

MEDICINA FÓRUM

2023. NOVEMBER 15.

A kiberbiztonság egészségügyi vonatkozásai, aktuális helyzetkép




NEMZETI
KIBERVÉDELMI INTÉZET

Nemzetbiztonsági Szakszolgálat

Nemzeti Kibervédelmi Intézet

CSIRT

- Incidens kezelés
- Riasztás
- Tájékoztatás

Technikai kivizsgálás

- Logelemzés
- Forensics
- Malware elemzés

Esemény- észlelés

- EWS
- Honeypot
- Big data
- Trendelemzés
- CTI

Sérülékenység vizsgálat

- Külső
- Belső
- Webes
- Wifi
- Social engineering

Tudatosítás

- Kiberhónap
- HUNEX
- HCSC
- Podcast
- Elemzések
- Figyelmeztetések

Hatóság

- Nyilvántartás
- Ellenőrzés
- Légügyi szakhatósági tevékenység
- SPOC



ÜGYFELEINK

1995. évi XCVII.
169/2010 korm. rend.
a légügyi védelmi programok
megfelelőségének értékelése

2009/2015 korm. hat.

2013. L tv.

Állami szervezetek
Önkormányzatok



2012. CLXVI. tv 2 §

Energia
Közlekedés
Agrárgazdaság
Egészségügy
Társadalombiztosítás
Pénzügy
Infokommunikációs technológiák
Víz
Közbiztonság-védelem
Honvédelem (HÁEIBEK)



2001. CVIII. tv 2 § j)

Online piactér
Keresőszolgáltatás
Felhőalapú szolgáltatás



271/2018 korm. rend.

Egyszerű adatátvitel
Gyorsítótárazás
Keresőszolgáltatás



Megfelelőség (hatóság)



Incidenskezelés



Sérülékenységvizsgálat

Légügyi
szereplők



Állami és
önkormányzati
szervek

Alapvető
szolgáltatások

Nemzeti
létfontosságú
rendszerlemek

NB védett
szervezetek



Közvetítő
szolgáltatók



Bejelentés
köteles
szolgáltatók





EGÉSZSÉGÜGYI ADATOK KIBERBIZTONSÁGI VESZÉLYEZTETETTSÉGE

Adathalászat (Phishing)

Ransomware-támadások

Szolgáltatás-leállítás (Denial of Service - DoS)

Hálózati sebezhetőségek

Adatlopás és jogosulatlan hozzáférés

Pszichológiai manipuláción alapuló támadások

Hibás alkalmazások

Kiberkémkedés



A Hatóság szerepe és tevékenysége

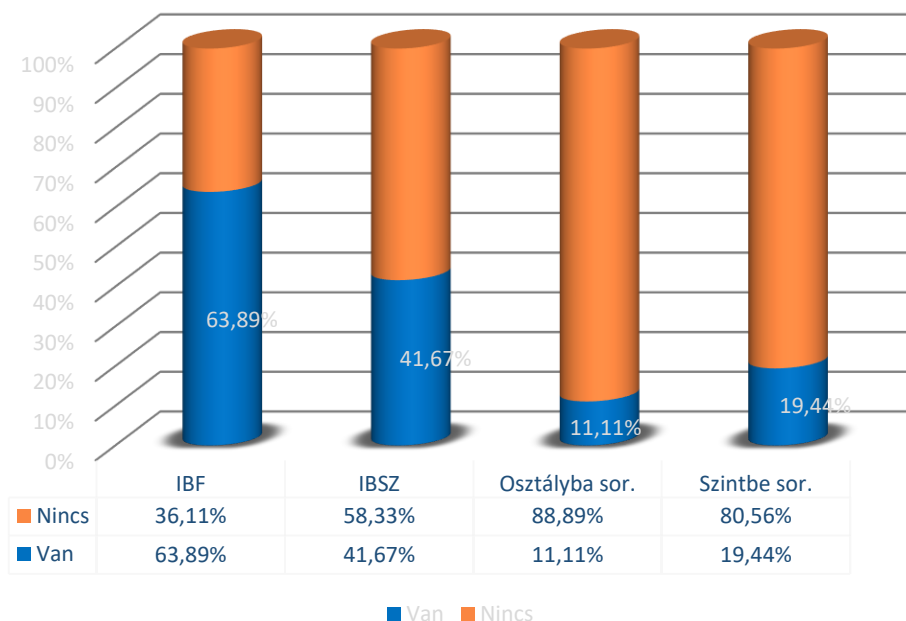
- ▶ 2022. februártól fokozott aktivitás a kritikus infrastruktúrák rezilienciájának növeléséhez
- ▶ 14 szervezet komplex ellenőrzése
- ▶ 36 egészségügy ágazathoz tartozó szervezet részellenőrzése
- ▶ Adatbekérő kampány

