DOI: 10.53020/IME-2025-KSZ-102

Az egészségügyi dolgozók kiberbiztonsági ismereteinek javítása a betegbiztonság javítása érdekében

Improving the Cyber Security Knowledge of Healthcare Workers to Improve Patient Safety

Vida Zoltán[1] ✉, Lám Judit[2,3]

[1]Budavári Önkormányzat Egészségügyi Szolgálata Szakorvosi Rendelőintézet

[2]Semmelweis Egyetem Egészségügyi Közszolgálati Kar Egészségügyi Menedzserképző Központ

[3]NEVES Egyesület a Betegbiztonságért

✉ orvosigazgato@marosrendelo.hu

Bevezetés: A digitalizáció korunk egyik leggyorsabb változásokat eredményező jelensége. A változások a szervezeti működésre veszélyes tényezők folyamatos átalakulását, megszűnését, újak keletkezését okozzák, emiatt a szervezetbiztonság fontos eszköze a dinamikus kockázatmenedzsment. A kiberbiztonság a szervezetbiztonság része, az egészségügyi szektorban szorosan kapcsolódik a betegbiztonsághoz.

Célkitűzés: A közlemény célja e rendkívül fontos és aktuális téma hazai és nemzetközi szakirodalmának bemutatása, levonható következtetések megállapítása és ismertetése, a szakirodalomra támaszkodva gyakorlatban is hasznosítható javaslatok megfogalmazása.

Módszer: Szakirodalmi kutatás történt hazai és nemzetközi közleményekben, rögzített keresőszavas kereséssel, gyűjtősablonnal, rögzített kritériumok alkalmazásával végzett tartalmi értékeléssel.

Eredmények: A bevont források száma 27 volt. A hazai jogi szabályozási és stratégiai dokumentumok bemutatását követően a közlemény az Európai Uniós szabályozókat tárgyalja. Az általános kiberbiztonság tárgyalása után a szervezeti szempontokat ismerteti, tárgyalja a kibertudatosság mérési lehetőségeit munkahelyi környezetben bemutató szakirodalmat. Az egészségügyi szektor területén az intézményeket, adatbázisokat érő támadásokat elemző szakirodalom bemutatását követően az egészségügyi eszközök kiberfenyegetésének problémája, végül a kibertudatossági attitűdvizsgálatok témája kerül tárgyalásra.

Megbeszélés: Megállapítható a teljes társadalmi kibertudatosság alacsony szintje és ebből adódóan a szervezetek munkavállalóinak hiányosságai. A problémák felmérésére alkalmas módszertan a szakirodalomban fellelhető, célzott oktatási anyagok összeállítása és alkalmazása lehetséges. Az attitűdvizsgálatok bevezetése és az eredmények felhasználása megkönnyíti a magatartásváltozás elérését, a kibertudatosság javulását.

Következtetés: Az egészségügy kiemelten veszélyeztetett helyzete indokolja a hiányosságok felmérését, oktatások bevezetését, vészhelyzeti tervek megalkotását és rendszeres tréningek végzését.

Kulcsszavak: hozzáállás, viselkedés, kiberbiztonság, betegbiztonság

Introduction: Digitalization is one of the fastest changing phenomena of our time. The changes cause the continuous transformation and elimination of dangerous risk factors to organizational functioning, and the creation of new ones, which is why dynamic risk management is an important tool for organizational security. Cyber security is part of organizational security, and in the healthcare sector it is closely related to patient security.

Objective: The purpose of the publication is to present the domestic and international literature on this extremely important and current topic, to establish and explain the conclusions that can be drawn, and to formulate proposals that can be used in practice based on the literature.

Method: Literature research was conducted in domestic and international publications with a fixed keyword search, a collection template, and a content evaluation using fixed criteria.

Results: The number of included documents was twenty-seven. After presenting the domestic legal regulatory and strategic documents, the publication discusses the European Union regulators. After the discussion of general cyber security topics, the publication describes the organizational aspects and discusses in detail the literature presenting the measurement possibilities of cyber awareness in the workplace. After the presentation of the literature analysing attacks on institutions and databases in the field of the healthcare sector, the problem of cyber threats to healthcare devices and finally the topic of cyber awareness attitude surveys is discussed.

Discussion: The low level of overall social cyber awareness and, consequently, the deficiencies of the employees of the organizations can be established. A suitable methodology for assessing the problems can be found in the literature, and it is possible to compile and apply targeted educational materials. The introduction of attitude surveys and the use of the results make it easier to achieve behavioural change and to improve cyber awareness.

Conclusion: The extremely vulnerable situation of the healthcare sector justifies the assessment of cyber

security deficiencies, the introduction of education, the creation of emergency plans and the conduct of regular trainings.

