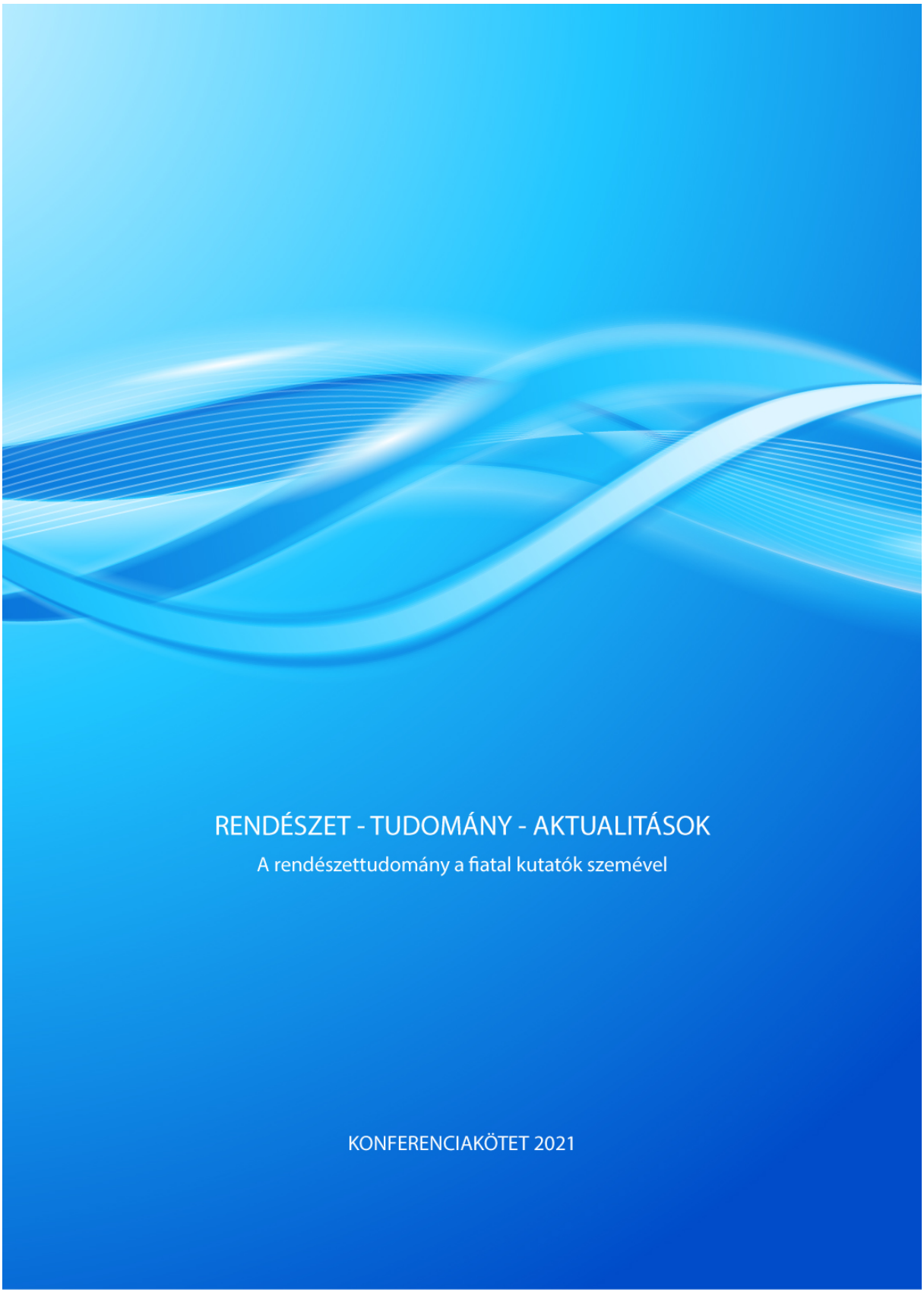

RENDÉSZET - TUDOMÁNY - AKTUALITÁSOK

A rendészettudomány a fiatal kutatók szemével

KONFERENCIAKÖTET 2021

RENDÉSZET-TUDOMÁNY-AKTUALITÁSOK - 2021
A rendészettudomány a fiatal kutatók szemével

Online konferenciakötet

Szerkesztette:

Baráth Noémi Emőke

Mezei József

Doktoranduszok Országos Szövetsége Kiadó

Doktoranduszok Országos Szövetsége

Rendészettudományi Osztály

Budapest

ISBN: 978-615-5586-89-7

A kötetben megjelent tanulmányok szakmai lektorai és szekcióvezetői:

Dr. Auer Ádám
Dr. Farkas Johanna
Dr. Hegedűs Judit
Dr. Kemény János
Dr. Regényi Kund
Dr. Ritecz György
Dr. Tóthi Gábor
Prof. Dr. Sallai János
Dr. Czenczer Orsolya

A Doktoranduszok Országos Szövetsége Rendészettudományi Osztály 2020/2021-es év tisztségviselői és a konferencia szervezői:

Baráth Noémi Emőke- elnök
Mezei József -általános alelnök
Kovács Szitkay Eszter - titkár
Fekete Márta- büntetés-végrehajtási területért felelős tudományos referens
Schmidt Laura - kommunikációs referens
Szigetvári Oszkár - rendőrségi területért felelős tudományos referens
Beke József - nemzetbiztonsági területért felelős tudományos referens
dr. Pozsgai Petra – nemzetközi referens
Görömbei Zoltán- osztálytag
Molnár Tamás -osztálytag
Suhajda Attila -osztálytag
Pászti Péter - osztálytag

A kötet a Rendészet-Tudomány-Aktualitások 2021. A rendészettudomány a fiatal kutatók szemével című tudományos konferencián elhangzott előadásokat tartalmazza.

