Felkészülés a NIS2-re azoknak, akik nem szeretnek veszélyesen élni

Mihály Zala
Partner
Head of Technology Risk and Cybersecurity
Ernst & Young Consulting Ltd.

The better the question. The better the answer.
The better the world works.

Building a better working world

Támadók motivációi

Mi a támadók motivációja?

Adatgyűjtés

A támadó elsődleges motivációja az adatgyűjtés

Technikai adatok

- elérhető eszközök
- elérhető szolgáltatások
- ismert sérülékenységek
- felhasznált technológiák

Személyes adatok

- felhasználónevek
- jelszavak
- e-mail címek
- közösségi profilok

Technológiai fókuszú támadás

Social Engineering fókuszú támadás

Testre szabott támadások

- ipari kémkedés
- versenytárs lejáratása
- személyes bosszú
- szellemi tulajdon megszerzése

Kitekintés: Európai információbiztonsági rendeletek fejlődése

2016	2018	2024*	2025*
NIS Hálózat- és információbiztonsági irányelv	**GDPR** Az európai adatvédelmi rendelet	**NIS2** Hálózat- és információbiztonsági irányelv II.	**DORA** Digital Operational Resilience Act
Az EU kritikus infrastruktúrájának védelme a kiberfenyegetések ellen	Az egyének személyes adatainak védelme	Az eredeti NIS irányelv továbbfejlesztése és kibővítése	Az európai pénzügyi szektor digitális működőképességének biztosítása
Az információs rendszerek és hálózatok biztonságának javítása	Az adatok gyűjtése, feldolgozása és tárolása szabályozása	Nagyobb figyelem az Ipar 4.0 és a kritikus infrastruktúra digitális biztonságára	IT rendszerek és digitális szolgáltatások megbízhatóságának javítása
Kötelező jelentéstétel és együttműködési követelmények	Szigorú adatvédelmi követelmények és büntetések	Kiberbiztonsági követelmények és együttműködés megerősítése	Az operatív ellenállóképesség és az incidenskezelésre való felkészülés

* Tervezett tagországi bevezetés dátuma

NIS2: Érintett szektorok

Kiemelten kritikus ágazatok

alapvető szervezetek

- energetika
- közlekedés
- egészségügy
- ivóvíz, szennyvíz
- hírközlési szolgáltatás
- digitális infrastruktúra
- kihelyezett ICT szolgáltatások
- űrkutatás

Egyéb kiemelt ágazatok

fontos szervezetek

- postai és futárszolgálatok
- élelmiszer előállítása, feldolgozása és forgalmazása
- hulladékgazdálkodás
- vegyszerek előállítása és forgalmazása
- gyártás
- digitális szolgáltatók
- kutatás

NIS2: teljesítendő főbb követelmények

Információbiztonsági Irányítási Rendszer

- Teljeskörű IT biztonsági irányítási rendszer adminisztratív, logikai és fizikai védelmi intézkedésekkel.
- A biztonsági vezető és a felhasználók felelősségének egyértelmű meghatározása.

Üzletmenet folytonosság

- BCP/DRP tervek szabályozása
- gyakorlatok szervezése

Beszállítók ellenőrzése

- beszállítók kockázatelemzése
- beszállítói auditok

Biztonságtudatosság növelése

- képzések
- szimulációs gyakorlatok

IT biztonság kockázatmenedzsment

- feltárás (rendszeres vizsgálatok)
- kezelés (rendszerenként)

Incidens menedzsment

- megelőzés/detektálás/kezelés
- bejelentési kötelezettség

IT rendszerek menedzsmentje

- beszerzés/selejtezés
- fejlesztés/üzemeltetés

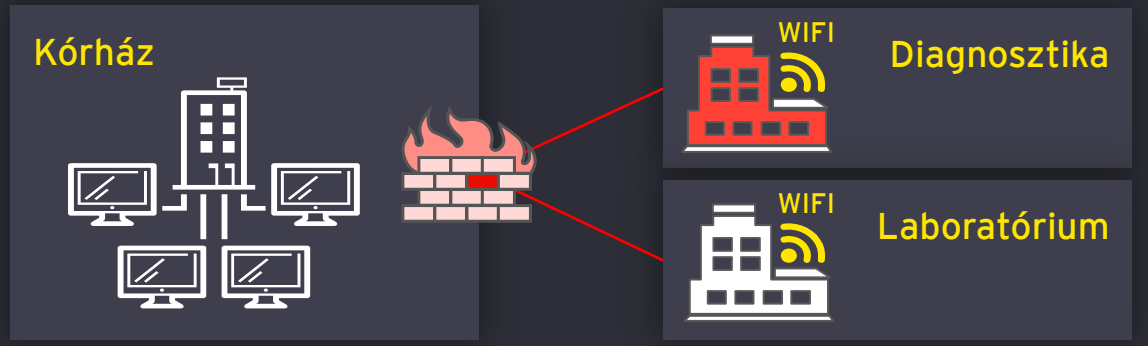
Esettanulmány egészségügyben zsaroló vírus támadásról

