MIÉRT NEM ALSZANAK A CISO-K (SE)

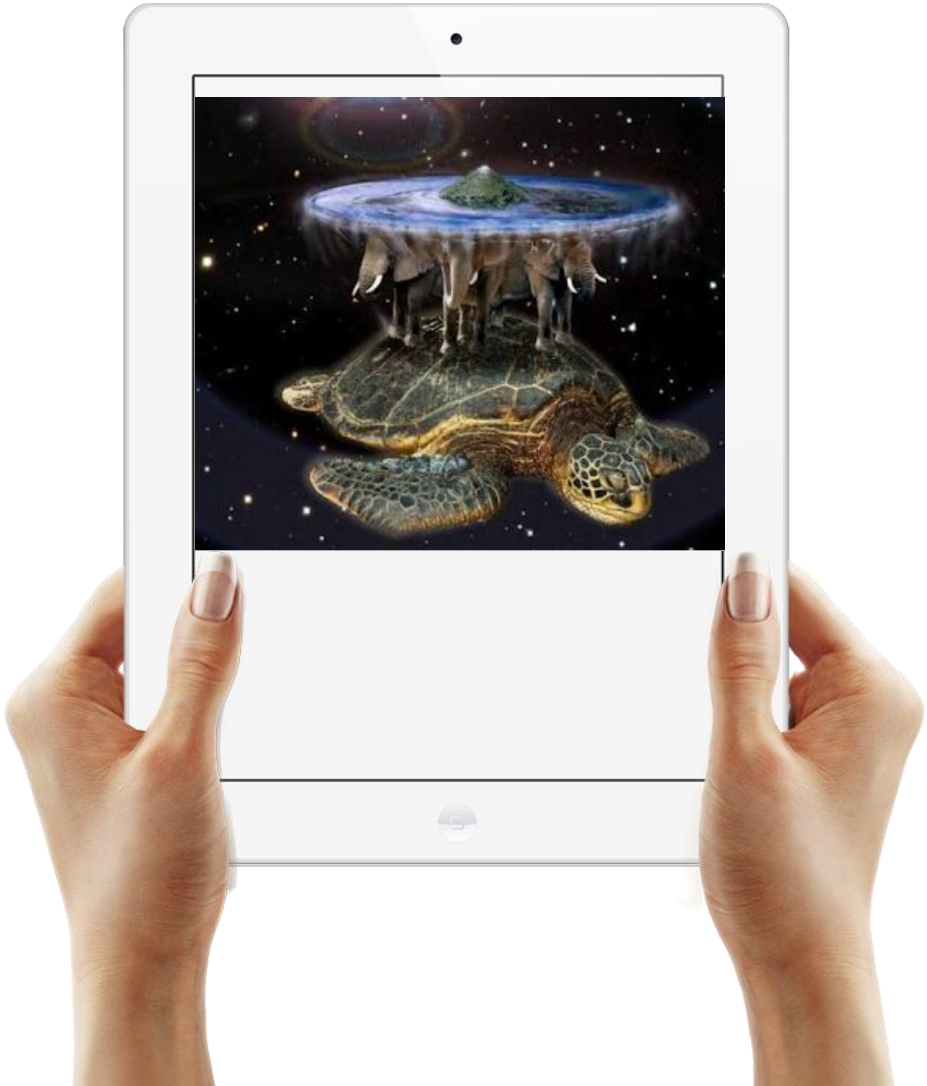
Hári Krisztián

Nemzeti Infokommunikációs Szolgáltató – HUN-SOC

2021

ÜGYFÉL

- Bármit, bárhonnan, bármikor
- Elektronikus ügyintézés
- Otthoni munkavégzés
- Technológiai függőség



