NEMZETI INFOKOMMUNIKÁCIÓS SZOLGÁLTATÓ KIBERBIZTONSÁG

Hári Krisztián

Elektronikus információbiztonsági igazgató - CISO

NISZ Zrt.

HTE konferencia

2022

- Geopolitika határozza meg a támadásokat
- TOP2 támadási forma a Ransomware és DDoS
- Államilag szponzorált támadások zero-day alapúak

2021

42 ország,

128 kormányzati szerv

LEGFŐBB FENYEGETETTSÉGEK

Ransomware

Több mint 10 terrabyte adat lopás havonta.
Feltehetően az áldozatok több mint 60% fizet.

Malware

Továbbra is folyamatosan növekszik a támadások száma (crypto-jacking, IoT).
A felhő átállások tovább növelik a támadási lehetőségeket.
2021-ben 66 darab zero-day-t használtak fel.

Social engineering

Social engineering és kiemelten a phishing támadások, továbbra is kedvelt támadási formák, kihasználva az Ukrán – Orosz konfliktust.

Forrás adatok támadása

Az adatok forrására koncentráló támadások, azok megszerzésére, közzétételére, manipulálására és/vagy megsemmisítésére fókuszálva.

Elérhetetlenné tétel - DoS

Második legtöbbet használt támadási forma.
Újabb és újabb rekord méretű támadásokkal.

Elérhetetlenné tétel – Internetes trükkök

Internet infrastruktúra megsemmisítése, forgalom eltérítések.

Dezinformáció, félre informálás

MI alapú dezinformáció, deepfake és dezinformáció mint szolgáltatás, például választások, zöld átállás, covid-19 és Ukrán-Orosz konfliktus információi ellen.

Ellátási láncok elleni támadások

2021-ben már a behatolások 17% az ellátási lánc elleni támadásra alapult.

NISZ

Intézményi ügyfelek

- Kiszolgált intézmények száma
  275 db
- Vezetékes telefon felhasználók
  104 671 db
- Postafiók-felhasználók száma
  35 641 db postafiók
  28 334 db felhasználó
- Mobiltelefon (mobil internet) felhasználók
  17 428 fő
- Asztali és mobil Munkaállomás-felhasználók
  21 799 db

Technikai háttér

- Nyomtatók
  19 696 db
- Alkalmazások (alkalmazáspéldány)
  883 db
- Tárolórendszerek kapacitása
  36 400 000 GB
- Szerverek száma-fizikai
  3 481
- Nemzeti Távközlési Gerinchálózat végpontok
  9 579 db

NISZ

Állampolgárok

Cégkapu (regisztráltak száma)
678 394 db

Ügyfélkapu (regisztráltak száma)
5 495 834 db

Hivatali kapu (regisztráltak száma)
15 092 db

Beérkező hívások száma
16 677 388 db

Chat beszélgetések száma
1 521 503 db

Kezelt emailek száma
1 860 487 db

1818


TE MONDD, HOGY KIBERTÁMADÁS

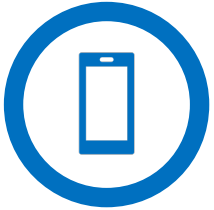
KIBERBIZTONSÁGI SZOLGÁLTATÁSAINK

- Levelezés-védelemi szolgáltatás
- Hálózati forgalom védelme
- Biztonsági naplógyűjtés és elemzés
- Végpont és szervervédelem
- Integritás-védelem
- Hordozható eszköz védelem
- Központi Internet elérés védelem
- Privilegizált felhasználók védelme
- 7x24 órás kiberbiztonsági felügyelet
- Kiberbiztonsági tanácsadás
- Felhasználói és hálózati adatszivárgás megelőzés
- Adatmentesítés
- Túlterheléses támadás (DDoS) elleni védelem
- Jogosultság-kezelés

STATISZTIKÁINK - HAVI

1.484

Biztonsági esemény



732

Levél támadási kísérlet

636

Hálózati támadási kísérlet

4.400

Túlterheléses támadási kísérlet

KÖRNYEZETÜNK

TECHNOLÓGIAI

- Avulás
- >50 CVE naponta
- Biztonságos fejlesztések hiánya
- APT-k zero-day

FINANSZÍROZÁSI

A finanszírozási szabályok áttekintése, EU és hazai finanszírozású projektek fentarthatóságának biztosítása, a termék, szolgáltatás életútjának tervezése.