Megyei kórház

- *Teljes megye ellátása (1,5m fő)*
- *800 aktív ágy*
- *6 dolgozó az IT osztályon*

Kiváltó ok: kórházi beszállítók egy routeren keresztül össze voltak kötve a kórház IT rendszerével,

beszállító titkársági gépén zsarolóvírus fertőzés



Mi segíthetett volna a megelőzésben?

Megfelelően kidolgozott és működtetett **IT biztonság irányítási rendszer**:

a) Részletes szabályzók (adminisztratív, fizikai, logikai) rendszeres auditokkal támogatva

b) Kockázatmenedzsment

c) Beszállítói auditok

d) Biztonságtudatossági képzések, adathalász szimulációk

e) Sérülékenységek feltárása

f) BCP/DRP gyakorlatok

Általános tanulságok*

- a **kiberbiztonság** a kórházi működés és a betegbiztonság szempontjából kritikus tényező
- az információbiztonsági **képzettségét, biztonságtudatosságát** naprakészen kell tartani
- Az IT szinten kapcsolódó **beszállítók** illetve az **ellátási lánc** jelentős biztonsági kockázatot hordozhatnak
- A biztonság növelése érdekében szükség esetén külső cégeket, tanácsadókat is szükséges alkalmazni
- Mentések, naplózás, végpontvédelem, kártékony kódok elleni védelem, tűzfalak, gyakorlatban tesztelt BCP/DRP tervek, biztonságtudatossági képzések!

* Forrás: http://real.mtak.hu/132133/1/fa3312dbda1220b77b7dbe62700a997f.pdf

NIS2 felkészülési lehetőségek

Információbiztonsági Irányítási Rendszer

- Teljeskörű IT biztonsági irányítási rendszer adminisztratív, logikai és fizikai védelmi intézkedések
- A biztonsági vezető és a felhasználók felelősségének egyértelmű meghatározása.

GAP analízis

Irányítási rendszer kialakítása

Üzletmenet folytonosság

- BCP/DRP tervek szabályozása
- gyakorlatok szervezése

Beszállítók ellenőrzése

- beszállítók kockázate
- beszállítói auditok

Beszállítói auditok

Biztonságtudatosság növelése

- képzések
- szimulációs gyakorla

Adathalász szimulációs keretrendszer

IT biztonság kockázatmenedzsment

- feltárás (rendszeres vizsgálatok)
- kezelés (rendszerenként)

Kibertámadás szimuláció

Incidens menedzsment

- megelőzés/detektálás/kezelés
- bejelentési kötelezettség

IT rendszerek menedzsmentje

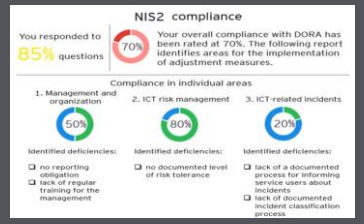
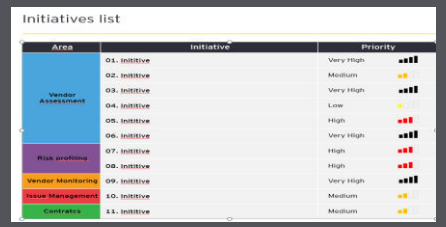
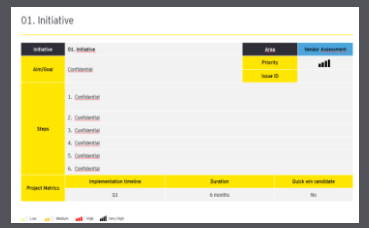
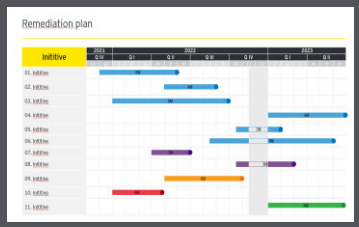
- beszerzés/selejtezés
- fejlesztés/üzemeltetés

NIS2 felkészülési lehetőségek: GAP analízis

A NIS2 hiányosságok felmérését támogató digitális audit (DRC) eszköz, amely hatékony adatgyűjtést, gyors értékelést és egyértelmű akció tervet biztosít a szervezetek számára.