Keywords*: attitude, behaviour, cyber security, patient safety*

BEVEZETÉS

Minden szervezet alapvető érdeke és törekvése működőképességének, stabilitásának megőrzése, a veszélyekkel szembeni megelőző és megküzdő tevékenységekkel a szervezet biztonságának kialakítása és folyamatos fenntartása. A digitalizáció korunk egyik leggyorsabb változásokat eredményező jelensége, ami a szervezeti működésre ható tényezők átalakulását, megszűnését, újak keletkezését okozza. Az elektronikus adatok és információk bizalmasságának, sértetlenségének, rendelkezésre állásának és folytonos védelmének biztosítása új és egyre növekvő feladat a szervezetek számára. Ha ezeket a változásokat a kockázatmenedzsment tevékenység nem követi dinamikusan, a szervezet kiberbiztonsága csökken. A kiberbiztonság két nagy terület felől közelíthető meg. Az egyik technológiai, professzionális jellegű, a szükséges technikai feltételek, eszközök, rendszerek biztosítása, üzemeltetése, informatikai, adatvédelmi, információbiztonsági szakértők alkalmazása. A másik kiberbiztonsági átgondolást érdemlő terület a lényegesen jelentősebb létszámú csoport, az ágazatra jellemző képzettségű, az ágazat alapfolyamataiban tevékenykedő szakemberek kiberbiztonsági tudása, ismerete, készségei, attitűdje. Az ismerethiány és gyakorlatlanság miatt az ő viselkedésük, hozzáállásuk a digitális munkavégzési térben gyakran a leggyengébb láncszemet jelenti a kiberbiztonság szempontjából. A helyzetet rontja, hogy a szolgáltatásokat igénybe vevőkkel vagy igénybevételt álcaként használó rosszindulatú támadókkal ők kerülnek elsődlegesen és nagy gyakorisággal kapcsolatba. Ennek következtében a szervezet kiberbiztonsági eredményessége e munkatársak ismeretein, éberségén, reagálásán vagy hanyagságán múlik [1].

A kiberbiztonsági problémák az egészségügyi szektorban határozottan megjelennek. A technológiák modernizációja, a digitalizációs fejlesztések üteme és ezzel összefüggésben az új veszélyforrások megjelenése is rohamos üteműnek mondható. A szervezeti kultúra jellemzői közül kiemelendő, hogy az egészségügyi ágazatban magas színvonalú szakmai képzettséggel, hivatástudattal rendelkező, szakmailag elkötelezett munkatársak végzik tevékenységüket, akik képzése csak korlátozottan terjed ki a kapcsolódó, támogató tudományterületekre (itt említhető például a jog, kommunikáció, informatika – kiberbiztonság). Ennek következménye, hogy a munkatársak segítő hivatáshoz kötődő, szakmai értékeket előtérbe helyező attitűdje és alapképzettségük hiányosságai miatt kibertudatosságuk alacsony [2]. A kiberbiztonsági fenyegetettség az egészségügyi ágazatban szolgáltató szervezetek esetében – a tevékenységből eredően – legtöbbször nem technológiai, informatikai kérdésként, hanem betegbiztonsági problémaként jelenik meg [3]. A kiberbűnözés közvetlen és erőteljes, gyakran végzetes hatást gyakorolhat az egészségügyi intézmények működésére, akár folyamatok blokkolása, akár egészségügyi adatok törlése, módosítása vagy hozzáférésének gátlása formájában. Egy kibertámadás az egészségügyben legtöbbször betegbiztonsági problémát okoz, az ellátás eredményességét befolyásolja, veszélyeztetéshez, károsodáshoz vezethet [4].

Fentiekre tekintettel, a kiberbiztonsági gondolkodás speciális ágazati-szakmai területére koncentrálva, a digitális érettség felmérése, attitűdvizsgálatok végzése, a szervezeti kultúra ilyen szempontú vizsgálata mindenképpen fontos információkat szolgáltat a szervezet egészére jellemző kiberbiztonsági szintről. A felmérés eredményeire alapozva lehetséges és szükséges a hiányosságok ismeretében fejlesztett tananyaggal végzett célzott és hatásos oktatás, illetve a betegbiztonságot támogató szervezeti kultúra kibertudatossági elemeire vonatkozó fejlesztés, képzés. Csak a kiberbiztonság folyamatos, a digitalizációs fejlesztéseket arányosan követő és időben párhuzamosan végzett fejlesztése védheti meg az egészségügyi intézményeket új és korábban nem ismert mértékű betegbiztonsági problémáktól [1].

CÉLKITŰZÉS

Jelen közlemény célja e rendkívül aktuális téma legfontosabb hazai és nemzetközi szakirodalmának bemutatása, levonható következtetések megállapítása és ismertetése, a szakirodalomra támaszkodva gyakorlatban is hasznosítható javaslatok megfogalmazása. A távlati cél az egészségügyi intézményekben a kiberbiztonság és kibertudatosság javításának támogatása.

MÓDSZEREK

Irodalomkutatás történt több tudományos adatbázisban (köztük: PubMed, ScienceDirect) 2017 és 2024 között megjelent hazai és nemzetközi közlemények keresésével. A keresés rögzített keresőszavak (attitudes, behaviours, digitalisation, cyber-awareness, cyber-hygiene, cybersecurity, patient safety) segítségével zajlott. A kutatási szempontból megfelelőnek ítélt cikkek irodalomjegyzékeinek feldolgozása további releváns közlemények besorolását eredményezte a találatok közé. A cikkek tartalmának rögzítésére a kutatáshoz készített gyűjtősablon szolgált. Rögzített kritériumok alkalmazásával történt a közlemények tartalmi értékelése. A beválogatási tartalmi kritériumok a digitalizáció, kiberbiztonsági tudatosság, betegbiztonsági szempontok tárgyalása volt.

