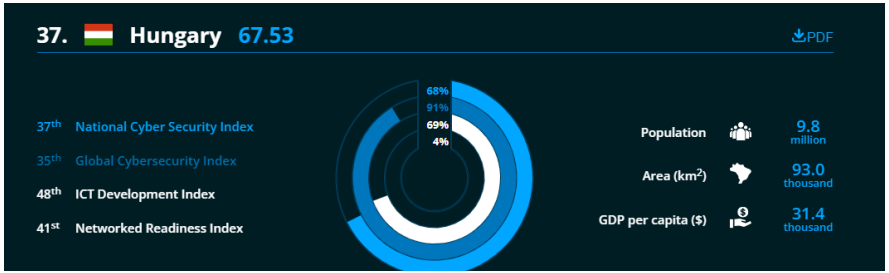
AI-alapú Anomália Detekció

A Digitális Védelem Új Határa

Összeállítója a Nemzetközi Távközlési Egyesület (ITU), az ENSZ telekommunikációval foglalkozó szakosított szervezete. Azt méri, hogy a vizsgált országok milyen intézkedéseket hoznak a kiberbiztonsági kockázatok kezelésére. Öt szempont alapján értékeli az országok teljesítményét:

- Jogszabályi intézkedése
- Technikai intézkedéseket
- Szervezeti intézkedéseket
- kapacitásfejlesztési intézkedéseket
- kooperáció mértékét



1. 2015-ös első kiadásban Magyarország: 0,6765-os összesített pontszámot ért el, ezzel **globálisan a 6. helyen állt (mivel több holtverseny is előállt, ez valójában azt jelenti, hogy az első 15-19. között volt), Európán belül pedig a 3. (5-8.) helyen**.
2. A 2017-es második kiadásban 0,534-es pontszámmal **globálisan az 51. (a holtversenyeket is figyelembe véve 57.) helyre esett vissza, míg Európában a 25.-re.**
3. A legutóbbi, 2023-as adat szerint az értékelt 194 ország közül Magyarország **globálisan 37. helyre került, Európában pedig a 22. (23.) helyre**. A szűkebb régiónkból Horvátország, Ausztria és Lengyelország mellett Szlovákia és Csehország, Románia is elénk került, de újra megelőztük például Izraelt.

neti

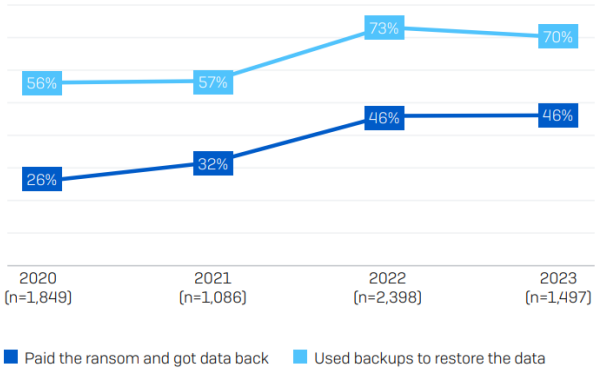
Nemzetközi kitekintés ransomware támadások

2020	2021	2022	2023
51%	37%	66%	66%

100-250 employees 62%
251-500 employees 62%
501-1000 employees 62%
1001 – 3000 employees 73%
3001 – 5000 employees 63%

30%
Of ransomware attacks where data was encrypted reported that data was also stolen

Use backups to restore data	Paid the ransom and got data back	Use other means to get data back
70%	46%	2%