	1. Gap analízis	2. Riporting	3. Akció terv
CLIENT	**1. SELF-ASSESSMENT WITH DRC TOOL** ▸ Self-assessment powered by DRC tool ▸ Providing justification for compliance areas ▸ Automized reporting		

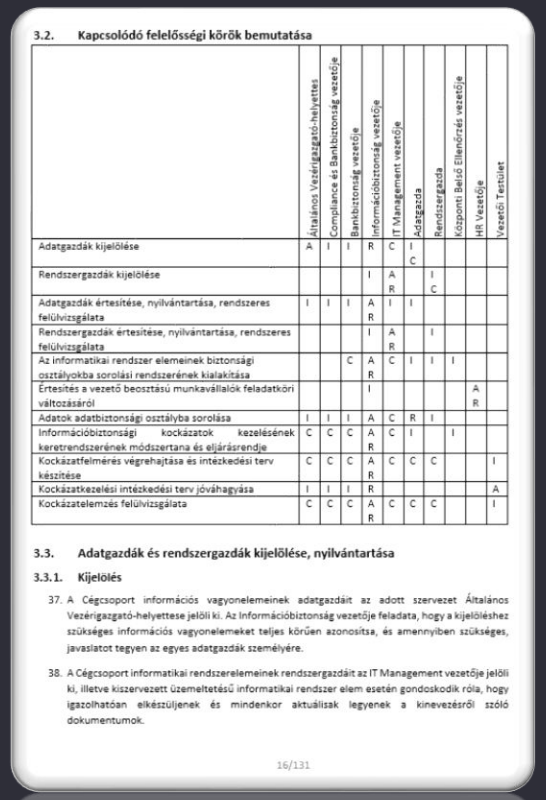
EY	**2. WORKSHOPS: VALIDATE & RECOMMEND**
	COMPLIANCE — Validation of compl. by review of evidences and test of one
	NON-COMPL — Workshops to develop recommendations on closing gaps
		Reporting on NIS2 compliance across in-scope entities:
		▸ Detailed report per entity containing:
		  ▸ Description compliance areas as well as gaps
		  ▸ Recommendations for closing the gaps
		  ▸ Maturity level
		▸ Consolidated compliance report
			Preparing road map of initiatives aiming on rising operational resilience and closing gaps:
			▸ A list of initiatives / projects with an action plan
			▸ Implementation schedule for the initiatives
			▸ An estimate of the time and resource required for each initiative

WORK PRODUCTS	 	 	 

NIS2 felkészülési lehetőségek: Információbiztonsági irányítási rendszer

Javasolt megközelítés

- NIST 800-53 nemzetközi szabvány alkalmazása (IBTV, 41/2015 BM rendelet)
- Szabványok, jogszabályok mapp-elése (ISO27001, BM VHR, MNB utasítások, stb.)
- RACI mátrix a felelősségek egyértelmű azonosításához



3.2. Kapcsolódó felelősségi körök bemutatása

	Általános Vezérigazgató-helyettes	Compliance és Bankbiztonság vezetője	Bankbiztonság vezetője	Információbiztonság vezetője	IT Management vezetője	Adatgazda	Rendszergazda	Központi Belső Ellenőrzés vezetője	HR Vezetője	Vezetői Testület
Adatgazdák kijelölése	A	I	I	R	C	I C				
Rendszergazdák kijelölése				I	A R		I C			
Adatgazdák értesítése, nyilvántartása, rendszeres felülvizsgálata	I	I	I	A R	I	I				
Rendszergazdák értesítése, nyilvántartása, rendszeres felülvizsgálata				I	A R		I			
Az informatikai rendszer elemeinek biztonsági osztályokba sorolási rendszerének kialakítása			C	A R	C	I	I	I		
Értesítés a vezető beosztású munkavállalók feladatkörí változásáról				I					A R	
Adatok adatbiztonsági osztályba sorolása	I	I	I	A	C	R	I			
Információbiztonsági kockázatok kezelésének keretrendszerének módszertana és eljárásrendje	C	C	C	A R	C	I		I		
Kockázatfelmérés végrehajtása és intézkedési terv készítése	C	C	C	A R	C	C	C			I
Kockázatkezelési intézkedési terv jóváhagyása	I	I	I	R						A
Kockázatelemzés felülvizsgálata	C	C	C	A R	C	C	C			I