Cél: a hiányosságokat feltárni, azok javítását előírni és kikényszeríteni

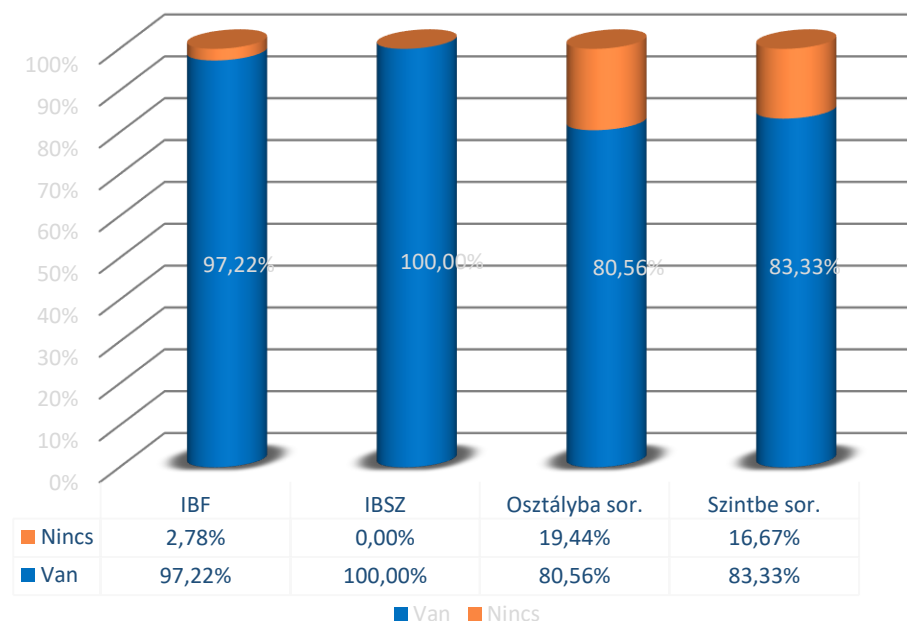


A 2022-ben folytatott adatbekérő kampány eredményei

**Egészségügy ágazat - Alapfeladatok
2022.07**



**Egészségügy ágazat - Alapfeladatok
2023.03**





Nemzeti CSIRT

Incidenskezelési tapasztalatok

- **Fiók kompromittálódás**
 - Első sorban nem-adminisztrátori fiókok érintettek.
- **Adathalászat**
 - Kórházak munkatársait érinti nagy létszámban.
 - Egészségügyet legjobban érintő adathalászat jellegű megszemélyesítés -> EESZT
- **Az elmúlt évek során volt példa ransomware fertőzésre is**
 - Javuló biztonsági mentési eljárások miatt gyorsabb helyreállítás kevesebb adatvesztés
 - Legnagyobb veszélyt az adatszivárgás illetve a kórházi betegellátás akadályozása jelenti



Szolgáltatások/Megoldások SOC

- KÓRHÁZI INTÉZMÉNYEK VÉDELME
 - Tűzfalon keletkező események elemzése
 - Fenyegetettség elemzés
 - Szakértői támogatás
 - Incidenskezelés támogatása
- Térítésmentes az állami fenntartású kórházak számára



IOT Kutatás – Intelligens Kórház

- Intelligens kórház

- Modern, intelligens egészségügyi és informatikai kihívások azonosítása
- Internetre köthető orvosi eszközökkel kapcsolatos kihívások
- Biztonsági helyzetkép

