2025 kiemelt egészségügyi kiberbiztonsággal kapcsolatos hírei, eseményei

Major healthcare cybersecurity news and incidents in 2025

Palicz Tamás[1], Schmidt Judit[2,3]
[1]Semmelweis Egyetem Egészségügyi Közszolgálati Kar Digitális Egészségtudományi Intézet
[2]Semmelweis Egyetem Egészségügyi Közszolgálati Kar Egészségügyi Menedzserképző Központ
[3]Semmelweis Egyetem Doktori Iskola Mentális Egészségtudományi Tagozat

2022 áprilisában a Semmelweis Egyetem Egészségügyi Közszolgálati Kar Egészségügyi Menedzserképző Központja a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézettel (újabb nevén Nemzeti Kiberbiztonsági Intézettel) és a Magyar Egészségügyi Menedzsment Társasággal közösen elindította az Egészségügyi Kiberbiztonsági Szemle hírlevelet. 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 2024-ben megjelent összefoglalót követően a Digitális Egészségügy különszámban nyomtatva is bemutatjuk a 2025-ös év kiemelt egészségügyi kiberbiztonsági eseményeit is [1].

Kulcsszavak: kiberbiztonság, kibertámadás, zsarolóvírus, adatbiztonság

Keywords: cybersecurity, cyberattack, ransomware, data privacy

ZSAROLÓVÍRUS-TÁMADÁS A MARYLANDI EGÉSZSÉGÜGYI HÁLÓZAT ELLEN

2025 januárjában zsarolóvírus-támadás érte a marylandi Frederick Health Medical Groupot. A kiterjedt egészségügyi hálózatban emiatt a hatóságoknak le kellett állítaniuk az informatikai rendszereket, és le kellett mondaniuk több időpontot. Az intézmény figyelmeztette a betegeket, hogy a szolgáltatásban késések lesznek, mivel kibertámadással kell megküzdeniük. Szorosan együttműködtek a külső kiberbiztonsági szakértőikkel, hogy a lehető leggyorsabban és legbiztonságosabban, valamint a betegellátást előtérbe helyezve újra működőképessé tegyék a rendszereiket. Létesítményeik nyitva maradtak, és továbbra is biztosították a betegek ellátását a bevált biztonsági mentési folyamatok és egyéb, üzemszünetre érvényes eljárásmódok segítségével [2].

ADATSZIVÁRGÁS TÖRTÉNT AZ ORACLE HEALTH RENDSZERÉBEN

2025 márciusában látott napvilágot az egészségügyi szoftvereket kínáló Oracle Health-t (korábban Cernert) ért kibertámadás híre. Az incidensben több amerikai kórház és egészségügyi intézmény volt érintett. A kibertámadás elkövetője ellopta a rendszerben tárolt páciensadatokat a szerverekről, feltehetően az elektronikus egészségügyi nyilvántartásokból. A támadó feltört ügyfél-hozzáférési adatokat használt fel ahhoz, hogy 2025. január 22. után behatoljon a szerverekre, majd az adatokat egy távoli szerverre másolja. Ezt követően milliókat követelt kriptovalutában, hogy ne hozza nyilvánosságra vagy adja el az adatokat. Sőt, nyomásgyakorlásként nyilvános weboldalakat is létrehozott a támadásról [3].

ZSAROLÓVÍRUS-TÁMADÁS ÉRTE A DAVITA VESEDIALÍZIS-SZOLGÁLTATÓT

2025. április 14-én a denveri székhelyű DaVita bejelentette, hogy két nappal korábban kibertámadás áldozata lett. A vállalat azonnal aktiválta a vészhelyzeti protokollokat, elszigetelte az érintett rendszereket, és külső kiberbiztonsági szakértők bevonásával kezdett el dolgozni az incidens felmérésén és elhárításán. Az ügyet a hatóságoknak is jelentették. Ez nem az első ilyen incidens az iparágban: 2023-ban a DaVita versenytársának, a Fresenius Medical Care amerikai egységének rendszerét is feltörték, akkor félmillió beteg egészségügyi adatai kerültek illetéktelen kezekbe [4].

A KILLSEC ZSAROLÓVÍRUS TÁMADÁSAI VESZÉLYEZTETTÉK AZ EGÉSZSÉGÜGYI ÁGAZAT INFORMATIKAI RENDSZEREIT

A KillSec nevű zsarolóvírus egyre komolyabb fenyegetést jelentett az elmúlt évben az egészségügyi IT-rendszerekre Latin-Amerikában – többek közt Brazíliában –, kihasználva a felhőalapú tárolók hibás beállításait, a webalkalmazások sebezhetőségeit, valamint az adminisztratív távoli eléréseket. A támadók a megszerzett adatok kiszivárogtatásával fenyegetőztek. Több egészségügyi intézmény is komoly adatvesztést szenvedett el, beleértve az érzékeny betegadatokat [5].