EREDMÉNYEK

Nyers eredmények

A beválogatott szakmai források (szerző nélküli szakmai anyagok, publikációk, jogszabályok, módszertani levelek, ajánlások, stratégiai dokumentumok, könyvfejezetek) száma 27 volt.

Kiberbiztonság – kibertudatosság hazai szabályozási, stratégiai szempontjai

A digitalizáció és kiberbiztonság társadalmi szintű fontosságát mutatja, hogy országos és ágazati szinten is születtek stratégiai dokumentumok és jogi szabályozók, továbbá támogató és ellenőrző szervezetek és intézmények működnek, a szabályozási környezet rendezett. A digitalizáció és kiberbiztonság vonatkozásában említendő a 2013-as Nemzeti Kiberbiztonsági Stratégia [5] és a Nemzeti Infokommunikációs Stratégia 2014–2020 [6]. A kibervédelem hazai központi szerve a Nemzetbiztonsági Szakszolgálat szervezetén belül 2015. október 1-jével alapított Nemzeti Kibervédelmi Intézet [7]. Feladatai: eseménykezelési feladatok és hatósági felügyelet gyakorlása a létfontosságú információs rendszerek és rendszerelemek, valamint meghatározott elektronikus kereskedelmi szolgáltatók (online piactér, internetes keresőszolgáltatás, felhőszolgáltatás) esetében. Az Egészséges Magyarország Egészségügyi Ágazati Stratégia 2021-2027 kiadás [8] külön fejezetet szán a digitális egészségügy témájának. A Nemzeti Digitalizációs Stratégia 2021–2030 dokumentumban [9] – a digitális infrastruktúra fejlesztés fejezetben – az e-egészségügyi szolgáltatások kínálatának és igénybevételének növelése a célkitűzések között szerepel.

A kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény [10] hozta létre a Kiberbiztonsági Felügyeletet a Szabályozott Tevékenységek Felügyeleti Hatóságán belül. Feladatai hatósági nyilvántartás, ellenőrzés, auditálás a digitalizáció fejlődése szempontjából nélkülözhetetlen és kockázatosnak minősített tevékenységű vállalatok, szervezetek esetében. A hatósági nyilvántartásba vételt követően a szervezeteknek információs rendszereiket biztonsági osztályokba kell sorolniuk (egységes szabályozás szerinti kategóriákban: alap / jelentős / magas), a besorolt biztonsági osztálynak megfelelő védelmi intézkedéseket 2024. október 18-tól alkalmazniuk kell, és 2025. december 31-ig sort kell keríteni az első kiberbiztonsági auditra. A besorolás szempontjait és a konkrét védelmi intézkedéseket a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendelet rögzíti [11].

Kiberbiztonság – kibertudatosság Európai Uniós szabályozási, stratégiai szempontjai

Az Európai Unió hálózat- és információbiztonsággal (Network and Information Security = NIS) kapcsolatos szakpolitikája több mint két évtizedes múltra tekint vissza. Az Európai Hálózat- és Információbiztonsági Ügynökséget (ENISA) 2004-ben hozták létre. Az Európai Unió 2013-as Kiberbiztonsági Stratégiája [12] célja az alcímben megfogalmazott „nyílt, megbízható és biztonságos kibertér". A stratégiai prioritások közül kiemelhető a kibertámadásokkal szembeni ellenállóképesség elérése, a számítástechnikai bűnözés drasztikus csökkentése, a kibervédelmi politika és képességek, illetve a kiberbiztonsági ipari és technológiai erőforrások fejlesztése, továbbá összefüggő nemzetközi szakpolitika létrehozása a kibertér vonatkozásában az Európai Unió számára. 2016. július 6-án jelent meg az Európai Parlament és a Tanács (EU) 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről (NIS) [13]. Az irányelv célja olyan intézkedések megállapítása, melyek a hálózati és információs rendszerek magas szintű biztonságát az Európai Unión belül egységesen biztosítják. A 2022/2555 (EU) irányelv (NIS2) – 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 [14] a NIS rendelet továbbfejlesztéseként jelent meg. A NIS2 irányelv bővíti az érintett és biztonsági intézkedésre kötelezett szervezetek körét, szigorítja az incidensjelentési kötelezettségeket, erősíti a kockázatkezelési és a kockázatokkal arányos kiberbiztonsági intézkedésekre vonatkozó elvárásokat.

Kiberbiztonság – kibertudatosság a társadalomban

Széles fókuszú megközelítésben érdemes a digitalizáció hatásait és a kibertudatosságot elsőként társadalmi szinten vizsgálni.

Gyaraki szerint a kiberveszélyekkel szembeni biztonságtudatosság jelenleg még csak kialakulóban van, és különösen az otthoni eszközhasználat veszélyeztetett. Véleménye szerint a hétköznapi digitális életvitelben a kényelmi szolgáltatást nyújtó alkalmazások (bank, e-ügyintézés) és a közösségi oldalak biztonsági hiányosságai jelentenek nagy veszélyt. Gyakori probléma a jelszókezelés elégtelen biztonsága. Kiemeli a humán kockázatok szerepét a kibertérben, a felhasználók hanyagságát, kihasználhatóságát, naivitását [15].