7,83 milliárd

Lakosság

5,22 milliárd

Mobil felhasználó

4,66 milliárd

Internet felhasználó

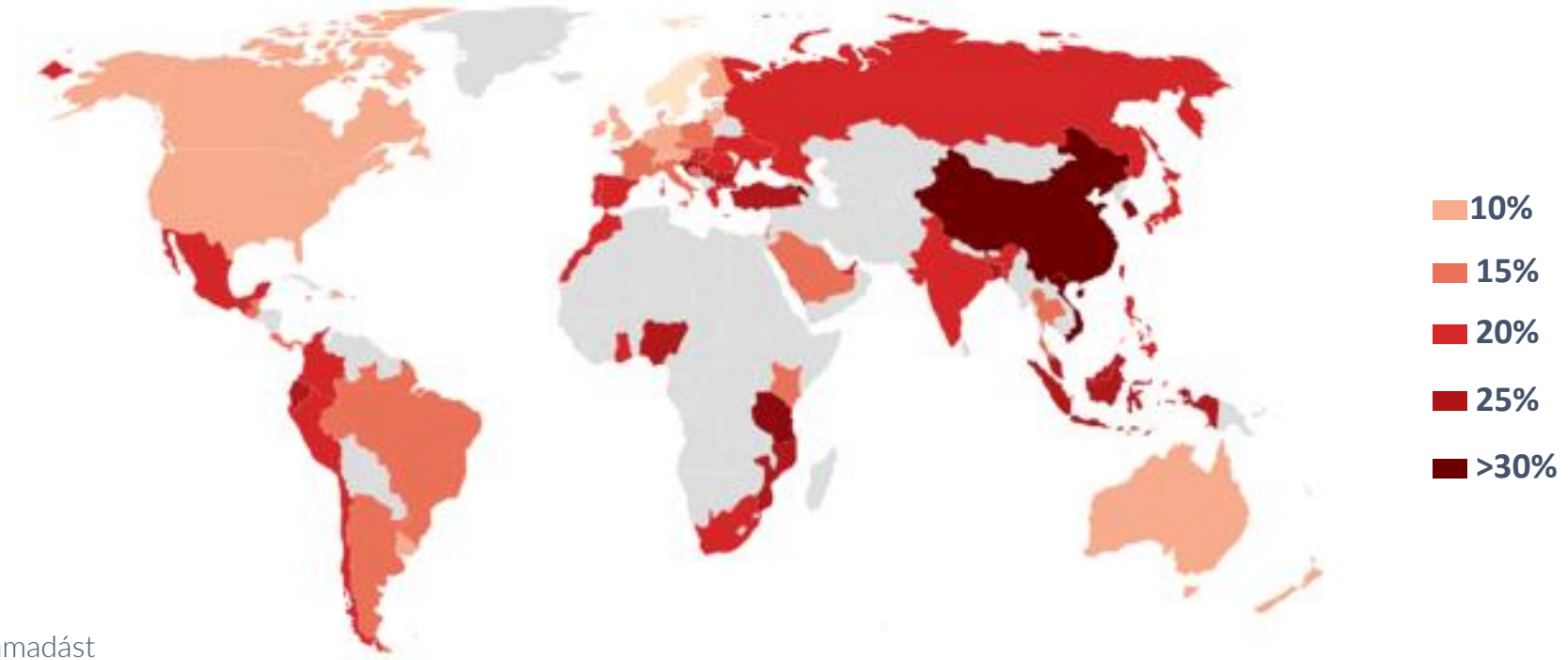
4,2 milliárd

Közösségi média felhasználó

Datareportal, Digital 2021, 2021 Január

Közösségi média	Mobil applikáció	TV nézés	Hírolvasás	Internet
2 óra 25 perc	4 óra 10 perc	3 óra 24 perc	2 óra 02 perc	6 óra 54 perc