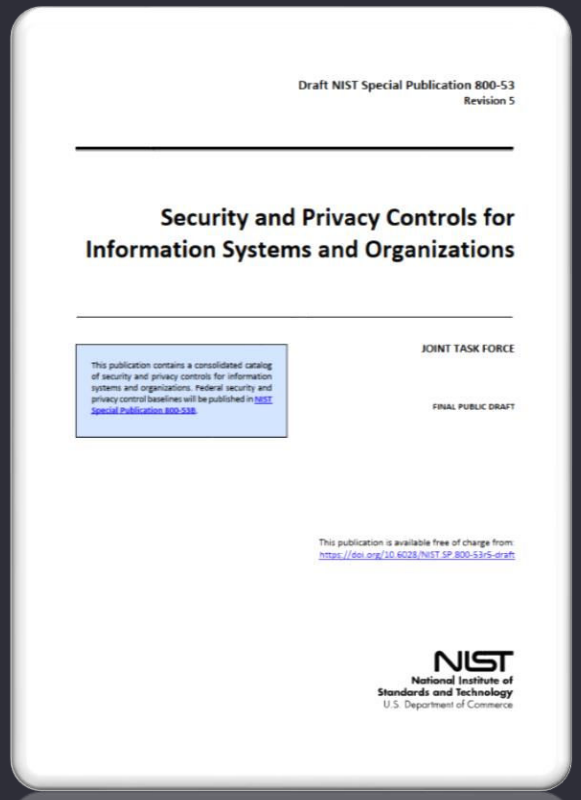
3.3. Adatgazdák és rendszergazdák kijelölése, nyilvántartása

3.3.1. Kijelölés

37. A Cégcsoport információs vagyonelemeinek adatgazdáit az adott szervezet Általános Vezérigazgató-helyettese jelöli ki. Az Információbiztonság vezetője feladata, hogy a kijelöléshez szükséges információs vagyonelemeket teljes körűen azonosítsa, és amennyiben szükséges, javaslatot tegyen az egyes adatgazdák személyére.

38. A Cégcsoport informatikai rendszerelemeinek rendszergazdáit az IT Management vezetője jelöli ki, illetve kiszervezett üzemeltetésű informatikai rendszer elem esetén gondoskodik róla, hogy igazolhatóan elkészüljenek és mindenkor aktuálisak legyenek a kinevezésről szóló dokumentumok.

16/131



Draft NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

JOINT TASK FORCE

This publication contains a consolidated catalog of security and privacy controls for information systems and organizations. Federal security and privacy control baselines will be published in NIST Special Publication 800-53B.