Krasznay az okoseszközök elterjedését és ennek hatásait vizsgálja a társadalomban, a hétköznapi élet vonatkozásában. Álláspontja szerint az életvitel jelentős átalakulása zajlik a hordható mobileszközök és az otthoni környezetben megjelenő technológiák miatt. Tárgyalja a társadalomban élő generációk digitális készségeinek és attitűdjének jellemzőit is [16].

Kiberbiztonság – kibertudatosság a szervezetekben

A társadalomban megfigyelhető digitális technológiai átalakulások a szervezetekben is jelentős hatást gyakorolnak a munkafolyamatokra, és számos biztonsági kérdést vetnek fel.

Hadlington tanulmánya a kiberbiztonsággal kapcsolatos attitűdök, az impulzivitás, az internetfüggőség hatásait, kapcsolatát tárta fel a kockázatos kiberbiztonsági magatartásokra vonatkozóan. Az eredmények azt mutatták, hogy azok az egyének, akik elutasítóak vagy nem ismerik a rossz kiberbiztonságból eredő veszélyeket, nagyobb valószínűséggel vállalnak kockázatos kiberbiztonsági magatartást. A helyes kiberbiztonsági attitűd kialakítása emiatt minden szervezet számára kiemelten fontos. Az impulzivitás és kockázatos kiberbiztonsági magatartások összefüggése tekintetében megállapítható volt, hogy a magas impulzivitással rendelkező munkatársak gyakran gondolkodás, megfontolás nélkül cse-

lekszenek, kevés figyelmet fordítanak tetteik lehetséges következményeire, emiatt az impulzivitásban mérhető magas pontszám pozitív előrejelzője a kockázatos kiberbiztonsági magatartásformáknak. Az internetfüggőség és kockázatos kiberbiztonsági magatartások vizsgálata vonatkozásában a kutatás kimutatta, hogy az egyének problémás vagy függőséget okozó szintű internethasználata korrelációt mutat a kockázatos kiberbiztonsági magatartással. A tanulmány felhívta a figyelmet az egyéni attitűdbeli különbségek feltárásának fontosságára a kockázatok felmérése és a hatékonyabb, személyre szabottabb képzési és figyelemfelkeltő módszerek alkalmazhatósága érdekében [1].

Alkalmazottak kibertudatosságát vizsgálta a Center for Generational Kinetics (CGK) kutatóintézet magas kiberfenyegetettségű ágazatokban. A vizsgálat megállapította, hogy az alkalmazottak 41%-a szerint a biztonsági irányelvek akadályozzák és megnehezítik a munkavégzésüket, 36 %-uk pedig elismerte, hogy képes e biztonsági szabályok megkerülésére. A válaszadók 64%-a használt saját, személyes eszközt munkavégzéshez, de ezeknek az eszközöknek csak 43%-a volt biztonságos és védett. A kutatás a jelszóhasználat terén jelentős kockázatokat tárt fel. Az alkalmazottak rutinszerűen használtak nem engedélyezett alkalmazásokat érzékeny adatokkal végzett munkahelyi tevékenységekhez [17].

Kiberbiztonság – kibertudatosság az egészségügyben

Az egészségügyi ágazatban a kiberbiztonság speciális kérdéseket és problémákat vet fel. A létfontosságú infrastruktúra, a megszakítás nélküli működőképesség szükségessége és a magas fokú digitalizáltság különösen veszélyeztetett ágazattá teszi az egészségügyet. Míg korábban a kórházi adatbázisok megkímélt területnek számítottak a hackerek szemszögéből, az utóbb évek tapasztalatai a „kegyelmi időszak" elmúlására utalnak.

A veszélyeztetettség komolyságára utal, hogy 2021 decemberében egy kanadai egészségügyi ellátóintézményt egyszerre két hackercsoport támadott meg sikeresen egy nem frissített szerverösszetevőn keresztül. Több lépcsőben törtek be az intézményi hálózatba, és szenzitív egészségügyi adatokhoz fértek hozzá [18].

A Vermonti Egyetem (USA) Klinikai Központja kibertámadás utáni működési zavara részlegenként változó ideig, de legalább 25 napig tartott, a teljes helyreállítás csak 40 nap után sikerült. A működési kiesés számos intézményi informatikai rendszert érintett, az átmeneti időszakban már évek-évtizedek óta nem használt manuális és offline módszerekkel kellett az információk áramlását, a dokumentumok továbbítását biztosítani [3].

