 DOI: 10.53020/IME-2025-KSZ-105

2024 kiemelt egészségügyi kiberbiztonsággal kapcsolatos hírei, eseményei

Major healthcare cybersecurity news and incidents in 2024

Palicz Tamás[1], Schmidt Judit[1,2]
[1]Semmelweis Egyetem Egészségügyi Közszolgálati Kar Egészségügyi Menedzserképző Központ
[2]Semmelweis Egyetem Doktori Iskola Mentális Egészségtudományi Tagozat

2022 áprilisában a Semmelweis Egyetem Egészségügyi Menedzserképző Központ a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézettel és a Magyar Egészségügyi Menedzsment Társasággal közösen elindította az Egészségügyi Kiberbiztonsági Szemle hírlevelet a regisztrált olvasók számára. A szemle az egészségügyi kiberbiztonsági témában megjelent hazai és nemzetközi publikációkat, kutatásokat és cikkeket monitorozza. Az alapítók célja, hogy az intézményvezetők, orvosok, szakdolgozók folyamatos tájékoztatásával rendszeresen hiteles információkkal támogassa az egészségügyi intézmények és az ott tárolt adatok védelmét, kiberbiztonságát. A Digitális Egészségügy különszámban nyomtatva is bemutatjuk a 2024-es év legnagyobb hatású egészségügyi kiberbiztonsági eseményeit.

Kulcsszavak: kiberbiztonság, kibertámadás, zsarolóvírus, adatbiztonság

Keywords: *cybersecurity, cyberattack, ransomware, data privacy*

2024-BEN ELSTARTOLT A NIS2 (NETWORK AND INFORMATION SYSTEMS DIRECTIVE 2)

A NIS2 (Network and Information Systems Directive 2) az Európai Bizottság kiberbiztonsági intézkedéseket és javaslatokat tartalmazó irányelve, amely kiemelten érinti az egészségügyi vállalkozásokat is. Ez a változás az 50 főnél több alkalmazottat foglalkoztató vagy évi 3,9 milliárd forintot meghaladó bevételű vállalkozások számára jelentős. Az Európai Bizottság által kiadott, az egész Unióra kiterjedő kiberbiztonsági irányelv egységes jogi keretet teremt a hálózati és információs rendszerek védelmére. Az egészségügy szempontjából különösen fontosnak számított ez a lépés, mert az ágazatban működő szervezeteknek – különösen a közép- és nagyvállalatoknak – kötelezővé teszi a kiberbiztonsági képességek fejlesztését, a kockázatkezelési intézkedések bevezetését, valamint a rendszeres képzést és incidenskezelést. A jogi környezet változtatásának célja, hogy javítsa az egészségügyi információs rendszerek folyamatos és megbízható működését, megvédje azokat a kibertámadásoktól, és elősegítse a tagállamok közötti együttműködést a kiberfenyegetések elleni védekezésben. A hazai aktualitások érdekében érdemes folyamatosan nyomon követni a Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet (https://nki.gov.hu/) és a Szabályozott Tevékenységek Felügyeleti Hatóságának weboldalát (https://sztfh.hu/) [1,2].

BETEGADATOKAT IS ÉRINTŐ KIBERTÁMADÁSOK TÖRTÉNTEK VILÁGSZERTE

Az egészségügyi rendszereket érintő kibertámadások a világ számos részén, mind Európában, mind az Amerikai Egyesült Államokban jelentős károkat, alkalmanként akár napokig tartó üzemszünetet okoztak. Ezek közül kiemeltük a nagyobb horderejű eseményeket.

Romániában 2024. február 11-én éjjel került sor a számos szolgáltató informatikai rendszerét működtető Hipocrate nevű informatikai rendszer elleni zsarolóvírus-támadásra, amely integrálja és összekapcsolja a kórházak összes orvosi tevékenységét. Az incidens miatt legalább száz kórház került offline állapotba. Ennek hatására a szervereken tárolt fájlok és az adatbázisok titkosítva lettek, így az érintett kórházak számára elérhetetlenné váltak. A támadás közvetlenül 21 kórházat érintett, majd ez a szám végül 25-re emelkedett. Ez az eset amiatt is jelentős, mert hazánkhoz viszonylag közel történt, így felhívta a figyelmet az itthoni egészségügyi intézmények kibervédelmi felkészültségének fontosságára is [3].