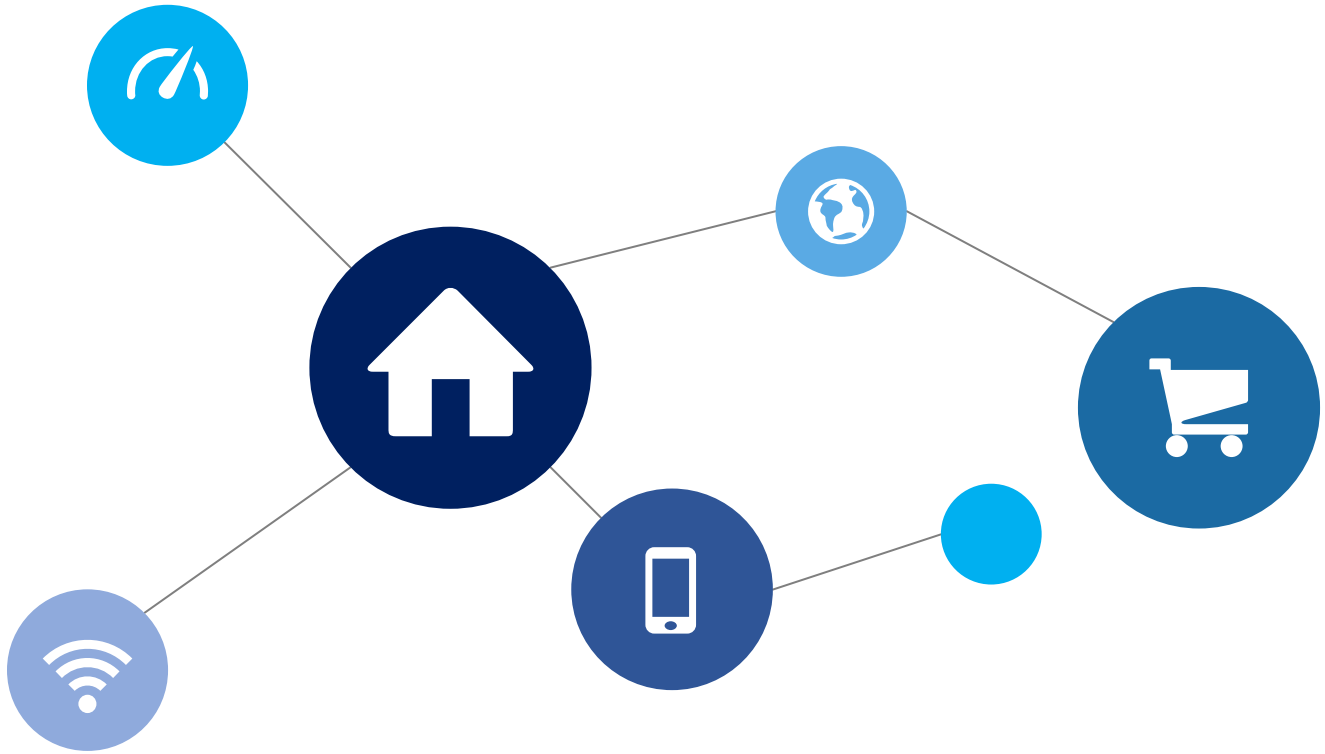
Datareportal, Digital 2021, 2021 Január



Malware és APT támadást elszenvedő gépek százaléka.

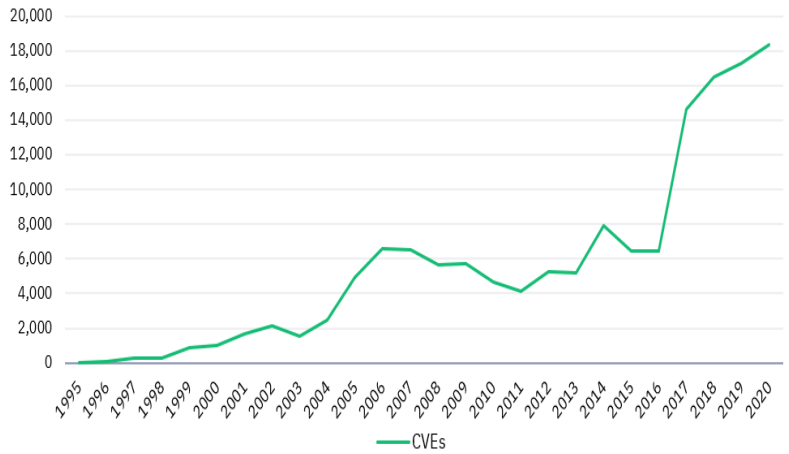
Avast, 2021 Augusztus

SZOLGÁLTATÓ



- Elérhetőség
- Architektúra
- Kapacitások
- Kiberbiztonság
- Szállítók, szoftverek, hardverek

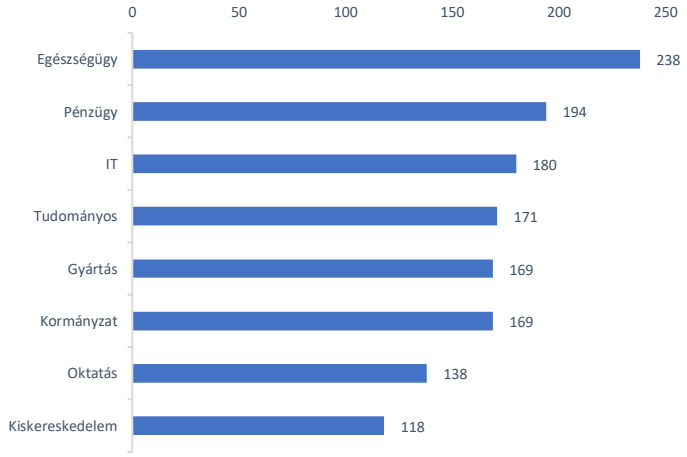
Sebezhetőségek



2020-ban több sebezhetőséget találtak, mint azt megelőzően összesen. 50 CVE naponta. 57%-a kritikus, vagy magas besorolású. 68%-a nem igényel felhasználói interakciót.