EGYÜTTMŰKÖDÉS

Iparági és iparágak között információ és feladatmegosztás, együttműködés.

SZABÁLYOZÁSI

Szabályozások hozzáigazítása a technológiai fejlődéshez és megváltozott működési modellekhez.

EU KIBERBIZTONSÁGI STRATÉGIA ELEMEI - 2020

RESILIENCE, TECHNOLOGICAL SOVEREIGNTY AND LEADERSHIP

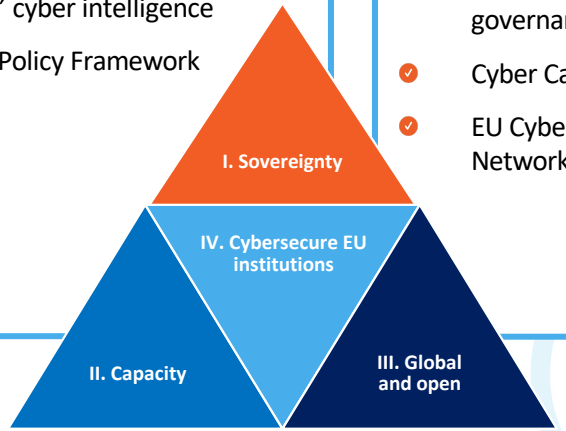
- Revised Directive on Security of Network and Information Systems (NIS 2)
- Cybersecurity Shield (CSIRT, SOC)
- Secure Communication Infrastructure: Quantum, NG Mobile, IPv6, DNS
- Competence Centre and Network of Coordination Centres (CCCN)
- EU workforce upskilling

BUILDING OPERATIONAL CAPACITY TO PREVENT, DETER AND RESPOND

- Cybersecurity crisis management framework
- Cybercrime agenda
- Member States' cyber intelligence
- Cyber Defence Policy Framework

COOPERATION TO ADVANCE A GLOBAL AND OPEN CYBERSPACE

- EU leadership on standards, norms and frameworks in standardisation bodies
- Promote Multi-Stakeholder Internet governance model
- Cyber Capaacity Building Agenda
- EU Cyber Dialogue and Diplomacy Network



DEP 2021 - 2022

European cyber shield

- Resilience, coordination and cybersecurity ranges
- SOCs
- 5G and digital infrastructures
- Uptake of innovative cybersecurity solutions
- Health sector cybersecurity

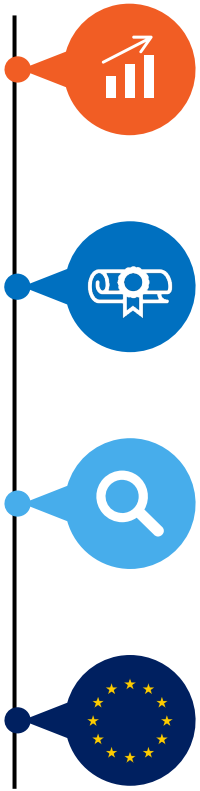
Support to legislation

- National Coordination Centres
- Community support
- NIS Directive implementation
- Testing and certification

Other

- EuroQCI
- Advanced digital skills

FELADATAINK



KIBER ÉS KIBERBIZTONSÁGI STRATÉGIA

Megújítani, modernizálni és az EU tagországokkal harmonizálni Magyarország kiber és kiberbiztonsági stratégiáját.

KÖVETELMÉNYEK ÉS TANÚSÍTÁSI RENDSZER

Egységes betartható, ellenőrizhető, mérhető követelmény rendszert kialakítani, tanúsítási lehetőséggel.

KIBER ELLENÁLLÓKÉPESSÉG FEJLESZTÉSE

Iparági, vagy közös szinten kialakítani azon kapacitásokat, amelyek lehetővé teszik az érzékelés, beavatkozást és helyreállítást országos szinten akár iparágtól függetlenül is.

EU EGYÜTTMŰKÖDÉS, FINANSZÍROZÁS

Részvétel a kiberrel kapcsolatos EU-s kezdeményezésekben, közös fejlesztésekben, az eredmények, támogatások felhasználása az ellenállóképesség fejlesztésére.

NISZ

KÖSZÖNÖM A FIGYELMET!