Palicz összefoglaló közleménye a zsarolóvírus-támadások egészségügyi ellátórendszerekben észlelt hatásait elemezve hangsúlyozza, hogy a közvetlen pénzügyi fenyegetettség és anyagi károkozás mellett az egészségügyi szolgáltatások jellemzői miatt további káros következményekkel is számolni kell. Az ellátás akadályozottsága és a folyamatok átszervezési szükségessége elsősorban sürgősségi területen okoz veszélyes időveszteséget, de a tervezhető ellátásokra is negatívan hat. A betegadatok átmeneti vagy végleges elérhetetlensége akár életveszélyes késedelemhez vagy tévedésekhez vezethet. A közlemény az NKI megelőzésre vonatkozó javaslatait ismerteti: rendszeres biztonsági mentések; szoftverek, alkalmazások, vírusvédelem naprakész frissítése; biztonságtudatos dolgozói internethasználat elérése (például ismeretlen feladótól érkezett e-mailek és mellékletek kezelése); felhasználói fiókok, hozzáférések felügyelete, rendszeres ellenőrzése. A közlemény ismerteti a sürgős teendőket már bekövetkezett zsarolóvírus-támadás esetén: a megtámadott eszköz azonnali leválasztása a hálózatról; az intézményi hálózat teljes külső kapcsolatainak megszakítása; a megtámadott eszköz újraformázása, újratelepítése és az incidens jelentése az NKI felé. Javasolja a zsarolásképpen titkosított állományok megőrzését, megtartását esetleges későbbi sikeres visszafejtés érdekében. A szerző az NKI ajánlását idézi, ami szerint nem javasolt a támadónak történő fizetés, mivel ez sem garantálja a titkosított állományok helyreállíthatóságát [4].

Palicz és munkatársai hazai zsarolóvírus-támadásokat elemző közleménye megtörtént eseteket, a megtett intézkedéseket és a támadások következményeit mutatja be két nagy egészségügyi intézmény (megyei kórház) esetében [19].

Boven tanulmánya szintén a zsarolóvírus-támadások következményeit elemzi az egyik legkritikusabb területen, az akut ellátásban, 2017 és 2022 között Európában és az Egyesült Államokban kórházak ellen elkövetett eseményeket vizsgálva. A tanulmány szak- és IT-személyzeti interjúkon alapult, és a támadások akut és felépülési fázisait is elemezte. Az eredmények azt mutatták, hogy a zsarolóvírus-támadások jelentős, kritikus hatást gyakorolnak az akut ellátók működésére és a nyilatkozók felkészültségüket elégtelennek érezték [20].

Keogh és munkatársai egy írországi rákközpont elleni zsarolóvírus-támadásról számolnak be nagyon találó, Digitális bénulás című közleményükben. A támadás az ellátás gyors és tartós összeomlását okozta, az informatikai rendszerek leálltak, a sugárterápiás kezelések és műtétek teljesen, a diagnosztika csaknem teljesen működésképtelenné vált. A teljes rendszerhelyreállítás 210 napig tartott [21].

Az egészségügyi szektorban a kiberfenyegetettség különleges területe, amikor nem a komplex rendszereket éri támadás, hanem a hálózatokon kommunikáló intelligens eszközök (IoT, Internet of Things) kerülnek támadás alá. A beszámolók infúziós pumpák, pacemakerek és más orvostechnikai eszközök sebezhetőségét ismertetik [22].

Gordon és munkatársai kutatása az egészségügyi dolgozók kibertudatossági attitűdjét vizsgálta, közel 3 millió szimulált e-mail kiküldésével 6 USA-beli egészségügyi intézmény dolgozói számára. Hétből egy email esetében a dolgozók a csatolt linket megnyitották, ami az adathalász-támadásokkal szembeni jelentős veszélyeztetettségre utal [23].

Hasonló olaszországi vizsgálatról számolnak be Rizzoni és munkatársai, ebben is szimulált adathalász e-maileket küldtek 6000 dolgozónak. Az eredmények rámutatnak, hogy a célzott adathalászat mennyivel veszélyesebb, mivel az általános

adathalász e-mailek 64%-át sikeresen nem nyitották meg a munkatársak, viszont egyéni, célzott e-mailek esetében már csak 38% volt a nem megnyitott e-mailek aránya [24].

Szintén európai attitűdvizsgálatra példa Gioulekas közleménye. Görög, portugál és romániai kórházakban vizsgálták a kiberbiztonsági kultúrát. Jelentős hiányosságokat találva kiemelték a képzési programok fontosságát [25].

Nifakos és munkatársai összefoglaló közleményben vizsgálták az egészségügyi intézmények dolgozói attitűdjének hatását a kiberbiztonságra. Az adathalász-támadásokkal összefüggésbe hozható felhasználói viselkedési jellemzők azonosításán kívül keresték a kockázatértékelési módszertanokat és a kiberbiztonsági politikákat. Vizsgálták a lehetséges kiberhigiénés és adathalász-támadások leküzdésére használt gyakorlatokat. Kitértek a támadások miatti szolgáltatáskiesések gazdasági és társadalmi hatásaira [26].

Nunes és munkatársai portugál egészségügyi intézményben vizsgálták a dolgozói attitűdöt a korábban ismertetett Hadlington módszerrel [1]. A kérdőívek portugál nyelvű változata jól használhatónak bizonyult egészségügyi környezetben alkalmazva is [2].

Pfenninger és munkatársai a megfelelő és gyakorlatias felkészülésre mutatnak módszertant tanulmányukban. Egy német egyetemi kórház (Universitätsklinikum Ulm) kibertámadás miatti teljes leállásra készülve nyolc hónapos program keretében minden folyamatát áttekintette IT-szempontból, vészhelyzeti terveket dolgozott ki, offline működési folyamatokat tervezett és 72 órás leállást modellező szimulációs gyakorlatot végzett. A tapasztalatokat részletes felmérés keretében gyűjtötték össze, a visszajelzések alapján további, jövőre vonatkozó intézkedési terveket alkottak [27].

