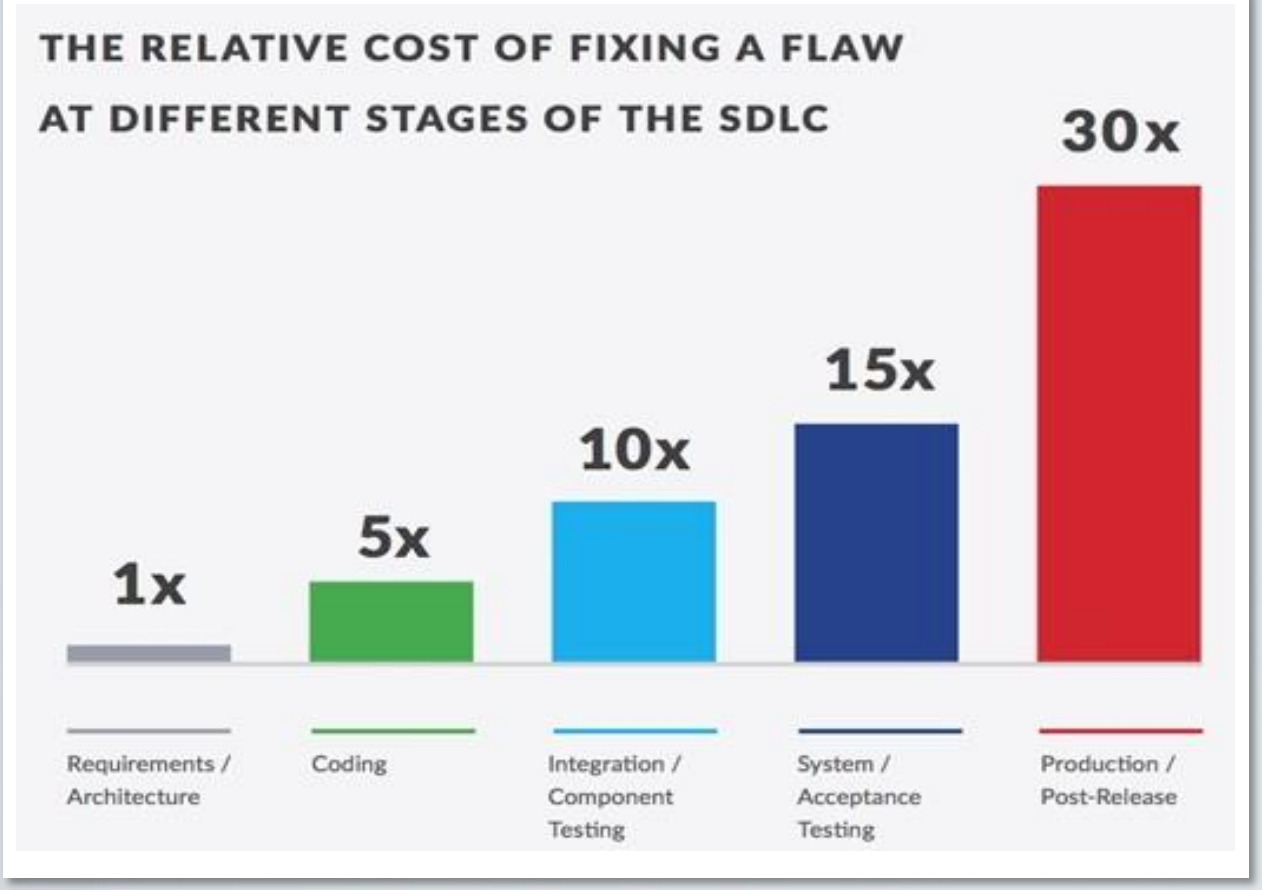
Minőségbiztosítás

Külső/Belső szabályzók

Tesztelések

Iparági sztenderdek

Hibajavítás költsége



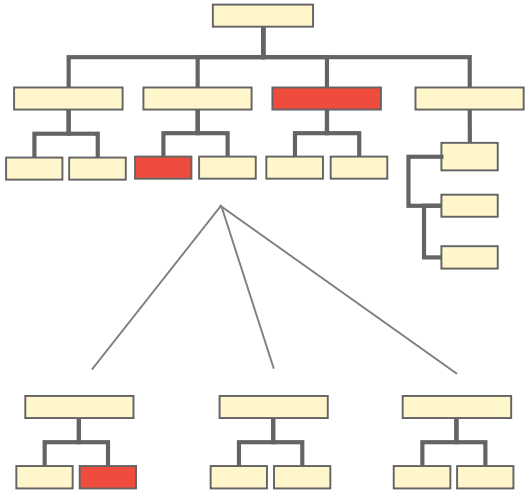
Integrált kiberbiztonsági kockázatkezelés - Fókuszterületek

- Kiber fókuszú vállalati ökoszisztéma
- Stratégia és innováció
- Kockázat fókuszú megközelítés
- Agilis, tudás alapú megközelítés
- Azonnali reagáló képesség és méretezhetőség