NIST NVD CVEs, 2020

Incidensek



TOP 8 szektor a bejelentett incidensek száma alapján.

RiskBasedSecurity, 2021 Q2

GDPR – 3 év

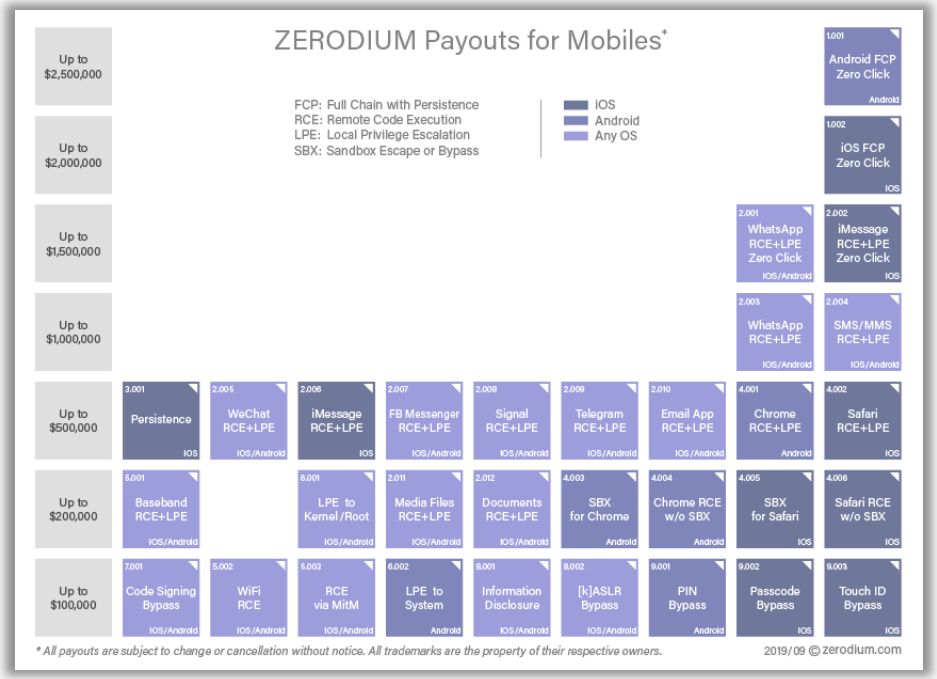
Amazon	746 m€
Google	50 m€
H&M	35 m€
TIM	27,8 m€
British Airways	22 m€
Marriott	20,4 m€
Wind	17 m€
Vodafone IT	12,3 m€
Notebooksbillinger.de	10,4 m€

- Gazdasági, politikai motiváció
- Minden online
- ML és AI
- Kár és a hatás is nagyobb
- Nem erre tervezett rendszerek

-= PACKAGES COMPARISON =-

	Package #3	Package #2	Package #1	Package #ELITE
Subscription	1 Month	6 Months	12 Months	12 Months
Darknet C&C Dashboard	Yes	Yes	Yes	Yes
Features: Delayed Start, Delayed Encryption, Mutex, Task Manager/Registry Editor Disabler, UAC Bypass, Desktop Wallpaper Changer	Yes	Yes	Yes	Yes
Offline Encryption	No	Yes	Yes	Yes
Support	No	Yes	Yes	Yes
Real-Time Client Manager	No	Yes	Yes	Yes
Dropper	No	Buy	Yes	Yes
Clone	No	Buy	Buy	Yes
FUD+Obfuscator	Buy	Buy	Buy	Yes
Unkillable Process	No	Buy	Buy	Yes
FUD Stub #	1	1	2	12
Price	120 USD	490 USD	900 USD	1900 USD

welivesecurity



306 milliárd €-s piac

5.000 milliárd € kár

Július

- Kínai APT Dél-kelet Ázsiában
- Pegazus
- USA, EU, NATO közös nyilatkozat a Kínai MS Exchange hack miatt
- Iráni adathalászat vs. amerikai katonaság ellen
- DDoS vs Orosz Védelmi Minisztérium
- Ukrán Védelmi Minisztérium vs Orosz hackerek