MEGBESZÉLÉS

A szakirodalom áttekintése alapján nemzetközi és hazai adatokra támaszkodva is kijelenthető, hogy a kibertudatosság társadalmi szinten elégtelen. A digitalizáció technológiai értelemben sokkal gyorsabban fejlődik, mint a felhasználók magatartásváltozása. Kultúraváltás zajlik, a társadalom életvitele átalakul, a kommunikációs technikák és kapcsolati módok megváltoznak, miközben a fizikai élet rutin biztonsági attitűdje nem jelenik meg a virtuális kapcsolatokban [15].

Hazai és uniós szinten is számos jogi szabályozás, stratégia készült a kiberbiztonság témakörében, de ezek széles körű társadalmi hatása még nem észlelhető. A kiépülőben lévő és fejlődő kiberbiztonsági intézményrendszer néhány éves múltja még nem eredményezett valós társadalmi beágyazottságot. A közoktatási és lakossági edukáció jelenleg még ismeretátadás szintjén is csak csekély hatást gyakorol az állampolgárokra, magatartásváltozáshoz pedig mélyebb beavatkozásokra, kiterjedtebb programokra lenne szükség [16].

A nem megfelelő kiberbiztonsági ismeretekkel rendelkező, nem biztonságos attitűdöt munkahelyi környezetbe magával hozó munkatárs a szervezeti kiberbiztonság „gyenge láncszeme". Belső meggyőződés hiányában a biztonsági feladatokat-szabályokat a dolgozók munkavégzésüket nehezítő, akadályozó körülményként élik meg, ha tehetik, megkerülik őket [17]. Sokak számára a kockázatok nem ismertek. A probléma gyökere ebben a témában is a szervezeti kultúra szintjén ragadható meg, az ismeretek átadásán túl a hozzáállás változtatására szükséges koncentrálni, mivel az attitűd komoly korrelációt mutat a kibertérbeli viselkedéssel. A hatásos megoldások erőforrás-igényesek, kidolgozásukhoz pszichológiai, pedagógiai ismeretek szükségesek, csak gyakorlati, tréningjellegű képzések, érzelmi szenzibilizáció lehet érdemi hatással az attitűdre. A helyzetfelmérésben, a szükséges oktatási anyagok összeállításában, a személyre szabott képzések biztosításában és a folyamatos monitorozásban is jól használható kérdőívek lelhetők a bemutatott szakirodalomban [1]. A szervezetek technológiai biztonsági szintje változó, a technikai módszerű sikeres kibertámadások azt mutatják, túl gyakran áll a háttérben nem frissített összetevő, elmaradt javítás vagy elégtelen vírusvédelmi megoldás [18]. A NIS2 szabályozás szisztematikus kockázatfelmérést előíró, a valós kockázati szinthez illesztett biztonsági megoldásokat megkövetelő elvárása sok szervezet prevenciós erőfeszítéseit teheti sikeresebbé [11].

Az egészségügyi szervezetek a fenti problémakörben hátrányosan érintettek. Az altruista szakmák praktikus, mindig a lényegesre (segítés, sürgősség, életmentés) koncentráló attitűdje gyakran bátorítja a dolgozókat kisebb szabályok figyelmen kívül hagyására „a nagyobb cél érdekében", ami a kiberbiztonsági, adatvédelmi, jogi szempontok háttérbe szorulásához vezethet. A beszámolók alapján látható, hogy az ágazatban is csak a gyakorlati, munkatársakat bevonó, mélyreható, a dolgozót személyében elérő tréningprogramok hatásosak [27]. A német klinikai példa sikerességében jelentős szerepe volt a folyamatok munkatársak bevonásával történt szisztematikus elemzésének, a percek alatt összeomló digitális rendszerek teljes leállása, a több hetes, évtizedek óta nem gyakorolt manuális-offline működés reális fenyegetése volt az az érzelmi eszköz, ami áttörhette a passzivitás gátjait. Egy saját részlegre fejlesztett kiberbiztonsági vészhelyzeti terv, a számos, egyáltalán nem működő funkció feltüntetésével, a részleges eredményességű vészmegoldások bemutatásával megrázó hatást gyakorolhat a kibertudatosságra.

Egy intézményi szintű, sikeres kibertámadás terror- vagy háborús helyzethez hasonlítható, váratlanul érkezik, nagyon gyorsan bekövetkezik a működés teljes blokkolása, és a helyreállítás hetekig tart [21]. Az egészségügyi ellátóintézmény 20-30 évvel korábbi működési állapotába zuhan, miközben számos ellátási funkciót (sürgős ellátás, intenzív osztályok, diagnosztika) nem, vagy nem azonnal lehetséges leállítani, és a lehetséges szinten a helyreállítási időszakban is működtetni kell. Ebből a szempontból a magasabb fejlettségű, digitalizáltabb intézmények nehezebb helyzetben vannak, az IT-behatolási kapuk és a munkatársak nagyobb száma, a dolgozók és folyamatok nagyobb digitális függősége miatt. A NIS2 irányelvvel összhangban a magas digitalizáltságú intézmények veszélyeztetettségi foka is magasabb, ennek megfelelő biztonsági besorolás és kiberbiztonsági tevékenység szükséges számukra [11].