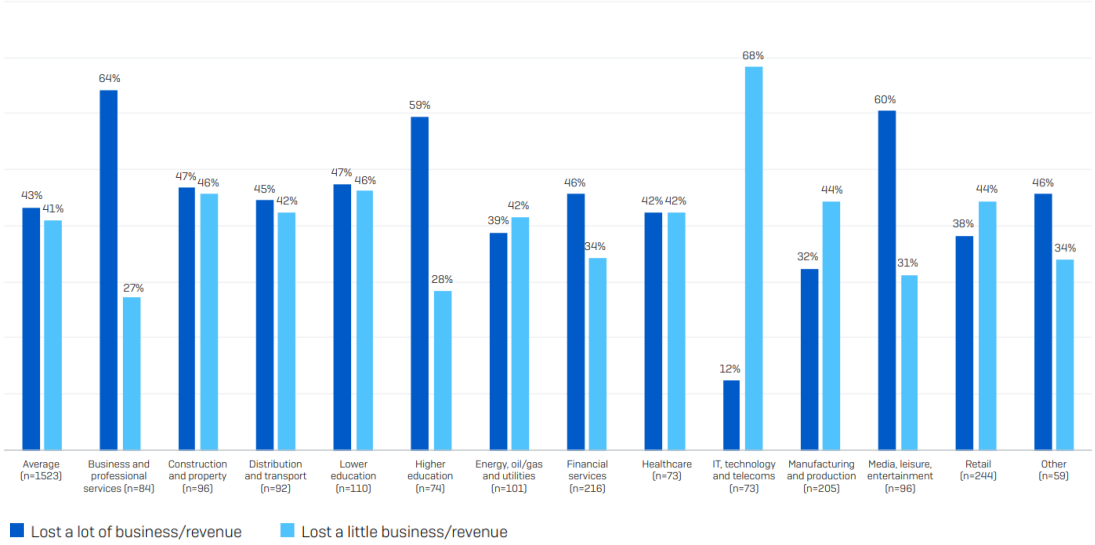
Mean Recovery Cost

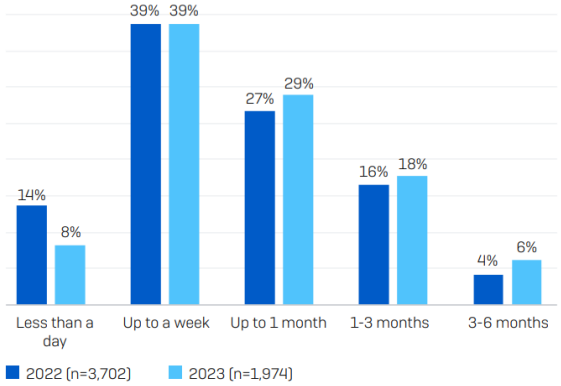
2021	2022	2023
$1.85M	$1.4M	$1.82M

A Sophos Whitepaper. May 2023 The State of Ransomware 2023

neti

Loss of Business/Revenue by Industry





Attacks Are Happening Faster Than Organizations Can Respond...

Average Days from "Compromise" to "Exfil"[1]

Industry average
6 DAYS
to remediate

GDPR adopted rule
3 DAYS
Data Breach
Notification[2]

Sources:
1) Unit 42 Cloud Threat Report - Volume 7, 2023, Unit 42 Engagement Experience;
2) Under the GDPR Notification Rules, an incident that causes accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

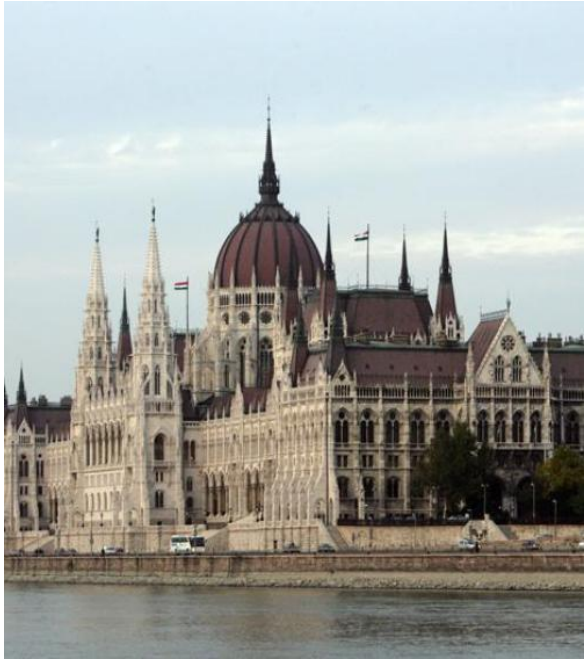
neti

- Tavaly Magyarországon többféle kibertámadás is előfordult, ugyanakkor az adathalászat (phising), a ransomware és az elosztott szolgáltatásmegtagadás (DDoS) kiemelkedett az élmezőnyből. Az idei év első két hónapjában mindez folytatódott.

- A támadások két cégméret szerint voltak csoportosíthatók a hazai kibertájképet nézve: kis- és középvállalkozások (kkv) és nagyvállalatok.

- A nagyvállalatok működését DDoS-támadásokkal igyekeztek ellehetetleníteni, és **komoly adatlopási kísérletek** célpontjai voltak. Noha erősebb és összetettebb védelmi rendszereik vannak, sok esetben ezek sem voltak elég naprakészek a szofisztikált támadásokkal szemben.