A KIBERTÁMADÁSOK MIATT AZ EGÉSZSÉGÜGYI SZERVEZETEK TÖBBSÉGE ÉSZLELT ZAVAROKAT A BETEGELLÁTÁSBAN

Az amerikai egészségügyi informatikai és kiberbiztonsági szakemberek körében végzett felmérés, a 2025 Ponemon

Healthcare Cybersecurity Report szerint a megkérdezett szervezetek 93%-a tapasztalt legalább egy kibertámadást az elmúlt 12 hónapban, és 72%-uk jelentette, hogy a támadások zavart okoztak a betegellátásban. A negatív hatások általában a késedelmes felvételnél, a meghosszabbodott kórházi tartózkodásnál és az orvosi beavatkozásokból eredő szövődmények növekedésénél voltak érzékelhetőek. A válaszadók 29%-a pedig a halálozási arány növekedéséről számolt be. A probléma egyre súlyosabb, mivel 2025-ben az egészségügyi szervezetek 69%-a jelentette, hogy a kibertámadások negatívan érintették a betegellátást [6].

ÜNNEPNAPOKON ÉS HÉTVÉGÉKEN GYAKORIBBAK AZ EGÉSZSÉGÜGYET ÉRINTŐ KIBERTÁMADÁSOK

A Semperis által a 2025 Ransomware Holiday Risk Report című jelentésben közölt adatok szerint a globális zsarolóvírus-támadások többsége hétvégéken és ünnepnapokon történik, amikor a kiberbiztonsági személyzet gyakran kisebb létszámban dolgozik. Az egészségügyben különösen jelentős ez a jelenség: az esetek 47%-a hétvégére vagy ünnepnapra esett, ami rámutat a fokozott éberség szükségességére [7].

OKTÓBERBEN ZAJLOTT LE A VII. KIBERBIZTONSÁGI JÁTS(S)ZMA

Az Európai Kiberbiztonsági Hónap kampány részeként 2025 októberében 7. alkalommal került megrendezésre a Kiberbiztonsági Játs(s)zMa nevű online vetélkedő a Belügyi Tudományos Tanács és a Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet (NKI) szervezésében, a Magyar Egészségügyi Menedzsment Társaság (MEMT) szakmai támogatásával. 2025. október 20-án az egészségügyi köznevelési intézményekben tanulók vetélkedőjén az alábbi sorrend született: 1. Nógrád Vármegyei Szakképzési Centrum Szent-Györgyi Albert Technikum (Balassagyarmat) – DOPANIN, 2. Miskolci Egyetem Ferenczi Sándor Egészségügyi Technikum – Malackák, 3. Pécsi Tudományegyetem Szent-Györgyi Albert Egészségügyi Technikum és Szakképző Iskola – SZBB. 2025. október 29-én került sor az egészségügyi dolgozók vetélkedőjére, ahol a következő eredmények születtek: 1. Tolna Vármegyei Balassa János Kórház – BalassaLegal, 2. helyezett: Ajkai Magyar Imre Kórház – AMIKÁK, 3. Észak-budai Szent János Centrumkórház – Kiberpajzs Alakulat [8].

EGÉSZSÉGÜGYI INCIDENSEK A 2025-ÖS ÉVBEN A NEMZETBIZTONSÁGI SZAKSZOLGÁLAT NEMZETI KIBERBIZTONSÁGI INTÉZET ADATAI ALAPJÁN

A 2025-ös év eseményei világosan jelzik, hogy a magyar egészségügyi intézmények sem mentesek a kibertámadásoktól. Az előfordult incidensek alapján a fenyegetések spektruma széles: a zsarolóvírus-támadásoktól az adathalászaton és weboldal-kompromittáláson át egészen a jogosulatlan hozzáférésekig és belső információbiztonsági hibákig terjed.

Az év elején egy kórház és rendelőintézet ellen végrehajtott zsarolóvírus-támadás több munkaállomást és virtuális szervert érintett. Bár a helyreállítás a biztonsági mentésekből megkezdődött, a vizsgálat feltárta, hogy jelszóval nem védett, rendszergazdai jogosultságú fiók is jelen volt a rendszerben – ez a klasszikus, de továbbra is gyakori sérülékenységek közé tartozik. Az eset rávilágít az alapvető hozzáférés-kezelési hiányosságok kockázatára.

Több magyar egészségügyi intézmény számolt be adathalász e-mailekről és CEO-fraud típusú próbálkozásokról (olyan csalási módszer, amikor a támadók a vezetőnek – például az igazgatónak vagy főorvosnak – adják ki magukat, és sürgős pénzügyi vagy adatátadási kéréseket küldenek), amelyek célja jellemzően hitelesítési adatok megszerzése vagy pénzügyi manipuláció. Egy másik esetben brute force támadás (olyan módszer, amikor a támadók nagyszámú jelszókombinációt próbálnak ki egymás után a hozzáférés megszerzéséhez) következtében több tízezer fiók zárolása történt egy levelezőrendszerben, ami jól mutatja az automatizált támadások volumenét, még akkor is, ha azokat gyorsan sikerült kezelni.