KÖVETKEZTETÉSEK

A szakirodalom alapján bemutatott, egészségügyben is bevált kérdőívek hazai alkalmazására még nincs adat. A módszer a közölt bizonyítékok alapján a kitűzött céloknak megfelelő, hatásos eszköz, így hazai adaptációja segíthetné az egészségügyi intézményeket a helyzetfelmérésben és a kiberbiztonsági képzések bevezetésében. Az oktatás-képzés fontos szervezeti-intézményi feladat a jelenleg zajló NIS2 kibervédelmi felkészülésben is. A jogszabályban meghatározott, biztonsági osztálynak megfelelő védelmi intézkedések körében előírt biztonságtudatossági képzések eredményességét a tárgyalt szempontok figyelembevétele növelheti.

A szervezetbiztonság kritikus alterületeként tárgyalt kiberbiztonság sérülékenysége valós, az egészségügyet évről évre súlyosabban fenyegető probléma, aminek kapcsolódó betegbiztonsági következményei lehetnek. A bemutatott komplex eszközök, stratégiai gondolkodás, egységes kockázatkezelési szemlélet, a technológiára és a humán szempontokra egyaránt koncentráló változásvezetés, magatartásbefolyásoló tréningek és ismeretátadó oktató programok segítségével a hazai egészségügyi intézmények védelme is javítható lenne.

Anyagi támogatás
A publikáció elkészítése anyagi támogatás nélkül történt.

Érdekeltségek
A szerzőknek nincsenek érdekeltségeik.

IRODALMI HIVATKOZÁSOK

[1] Hadlington L: Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon. 2017; 3(7): 00346. https://doi.org/10.1016/j.heliyon.2017.e00346.

[2] Nunes P, Antunes M, Silva C: Evaluating cybersecurity attitudes and behaviors in Portuguese healthcare institutions. Procedia Comput. Sci. 2021; 181: 173–181. https://doi.org/10.1016/j.procs.2021.01.118.

[3] Stowman A, Frisch N, Gibson P et al.: Anatomy of a Cyberattack. Am. J. Clin. Pathol. 2022; 157(4): 510-517. https://doi.org/10.1093/ajcp/aqab162.

[4] Palicz T, Sas T, Tisóczki J et al.: "Your money or your life!" – Ransomwares in healthcare information systems [„Pénzt vagy életet!" – Zsarolóvírusok az egészségügyi informatikai rendszerekben]. Orvosi Hetilap. 2020; 161(36): 1498-1505. https://doi.org/10.1556/650.2020.31788. [Hungarian]

[5] 1139/2013. (III. 21.) Government decision on the National Cyber Security Strategy of Hungary [Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról] (2024. december 26-i állapot) [Hungarian]

[6] National Infocommunication Strategy [Nemzeti Infokommunikációs Stratégia] 2014–2020. https://2010-2014.kormany.hu/download/b/fd/21000/Nemzeti%20Infokommunik%C3%A1ci%C3%B3s%20Strat%C3%A9gia%202014-2020.pdf (megtekintve: 2024. december 26.) [Hungarian]

[7] Nemzeti Kibervédelmi Intézet. https://nbsz.gov.hu/tevekenyseg-mukodes/nemzeti-kibervedelmi-intezet (megtekintve: 2024. december 26.) [Hungarian]

[8] Healthy Hungary Health Sector Strategy [Egészséges Magyarország Egészségügyi Ágazati Stratégia] 2021-2027. https://mok.hu/public/media/source/Transzparencia/Allasfoglalasok/Eg%C3%A9szs%C3%A9ges%20Magyarorsz%C3%A1g%202021%E2%88%922027%20Eg%C3%A9szs%C3%A9g%C3%BCgyi%20%C3%81gazati%20Strat%C3%A9gia.pdf (megtekintve: 2024. december 26.) [Hungarian]

[9] National Digitalization Strategy [Nemzeti Digitalizációs Stratégia] 2021–2030. https://cdn.kormany.hu/uploads/document/6/60/602/6042669c9f12756a2b104f8295b866a8bb8f684.pdf (megtekintve: 2024. december 26.) [Hungarian]

[10] XXIII of 2023 Act on Cybersecurity Certification and Cybersecurity Supervision [2023. évi XXIII. törvény a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről] (2024. december 26-i állapot) [Hungarian]

[11] 2024. (VI. 24.) MK Decree on the requirements for classification in the security class, and on the specific protection measures to be applied in the case of each security class [7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről] (2024. december 26-i állapot) [Hungarian]

[12] EU Cybersecurity Strategy [Az Európai Unió Kiberbiztonsági Stratégiája]. 2013. (https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52013JC0001&from=EL) (megtekintve: 2024. december 26.)