FINAL PUBLIC DRAFT

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-53r5-draft

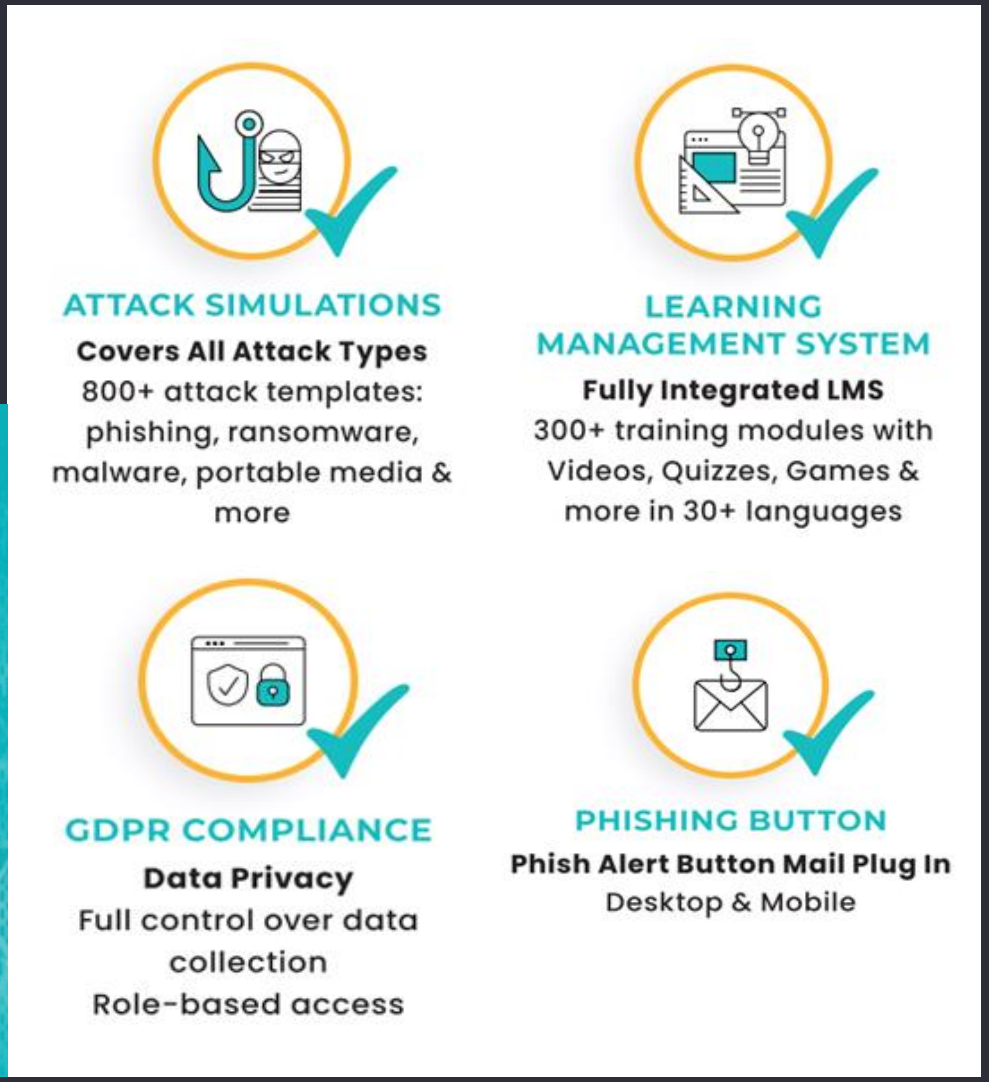
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NIS2 felkészülési lehetőségek: adathalász szimulációs keretrendszer

Mivel a kibertámadások 90%-a adathalász támadással kezdődik, ha kiemelt figyelmet fordítunk erre a területre, jelentősen csökkenteni tudjuk a kiberkockázatokat:

a) Oktatási keretrendszer

b) Adathalász szimulációs keretrendszer

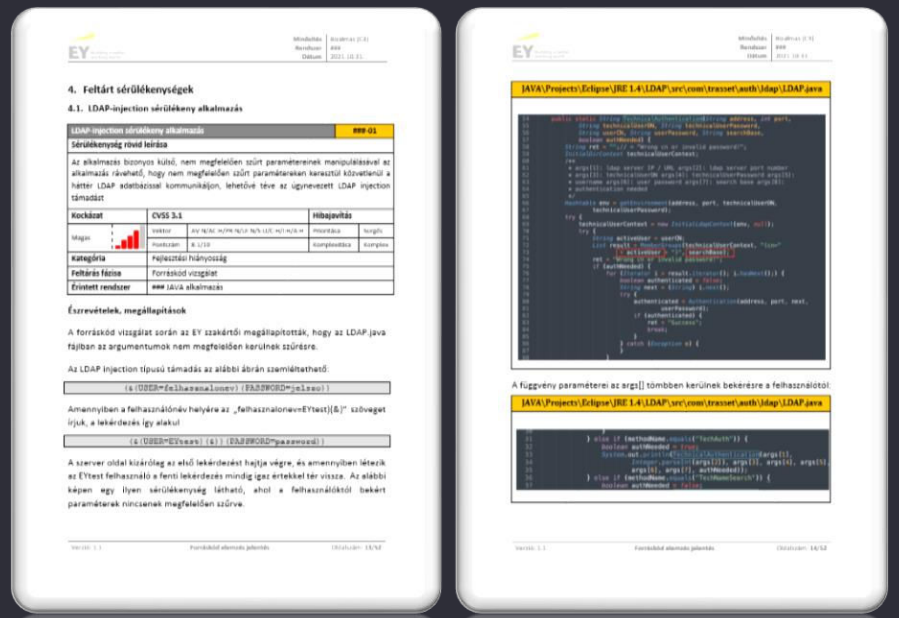


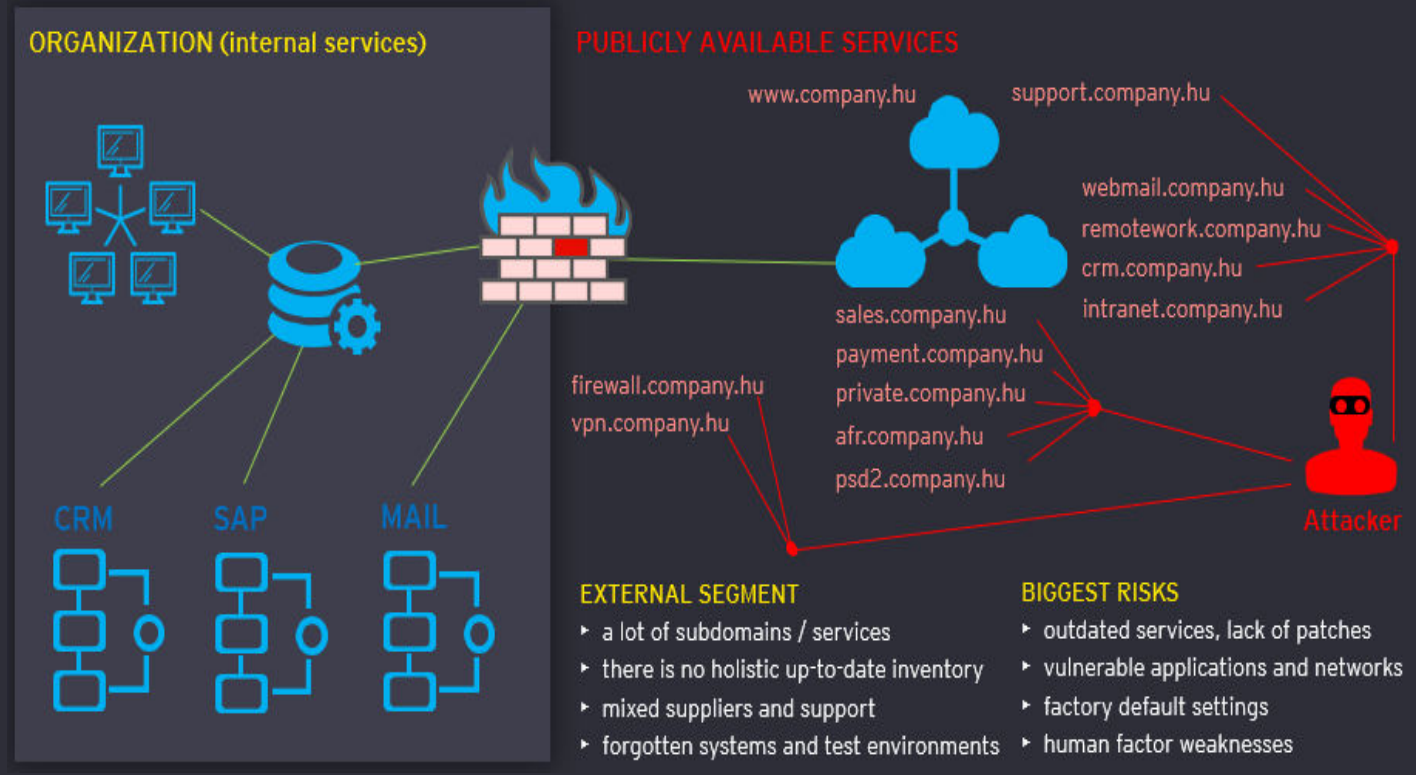
NIS2 felkészülési lehetőségek: Offensive Cyber Attack Simulation

Offensive Cyber Attack Simulation

Metodológia

- EY eXtreme hacking módszertan
- cvss v3.1 értékelési szabvány
- magasan képzett szakértők
- részletes dokumentáció, minden találat esetén reprodukciós evidencia és útmutató





EXTERNAL SEGMENT

- a lot of subdomains / services
- there is no holistic up-to-date inventory
- mixed suppliers and support
- forgotten systems and test environments

BIGGEST RISKS

- outdated services, lack of patches
- vulnerable applications and networks
- factory default settings
- human factor weaknesses

Köszönjük a figyelmet!

Minden harmadik válaszadó (36%) arra számít, hogy **olyan sikeres támadás fogja érni**, amelyet jobb költségallokációval **el lehetett volna kerülni**.
76% szerint a kollégák csak **akkor vonják be** az IT biztonságot a projektekbe, ha a **tervezési szakasz befejeződött**.

Mihály Zala
Partner | Head of Technology Risk and Cybersecurity
Ernst & Young Tanácsadó Kft.