A weboldal-defacement (amikor a támadók illetéktelenül módosítják vagy megrongálják egy szervezet weboldalának tartalmát, gyakran saját üzenetet vagy képet helyezve el rajta) és az adatbázistörléses behatolás azt jelzi, hogy nemcsak az adatok, hanem az intézményi reputáció és a szolgáltatások folytonossága is célponttá válhat. Emellett OSINT-alapú (nyilvánosan elérhető online forrásokra és adatokra támaszkodó) vizsgálatok több egészségügyi intézményhez köthető kiszivárgott felhasználónév-jelszó párost azonosítottak, ami rendszerszintű jelszókezelési problémákra utal.

Különösen tanulságos az az incidens, amely nem külső támadásból, hanem belső hibából fakadt: egy teljes orvosi állománynak kiküldött, hozzáférési adatokat tartalmazó táblázat komoly információbiztonsági kockázatot jelentett. Ez rámutat arra, hogy a technológiai védelem mellett a szervezeti folyamatok és a biztonságtudatosság fejlesztése is kulcskérdés. Fontos kiemelni, hogy az ilyen jellegű információbiztonsági incidenseket is jelenteni kell a Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet részére.

Az összkép egyértelmű: a magyar egészségügyi szektor 2025-ben is folyamatos és sokrétű kiberfenyegetettséggel szembesült. Az esetek többségében a helyreállítás megtörtént, és a szolgáltatáskiesés korlátozott maradt, de az incidensek azt bizonyítják, hogy Magyarország sem érinthetetlen. Az egészségügyi intézmények digitális infrastruktúrája – a betegadatok, a klinikai rendszerek és az adminisztratív folyamatok miatt – kiemelt célpontot jelent. A megelőzés, a jogosultságkezelés szigorítása, a rendszeres mentések, valamint a dolgozók biztonságtudatosságának erősítése jelentik a legfontosabb beavatkozási területeket.

Örömmel tájékoztatjuk olvasóinkat, hogy a 2026-os évtől a Kiberszemléhez új szakmai partnerként csatlakozik a Semmelweis Egyetem Egészségügyi Közszolgálati Karának Digitális Egészségtudományi Intézete, erősítve ezzel a tartalmak szakmai megalapozottságát és digitális egészségügyi fókuszát.

Értesüljön Ön is az egészségügyi kiberbiztonság témában megjelent hírekről, publikációkról! Iratkozzon fel az Egészségügyi Kiberbiztonsági Szemlére!

IRODALMI HIVATKOZÁSOK

[1] Palicz Tamás, Schmidt Judit: 2024 kiemelt egészségügyi kiberbiztonsággal kapcsolatos hírei, eseményei. IME Innováció Menedzsment Egészségügy, 2025, 24(KSZ 1), 32-34. https://doi.org/10.53020/IME-2025-KSZ-105

[2] Jonathan Greig: Maryland healthcare network forced to shut down IT systems after ransomware attack. URL: https://therecord.media/maryland-healthcare-ransomware-frederick-health

[3] Lawrence Abrams: Oracle Health breach compromises patient data at US hospitals. URL: https://www.bleepingcomputer.com/news/security/oracle-health-breach-compromises-patient-data-at-us-hospitals

[4] Pietje Kobus: Kidney Dialysis Provider DaVita Hit by Ransomware Attack. URL: https://www.hcinnovationgroup.com/cybersecurity/data-breaches/news/55282892/kidney-dialysis-provider-davita-hit-by-ransomware-attack

[5] Tushar Subhra Dutta: KillSec Ransomware Attacking Healthcare Industry IT Systems. URL: https://cybersecuritynews.com/killsec-ransomware-attacking

[6] Steve Alder: 72% of Healthcare Orgs Report Disruption to Patient Care Due to Cyberattacks. URL: https://www.hipaajournal.com/healthcare-cyberattacks-disrupt-patient-care

[7] Jill Hughes: Report: Healthcare cyberattacks surge on holidays, weekends. URL: https://www.techtarget.com/healthtechsecurity/news/366634663/Report-Healthcare-cyberattacks-surge-on-holidays-weekends

[8] Magyar Egészségügyi Menedzsment Társaság: Lezárult az idei VII. Kiberbiztonsági Játs(s)zMa vetélkedő. https://memt.hu/lezarult-az-idei-vii-kiberbiztonsagi-jatsszma-vetelkedo

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, 2025 decemberétől pedig a Semmelweis Egyetem Egészségügyi Közszolgálati Kar Digitális Egészségtudományi Intézet igazgatója.

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.