A 2024. február 21-ei, az amerikai Change Healthcare hálózatát érintő kibertámadás hosszú távú hatásai az egészségügyi szervezetekre máig (2025 júniusában is) érezhetők. Az Optumhoz tartozó Change Healthcare több mint száz szolgáltatást állított le, és 100 millió felett volt az érintett betegek száma. Az incidenst követően és még napjainkban is folyamatosan dolgoznak a szakemberek a rendszerek helyreállításán [4].

Szintén 2024 februárjában egy hatalmas kiberbiztonsági incidens rázta meg Franciaországot is, amelyben több mint 33 millió ember – a lakosság közel fele – esett áldozatul az ország története legnagyobb kibertámadásának [5].

2025 májusában az Ascension, az egyik legnagyobb amerikai egészségügyi szolgáltató vált feltételezhetően zsarolóvírus-támadás áldozatává, amely megzavarta az egészségügyi intézmények IT-rendszereit, valamint a mentők elterelését is eredményezte, ezzel is befolyásolva a folyamatos betegellátást. A támadás valószínűleg egy szoftveres sebezhetőséget használt ki. Vélhetően a Black Basta elnevezésű zsarolóvírus-csoport állhatott az incidens mögött [6].

A fentiek mellett szinte minden hónapra jutott néhány közelebbi és távolabbi ország egészségügyi rendszerét érintő kibertámadás. Minden egyes eset felhívta a figyelmet az egészségügyi intézmények, különös tekintettel az intézményvezetők felelősségére, feladataira és teendőire, nemcsak az egyes kiberincidensek által okozott károk mielőbbi

felszámolása, hanem az adatvédelmi intézkedések irányítása és a lehetséges megelőzés kapcsán is. Ez utóbbi fontos elemei közé tartozik többek között az egészségügyi intézményekben, intézményrendszerekben használt IT-hardveres és -szoftveres eszközök folyamatos ellenőrzése, karbantartása, frissítése, az egészségügyi és informatikai dolgozók rendszeres oktatása, a veszélyhelyzeti protokollok kialakítása, a külső és belső kommunikációt érintő irányelvek kidolgozása.

OKTÓBERBEN LEZAJLOTT A VI. KIBERBIZTONSÁGI JÁTS(S)ZMA

Az októberi Európai Kiberbiztonsági Hónap nevű kampány részeként 2024-ben 6. alkalommal került megrendezésre a Kiberbiztonsági Játs(s)zMa nevű online vetélkedő, amelyet a Belügyi Tudományos Tanács a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézettel közösen szervezett a Nemzeti Közszolgálati Egyetem, a Semmelweis Egyetem Egészségügyi Közszolgálati Kar Egészségügyi Menedzserképző Központ, valamint az Egészségbiztonsági Nemzeti Laboratórium Adatvezérelt Egészség Divízió szakmai támogatásával. Az egészségügyi köznevelési intézmények tanulói számára 2024. október 21-én került sor a vetélkedőre, amelyen a dobogós csapatok sorrendje így alakult: 1. Pulsusprincessek (PTE Szent-Györgyi Albert Egészségügyi Technikum és Szakképző Iskola), 2. Szurikáták (ME Ferenczi Sándor Egészségügyi Technikum), 3. Medentorok (NVSZC Szent-Györgyi Albert Technikum). 2024. október 25-én az egészségügyi dolgozók (a centrumkórházak és irányított intézmények; az irányító vármegyei intézmények, kórházak; az országos intézetek; a klinikák munkatársai) mérték össze a tudásukat. Az első három helyen végzett csapat a Pszichoteam-1+P (Észak-budai Szent János Centrumkórház), az Interteam (Jász-Nagykun-Szolnok Vármegyei Hetényi Géza Kórház-Rendelőintézet) és a Path-Ászok (Országos Onkológiai Intézet, Daganatpatológiai Központ) lett [7].