- Intelligens kórház biztonsági ajánlás

- Tipikus IoT ökoszisztémák feltérképezése
- Kiválasztott IoT ökoszisztémák biztonsági szempontú értékelése
- IoT ökoszisztéma biztonsági ajánlás kidolgozása



Szolgáltatások/Megoldások GovProbe 2.0

- Kormányzati Csapdarendszer (GovProbe) - Valós működést szimuláló, álcázott szolgáltatások
- A feltárt információk közvetlenül vagy automatizáltan hasznosíthatóak.
- Óránként:
 - ~50k csapda bejegyzés
 - ~200 malware letöltésre irányuló próbálkozás
- GovProbe 2.0
 - Magas interakciójú csapdák kifejlesztésével még inkább elérhetővé válik célzott támadások felderítése.
 - A GovProbe 2.0 szondák telepítése zajlik, kórházhoz is telepítünk



Prevenció

CTI + Tudatosítás

- Kiberfenyegetési kampányok, trendek monitorozása, figyelmeztetések
- Kiberbiztonsági elemzések, tájékoztatók szervezetek és a lakosság számára
- Igény szerint tudatosító előadások tartása
- Cybersec 2023, workshopok: fókuszban a kritikus ágazatok
 - Workshopok (nemsokára lehet jelentkezni)

EGYÜTTMŰKÖDÉSI MEGÁLLAPODÁS

Egészségügyi
Menedzserképző Központ
és a Nemzeti Kibervédelmi
Intézet együttműködése
2023. május 11.





Tudatosítás

NBSZ-NKI, SZTFH, Simmelweis EMK közös terméke



A BETEGEK RÁNK BÍZZÁK AZ ÉLETÜKET, DE MI VAJON MEGFELELŐEN VÉDJÜK ÖKET A KIBERVESZÉLYEKTŐL?

Az alábbiakban bemutatjuk az egészségügyi ágazatot fenyegető **öt legfontosabb** kiberbiztonsági fenyegetést és tippeket adunk azok enyhítésére!



Kiberh0nap@2023
OKTÓBER

E-MAIL ADATHALÁSZAT (PHISHING)

Az e-mailes adathalászat arra irányuló kísérlet, hogy e-mailt használva rávegyenek arra, hogy személyes adatokat adjunk meg, vagy olyan fertőzött linkekre kattintsunk, amelyek révén a hackerek hozzáférhetnek a betegeink összes adatához.

A sikeres támadások 90%-a ilyen adathalászzal indul!

- A fájlok csapdák lehetnek!
Ellenőrizze azokat, mielőtt a beágyazott hivatkozásokra kattint!
- A weboldalak csalók is lehetnek;
saját maga írja be az URL-eket, és ne linken keresztül érje el azokat!
- A jelszóval védett dokumentumok csatlások is lehetnek;
kinyitás előtt ellenőrizze azokat!



ESZKÖZÖK ELVESZTÉSE VAGY ELLOPÁSA

Tudta? A mindennapi eszközök, például laptopok, okos-telefonok és USB-meghajtók gyakran elvesznek vagy ellopják, és idegenek kezébe kerülhetnek.

- Soha ne hagyja felügyelet nélkül laptopját vagy berendezését!
- Mindig titkosítsa az érzékeny adatokat, amelyek a készülékein vannak!
- Azonnal értesítse az informatikust, vagy a kijelölt személyt, ha az eszköze elvész!



BENNFENTES, VÉLETLEN, ILLETVE SZÁNDÉKOS ADATVESZTÉS

Bennfentes fenyegetések minden szervezetben léteznek, ahol alkalmazottak, vállalkozók vagy más felhasználók hozzáférnek a szervezet technológiai infrastruktúrájához, hálózatahoz vagy adatbázisaihoz.