[13] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016/1148 Európai Parlament és a Tanács (EU) irányelv a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről (NIS)]. 2016. https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX%3A32016L1148 (2024. december 26-i állapot)

[14] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) [2022/2555 (EU) irányelv (NIS2) 2022/2555 Európai Parlament és a Tanács (EU) irányelv (NIS2) 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] https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A32022L2555 (2024. december 26-i állapot)
[15] Gyaraki R: The Role of Security Awareness, Questions about Cybersecurity [A biztonságtudatosság szerepe, avagy kérdések a kiberbiztonságról]. Magyar Rendészet. 2022; 2: 245-261. https://doi.org/10.32577/mr.2022.2.16. [Hungarian]
[16] Krasznay Cs: Smart devices in critical information infrastructures [Okoseszközök a kritikus információs infrastruktúrákban]. In: Török B: Információ és kiberbiztonság. Ludovika Egyetemi Kiadó, Budapest, 2020: 121-147. [Hungarian]
[17] Center for Generational Kinetics. 2022. https://www.businesswire.com/news/home/20220216005463/en/New-Study-Uncovers-the-Risky-Behaviors-of-Employees-Which-Could-Lead-to-Security-Breaches-in-Highly-Regulated-Industries (megtekintve: 2024. december 26.)
[18] Gallagher S: Conti and Karma actors attack healthcare provider at same time through Proxy Shell exploits. Sophos News. 2022. https://news.sophos.com/en-us/2022/02/28/conti-and-karma-actors-attack-healthcare-provider-at-same-time-through-proxyshell-exploits/ (megtekintve: 2024. december 26.)
[19] Palicz T, Sas T, Szabó Z et al.: Ransomware attacks in Hungarian hospitals – case studies [Magyar kórházakban előfordult zsarolóvírus támadások esetei]. IME. 2021; 2021/1: 32-38. https://doi.org/10.53020/IME-2021-105. [Hungarian]
[20] Boven L, Kusters R, Tin D et al.: Hacking Acute Care: A Qualitative Study on the Health Care Impacts of Ransomware Attacks Against Hospitals. Ann. Emerg. Med. 2024; 83(1): 46-56. https://doi.org/10.1101/2023.02.13.23285854.
[21] Keogh R, Harvey H, Brady C et al.: Dealing with digital paralysis: Surviving a cyberattack in a National Cancer Center. J. Cancer Policy. 2024; 39 https://www.sciencedirect.com/science/article/abs/pii/S2213538323000838?via%3Dihub https://doi.org/10.1016/j.jcpo.2023.100466
[22] McKeon J: Healthcare IoT, Medical Device Vulnerability Disclosures Skyrocket. 2022. https://healthitsecurity.com/news/healthcare-iot-medical-device-vulnerability-disclosure-skyrocket (megtekintve: 2024. április 26.)
[23] Gordon W, Wright A, Aiyagari R et al.: Assessment of Employee Susceptibility to Phishing Attacks at US Health Care Institutions. JAMA Netw. Open. 2019; 2(3). https://doi.org/10.1001/jamanetworkopen.2019.0393.
[24] Rizzoni F, Magalini S, Casaroli A et al.: Phishing simulation exercise in a large hospital: A case study. Digit. Health. 2022; 8. https://doi.org/10.1177/20552076221081716.
[25] Gioulekas F, Stamatiadis E, Tzikas A et al.: A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures. Healthcare. 2022; 10(2): 327. https://doi.org/10.3390/healthcare10020327.
[26] Nifakos S, Chandramouli K, Nikolaou Ch et al.: Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review. Sensors. 2021; 21(15): 5119. https://doi.org/10.3390/s21155119.
[27] Pfenninger E, Schmidt S, Rohland C et al.: Resilience against IT attacks on hospitals [Resilienz gegen IT-Angriffe an Kliniken]. Anaesthesiologie. 2023; 72: 852–862. [German] https://doi.org/10.1007/s00101-023-01331-y.

A SZERZŐK BEMUTATÁSA

Vida Zoltán 1999-ben végzett a Pécsi Orvostudományi Egyetem Orvostudományi Karán. 2013-ban a Pázmány Péter Katolikus Egyetem Jog- és Államtudományi Karán jogi szakokleveles orvos, 2018-ban a Semmelweis Egyetem Egészségügyi Menedzserképző Központban minőségügyi és betegbiztonsági menedzser oklevelet, 2021-ben ugyanitt Egészségügyi menedzser MSc diplomát szerzett. 25 éve dolgozik a diagnosztikai betegellátásban, hatéves kórházi orvosvezetői működést követően jelenleg a Budavári Önkormányzat Egészségügyi Szolgálata Szakorvosi Rendelőintézet orvosigazgatója. A Semmelweis Egyetem Egészségügyi Menedzserképző Központjában több minőségfejlesztési, betegbiztonsági projektben szakmai szakértőként vett részt.

Lám Judit 1995-ben szerzett diplomát a Semmelweis Egyetem Gyógyszerésztudományi Karán, 2002-ben szerezte PhD-fokozatát és egészségügyi szakmenedzseri oklevelét. A Semmelweis Egyetem Egészségügyi Menedzserképző Központjának docense, operatív igazgatóhelyettese, valamint az Egészségügyi Közszolgálati Kar általános dékánhelyettese. A Betegbiztonsági Tanszék vezetőjeként betegbiztonság és minőségügyi témakörökben rendszeresen oktat graduális és posztgraduális kurzusokon, a NEVES betegbiztonsági program társvezetője.