BUDAPEST LÁTTA VENDÉGÜL A 9TH ENISA EHEALTH SECURITY CONFERENCE RÉSZTVEVŐIT

2024. november 6-án rendezte meg a European Union Agency for Cybersecurity (ENISA) a Semmelweis Egyetem Egészségügyi Menedzserképző Központtal (SE EMK) és a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézettel (NKI) együttműködésben a 9. eHealth Security konferenciát a Semmelweis Egyetem Nagyvárad téri Elméleti Tömbjének dísztermében. Az egész napos, sikeresen és jó hangulatban lezajlott rendezvénynek idén először adott otthont Budapest, amely egyedülálló lehetőséget biztosított az érdekelt felek közössége számára, hogy feltárják a szakterület legújabb fejleményeit, a kihívásokat és a továbblépési lehetőségeket. Dr. Palicz Tamás a szervezőbizottság vezetőjeként szerepet vállalt a konferencia létrejöttében, valamint Challenges and opportunities with NIS2 implementation címmel készített prezentációjával előadóként, illetve a 3. szekció moderátoraként is részt vett a nemzetközi közönség előtt zajló, tartalmas szakmai párbeszédekben gazdag eseményen. Előadásában a NIS2 szabályozás emberi oldalait és az új szabályozás bevezetését övező, az egészségügyi szervezetek működését is jelentős mértékben érintő változásokkal kapcsolatos kihívásokat és az ezekben rejlő lehetőségeket részletezte [8].

IRODALMI HIVATKOZÁSOK

[1] 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). URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/hun

[2] Országgyűlés Információs Szolgálat: Kiberbiztonság az EU-ban és Magyarországon (infojegyzet 2024/28, 2024. október 31.). URL: https://www.parlament.hu/documents/d/guest/infojegyzet_2024_28_kiberbiztonsag

[3] Davey Winder. Ransomware Attack Takes 100 Hospitals Offline. URL: https://www.forbes.com/sites/daveywinder/2024/02/13/ransomware-attack-takes-100-hospitals-offline

[4] Jill McKeon: Healthcare Faces Uncertainty Amid Change Healthcare Cyberattack. URL: https://www.techtarget.com/healthtechsecurity/feature/Healthcare-Faces-Uncertainty-Amid-Change-Healthcare-Cyberattack?ut

[5] Over half of French citizens had their personal data stolen as France reels from massive cyberattack. URL: https://www.firstpost.com/tech/over-half-of-french-citizens-had-their-personal-data-stolen-as-france-reels-from-massive-cyberattack-13707912.html

[6] Sergiu Gatlan Ascension redirects ambulances after suspected ransomware attack. URL: https://www.bleepingcomputer.com/news/security/healthcare-giant-ascension-redirects-ambulances-after-suspected-Black-Basta-ransomware-attack.

[7] Semmelweis Egyetem Egészségügyi Menedzserképző Központ: A Kiberbiztonsági Játs(s)zma VI. eredményei. URL: https://semmelweis.hu/emk/2024/10/28/a-kiberbiztonsagi-jatsszma-vi-eredmenyei/

[8] Semmelweis Egyetem Egészségügyi Menedzserképző Központ: Budapesten megrendezett 9th ENISA eHealth Security Conference zárta az októberi európai kiberbiztonsági hónapot. URL: https://semmelweis.hu/emk/2024/11/08/9th-enisa-ehealth-security-conference-budapest/

A SZERZŐK BEMUTATÁSA

Palicz Tamás 1993-ban szerezte orvosdoktori diplomáját a Debreceni Egyetemen, majd 1998-ban belgyógyász szakorvos lett. 2003-tól dolgozik vezetőként, kezdetben a Semmelweis Egyetem Stratégiai és Működésfejlesztési Főigazgatóság főigazgató-helyetteseként, majd 2005-től a Kútvölgyi Klinikai Tömb orvosigazgatójaként szerzett tapasztalatot az egészségügyi szervezetek vezetésében. 2010 és 2013 között a Nemzeti Fejlesztési Ügynökség Humánerőforrás-programok Irányító Hatóságát (HEP IH) irányította. 2015 végétől a Semmelweis Egyetem Egészségügyi Menedzserképző Központ stratégiai igazgatóhelyettese, egészségügyi kiberbiztonsági szakértő.

Schmidt Judit 2005-ben dietetikusi, 2009-ben egészségügyi szaktanári diplomát szerzett a Semmelweis Egyetemen. 2024 óta a Semmelweis Egyetem Egészségügyi Menedzserképző Központ kommunikációs munkatársa, emellett aktív szerepet vállal betegedukációs programokban, szakmai közösségekben. 2025-től a Semmelweis Egyetem Doktori Iskola doktoranduszhallgatója.