Integrált kiberbiztonsági kockázatkezelés

1. Kiber fókuszú vállalati ökoszisztéma

Nincs kivétel



Dedikált döntéshozó

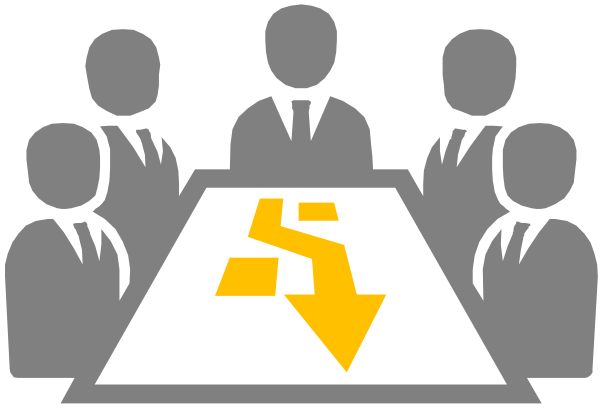
Beszerzések

Integrált kiberbiztonsági kockázatkezelés

2. Stratégia és innováció

Kiberbiztonság üzleti tervezés szerves része

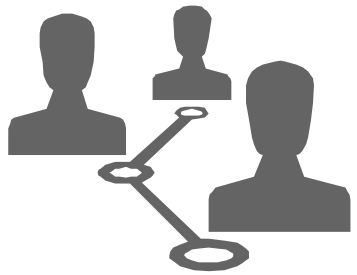
Kiberbiztonság
fókuszú stratégia



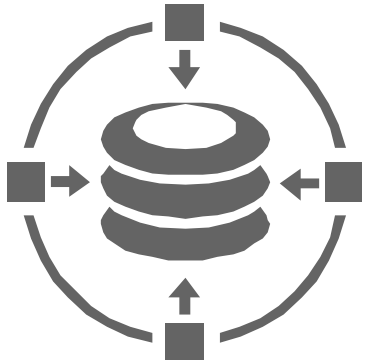
Integrált kiberbiztonsági kockázatkezelés

3. Kockázat fókuszú megközelítés

Biztonsági trendek követése

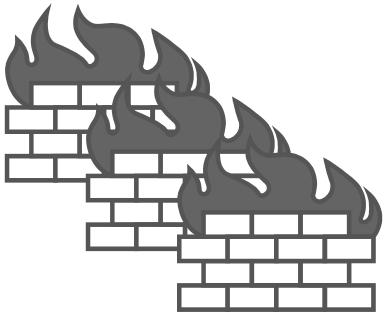


Valós kockázatok azonosítása



Szabályzók, ajánlások ismerete

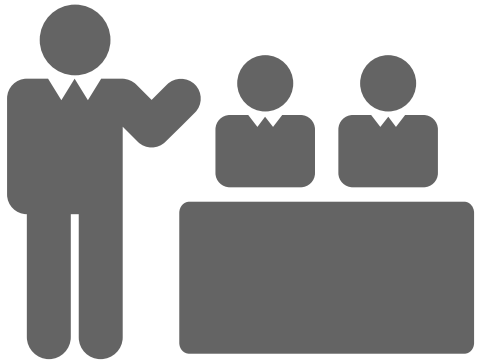
Több rétegű védelmi vonal



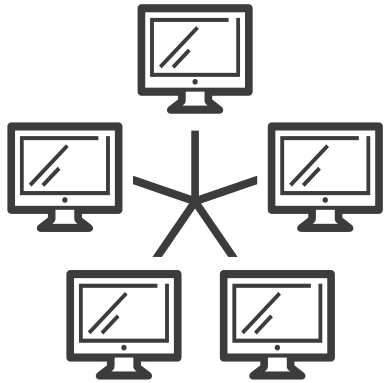
Integrált kiberbiztonsági kockázatkezelés

4. Agilis, tudás alapú megközelítés

Belső tudásképesség folyamatos fejlesztése



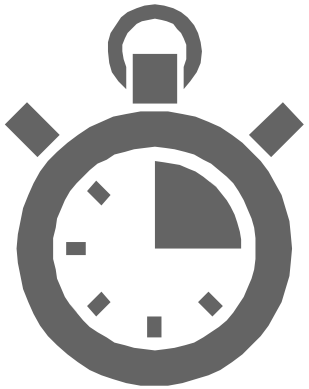
Fókusz a kritikus eszközök védelmére



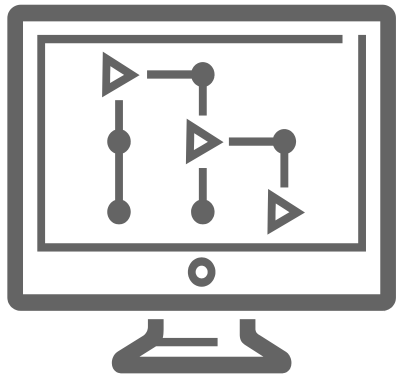
Integrált kiberbiztonsági kockázatkezelés

5. Azonnali reagáló képesség és méretezhetőség

Azonnali reagáló képesség



Skálázható rendszerkialakítás



Az EY globális információbiztonsági felmérése szerint (GISS) a válaszadók **kevesebb, mint 14% -a gondolja**, hogy információbiztonsági funkciójuk teljes mértékben **megfelel szervezeti igényeiknek.**

Mihály Zala

Mobile: +36 20 925 3020

Email: Mihály.Zala@hu.ey.com

Associate Partner | Cybersecurity, Technology Risk and Technology Consulting

Ernst & Young Tanácsadó Kft.

Köszönöm a figyelmet!

Building a better working world