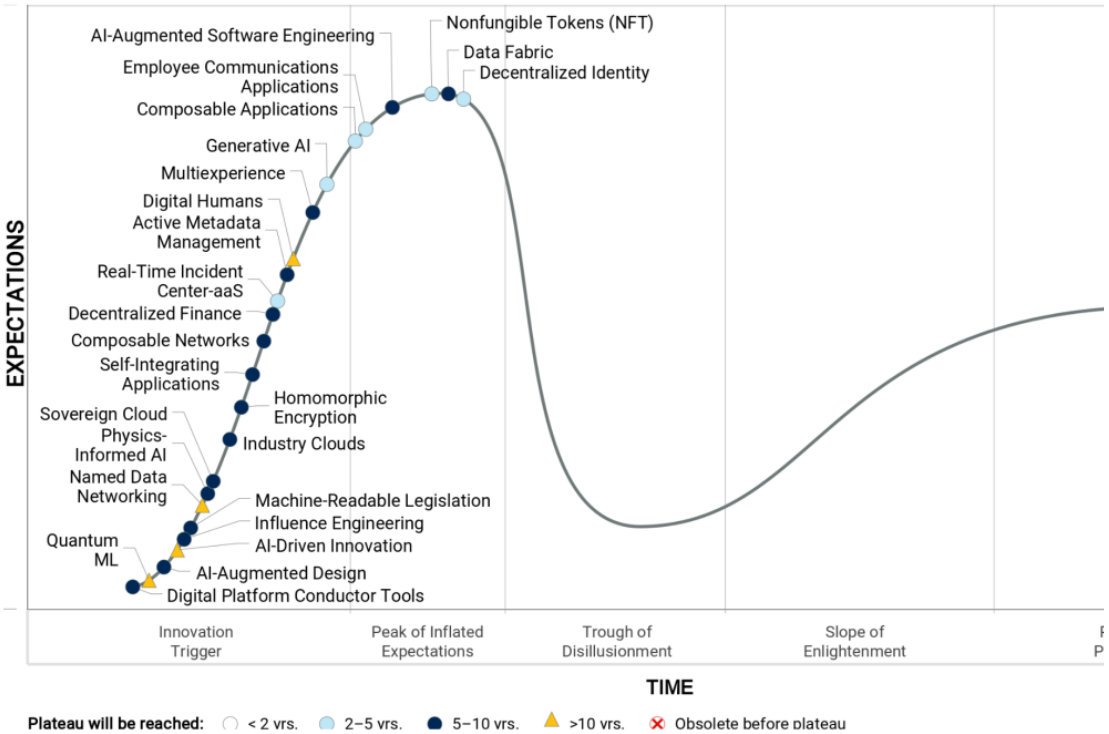
Augusztus

- Kínai támadások Dél-kelet Ázsiai mobil szolgáltatók ellen
- Orosz kiberkémkedés Szlovák kormányzat ellen
- Kibertámadás Belorusz rendőri és minisztériumi adatbázisok ellen

Szeptember

- Kínai támadások Norvég szolgálatok ellen
- Litván Védelmi Minisztérium Kínai cenzúrát talált népszerű 5G okostelefonban
- Kínai hackerek Afgán telekom adatokat loptak el