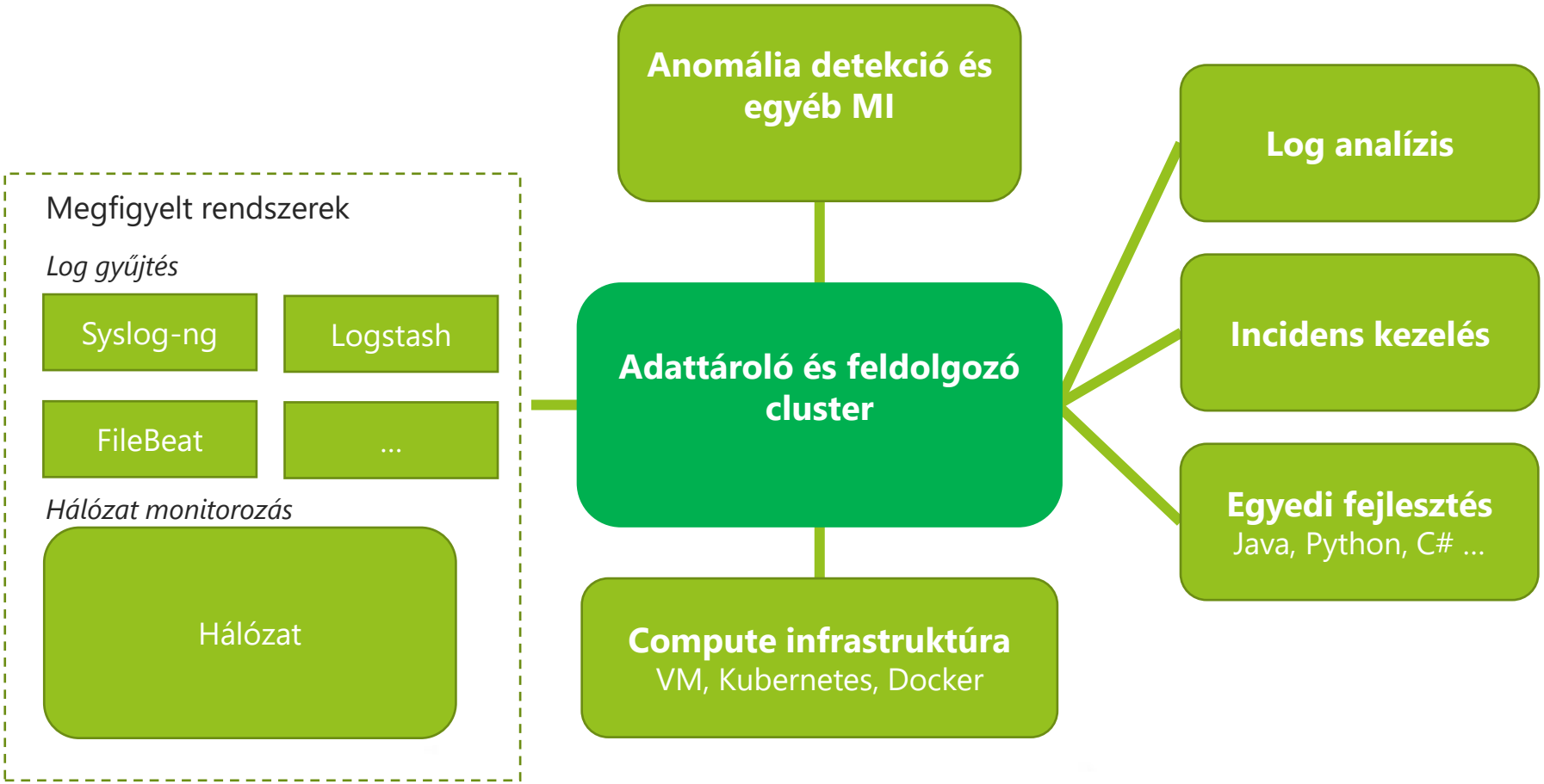
- A kibertolvajlás tekintetében a 2023-as év fordulópontnak számított hazánkban. A pénzügyi csalásokhoz köthető **online károk értéke meghaladta a 30 milliárd forintot**.



REAL TIME **ON-PREMISE** **KÖLTSÉGHATÉKONY** **AUTOMATIZÁLT**

EGY PLATFORM

- Az összes jelenlegi elterjedt SIEM vagy felhő alapú vagy forgalomkorlátos
- Az összes jelenlegi SIEM rendszert ki lehet iktatni/támadást el lehet fedni ha zajt keltenek, túlterhelik


Anomália detekció és egyéb MI
Log analízis
Megfigyelt rendszerek
Log gyűjtés
Syslog-ng
Logstash
FileBeat
...
Hálózat monitorozás
Hálózat
Adattároló és feldolgozó cluster
Incidens kezelés
Egyedi fejlesztés
Java, Python, C# ...
Compute infrastruktúra
VM, Kubernetes, Docker

KÖSZÖNÖM A MEGTISZTELŐ FIGYELMET!