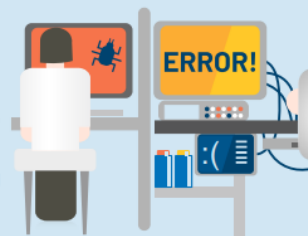
- Hallgasson az ösztöneire, és mindig jelezze azt, ha valami szokatlan, nem megfelelő történik a betegadatokkal vagy az informatikai rendszerrel!
- Véletlen tévedések folytán is előfordulnak adatvesztések vagy adatkezelési problémák (pl.: e-mail cím elgépelése).
Ha ilyen történik, azonnal értesítse a kijelölt szakembert, hogy megfelelően be lehessen avatkozni a további problémák megelőzése érdekében!
- Védje meg a betegek adatait azáltal is, hogy nem ad ki információkat, kivéve, ha megfelelően azonosította a kérelmező személyazonosságát!



TÁMADÁSOK A CSATLAKOZTATOTT ORVOSI ESZKÖZÖK ELLEN

Vegyük fontolóra a következőket: a kórház egy adathalász támadás áldozata, amely révén több kardiológiai monitorhoz csatlakoztatott szerver is érintetté válik. A támadás a rendszer teljes irányítását teszi lehetővé a hacker számára, így tetszés szerint ki- és bekapcsolhatja a rendszereket!

- A kórház védelme érdekében tájékozódjon, hogy hogyan lehet használni az informatikai rendszerhez kapcsolódó orvosi és nem orvosi eszközöket!
- A leggyakoribb problémát a lejárt támogatású vagy régi eszközök jelentik, ezért minden esetben tájékozódjon, hogy ezek alkalmasak-e az informatikai rendszerhez történő csatlakozásra és megfelelően frissített szoftverrel rendelkeznek-e!



Tájékozódjon
a friss egészségügyi
kiberbiztonsági hírekről!





HunEX gyakorlat



FÓKUSZBAN AZ EGÉSZSÉGÜGY

2023. November 02 – 6 intézmény

2023. November 23 – 18 intézmény



NIS 2 IRÁNYELV IMPLEMENTÁCIÓ

**AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2022/2555 IRÁNYELVE
(2022. december 14.)**

**az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító
intézkedésekről,**

**valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról
és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről
(NIS 2 irányelv)**



NIS 2 IRÁNYELV IMPLEMENTÁCIÓ

1. A 2011/24/EU európai parlamenti és tanácsi irányelv 3. cikkének g) pontjában meghatározott **egészségügyi szolgáltatók** (alapvető szolgáltatásokat nyújtó szereplőként azonosított)
2. Az (EU) 2022/2371 európai parlamenti és tanácsi rendelet 15. cikkében említett uniós **referencialaboratóriumok**
3. A 2001/83/EK európai parlamenti és tanácsi irányelv 1. cikkének 2. pontjában említett **gyógyszerek kutatásával és fejlesztésével foglalkozó szervezetek**
4. A NACE Rev. 2. C nemzetgazdasági ágának ágazatában említett **gyógyszeralapanyagokat és gyógyszerkészítményeket gyártó szervezetek**
5. Az (EU) 2022/123 európai parlamenti és tanácsi rendelet 22. cikkének értelmében vett népegészségügyi sükséghelyzetben **kritikus fontosságú orvostechnikai eszközöket** (a népegészségügyi sükséghelyzet kritikus fontosságú eszközeinek jegyzéke) **gyártó szervezetek**



LEGFONTOSABB VÁLTOZÁSOK

1. Az Ibtv. kiváltása egy új törvénnyel (új fogalomrendszer)
2. Szélesebb hatósági és incidenskezelési hatáskör
3. A 41/2015. BM. rendelet kiváltása új szabályozókkal
(NIST 800-53, NIST 800-82, felhőszolgáltatások)
3. Összhang megteremtése a Kibertantv.-vel
4. Ágazati CSIRT-ek
5. Kötelező gyakorlatok, stresszteszt, válságkezelési terv,



KÖSZÖNÖM A FIGYELMET!



dr Munkácsi Viktor nb. alezredes
Nemzetbiztonsági Szakszolgálat
Nemzeti Kibervédelmi Intézet
Incidenskezelési Főosztály vezetője
Mobil: +36-30-222-5073
E-mail: viktor.munkacsi@nki.gov.hu
Web: nki.gov.hu