Hype Cycle for Emerging Technologies, 2021

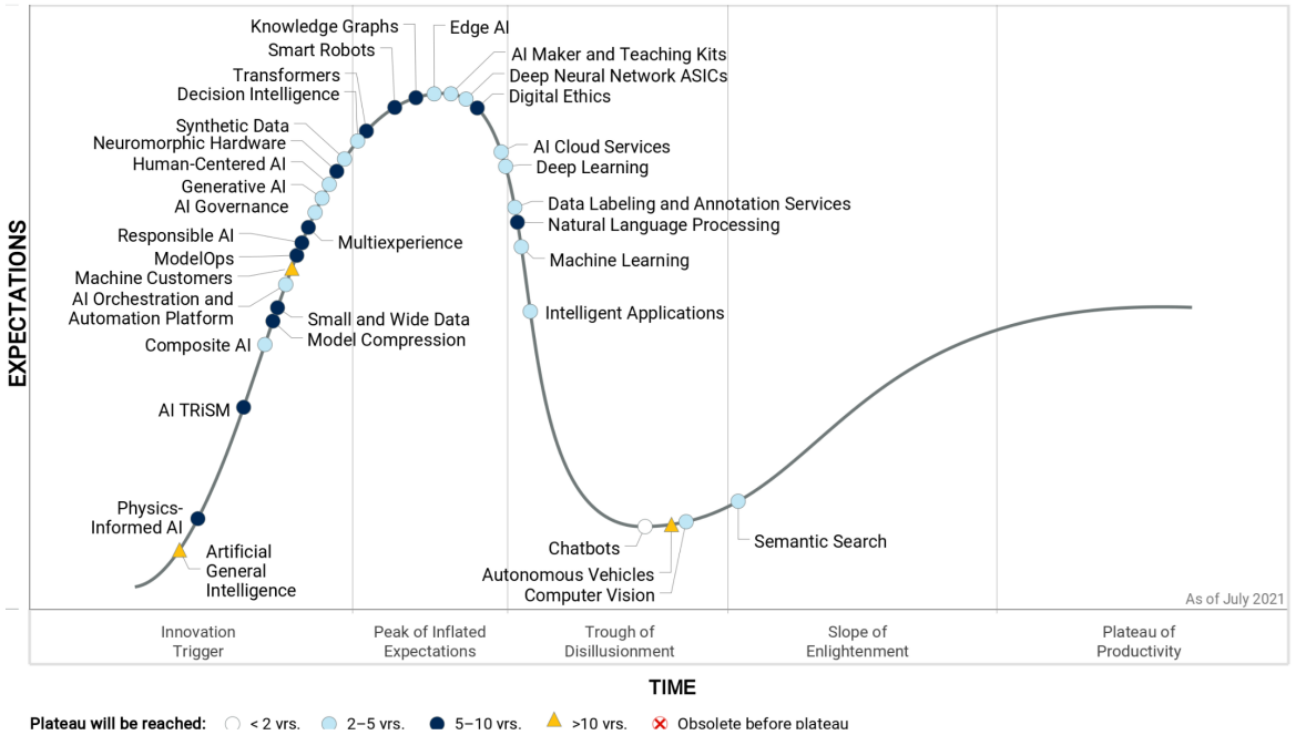


Plateau will be reached: < 2 yrs. 2–5 yrs. 5–10 yrs. >10 yrs. Obsolete before plateau

Source: Gartner (August 2021)

747576

Hype Cycle for Artificial Intelligence, 2021



Plateau will be reached: < 2 yrs. 2–5 yrs. 5–10 yrs. >10 yrs. Obsolete before plateau

Source: Gartner (July 2021)

747539

Forrás: Gartner

STATISZTIKÁK – NEMZETI KIBERBIZTONSÁGI INTÉZET

Incidensek ügyfélkör szerinti éves eloszlása

Intézményi felhasználók

Kiszolgált intézmények száma
286 db

Vezetékes telefon felhasználók
106 398 db

Postafiók-felhasználók száma
138 757 db postafiók
186 407 db felhasználó

Mobiltelefon (mobil internet) felhasználók
15 297 fő

Asztali és mobil Munkaállomás-felhasználók
28 424 db

Informatikai háttér

Nyomtatók
15 001 db

Alkalmazások (alkalmazáspéldány)
936 db

Tárolórendszerek kapacitása
24 000 000 GB

Szerverek száma-fizikai
2 928

Nemzeti Távközlési Gerinchálózat végpontok
10 852 db

Védelem

Védelmi technológiák

Érzékelés

Kiber esemény felismerési képességek és technikák

Válasz

Válasz adási képességek a felismert események alapján

Azonosítás

Rendszerek, személyek, értékek, adatok és képességek

Helyreállítás

Az ellenállóképesség fenntartása és visszaállítási képességek

Forrás: NIST

STRATÉGIAI ELEMEK

Humánképességek

A jövő magyar szakembereinek képzése és megőrzésüknek a biztosítása. A felhasználók kiberbiztonsági tudatosságának építése.

Passzív védelmek

Biztonságos fejlesztések, kontrollált és szabályozott környezetben, átvételi tesztelésekkel. Szoftver és hardverek vizsgálata a beszerzések előtt, mind üzemeltetési, mind biztonsági szempontból. (pl. ÁAFK)

Aktív védelmek

Nemzetközi sztenderdek alapján felépített operatív védelmi központ kialakítása és üzemeltetése. (HUN-SOC)

Mentés és helyreállítás

Mentési és helyreállítási környezetek, folyamatok és támogató endszerek kialakítása, amely biztosítja a nem várt események utáni üzletmenet folytonosságot. (pl. KAT)

KÖSZÖNÖM A FIGYELMET!