A rendezvény az Emberi Erőforrások Minisztériuma megbízásából az Emberi Erőforrás Támogatáskezelő által meghirdetett Nemzeti Tehetség Program NTP-FKT-M-18-0003 kódszámú pályázati támogatásból valósult meg.

Tartalomjegyzék

Fodorné Zagyi Orsolya: Az egészségügyi adatok védelme az e-health technológiák tükrében[1]

Absztrakt

A tanulmány középpontjában az egészségügyi adatok kezelésének és digitalizálásának adatvédelmi szempontú vizsgálata áll. Arra a kérdésre keresi a választ, hogy az e-health térnyerésével milyen újabb adatvédelmi kihívásokkal kell szembenéznie egy egészségügyi szolgáltatónak az adatkezelések során, elsősorban az orvostechnológiai eszközök tekintetében? A tanulmány elkészítése során alkalmazott módszer elsősorban szakirodalmi vizsgálat, ill. másodlagos adatelemzés. Az egészségügyi adatokat az információbiztonság hármas követelményével (bizalmasság, sértetlenség, rendelkezésre állás) megegyezően különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen kell védeni. A leggyakrabban kihasznált sebezhetőségek az orvostechnikai eszközökben: nem biztonságosak a firmware frissítések, a fizikai támadások figyelmen kívül hagyása, a gyártási karbantartáshoz használt parancsok engedélyezettek maradnak. A modern technológiák a felhasználásuk és terjedésük okán kikényszerítik alkalmazásuk további adatvédelmi szabályozását, amellyel elkerülhetőek lennének a kiberbűnözés fenyegetései.

Kulcsszavak: e-health, egészségügyi adatok, adatvédelem, digitalizálás, információbiztonság

1. Bevezetés

A „tárgyak internete” (Internet of things = IoT) forradalmat jelent az infokommunikációs eszközök világában. Az eszközök, a rendszerelemek és a hálózatok mindenütt jelen vannak és összekapcsolódnak. Ez a technológiai fejlődés az egészségügyi ágazatban is jelentős eredményeket mondhat magáénak. A csatlakoztatott orvostechnikai eszközök átalakítják az egészségügyi ipar működését mind a kórházakon belül, mind az egészségügyi ágazat különböző szereplői között. Noha a digitális egészségügynek sok hasznos alkalmazása van, a betegek személyes egészségügyi adatait illetően az érzékeny információk elkerülhetetlenül kiválthatnak adatbiztonsági problémákat. Ahogy növekszik a csatlakoztatott eszközök száma, úgy növekszik a támadási felület, és a támadási potenciál exponenciálisan változik. Ebben a tanulmányban az egészségügyi adatok kezelésének szabályozásába való betekintéssel ráirányítjuk a figyelmet az egészségügyi szolgáltatók és digitális egészségügyi eszközök sebezhetőségére, és néhány adatvédelmi probléma még megoldandó feladatára.

2. Az egészségügyi adatok kezelésének magyarországi szabályozása

[1] Phd hallgató, KRE-ÁJK, fzagyio@gmail.com

Az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény (a továbbiakban Eüak tv.) az egészségügyi ellátó-hálózattal kapcsolatba került vagy kerülő személyek személyiségi jogait védi az adatokhoz való illetéktelen hozzáféréssel szemben. A törvény felsorolja az egészségi állapotra vonatkozó különleges személyes adatok és az azokhoz kapcsolódó személyes adatok kezelésének feltételeit és céljait. „Az egészségügyi és személyazonosító adat kezelésének célja:

a. az egészség megőrzésének, javításának, fenntartásának előmozdítása,
b. a betegellátó eredményes gyógykezelési tevékenységének elősegítése, ideértve a szakfelügyeleti tevékenységet is, c) az érintett egészségi állapotának nyomon követése,
c. a népegészségügyi [16. §], közegészségügyi és járványügyi érdekből szükségessé váló intézkedések megtétele,
d. a betegjogok érvényesítése.” (Eüak tv. 4.§ (1))

A jogszabály alapelve az önkéntesség (Eüak tv. 12.§ (1)), amelyet csak néhány, a szükséges esetben tesz kötelező jellegűvé (pl.: fertőző betegségek esetén, egyes szűrő és alkalmassági vizsgálatok elvégzésekor). Az egészségügyi és a személyazonosító adatoknak az érintett részéről történő szolgáltatása önkéntes, amiről az érintettet tájékoztatni kell. Az érintett úgy veheti igénybe az egészségügyi ellátást, ha a kötelezően előírt személyazonosító adatokat megadja az egészségügyi szolgáltató részére. Az egészségügyi adatok felvétele a gyógykezelés része. Ha a beteg önként keresi fel az egészségügyi szolgáltatók valamelyikét, úgy az egyben felhatalmazás is az érintett adatainak kezelésére. Ha az érintett belátási képességének hiányában van vagy sürgősség esete forog fenn, az önkéntességet vélelmezni kell. Ez a feltételezés nagyban megkönnyíti az egészségügy működését. Egészségügyi és személyazonosító adatot mindezeken túl – törvényben meghatározott esetekben – az alábbi célból lehet kezelni: egészségügyi szakember-képzés, orvosszakmai és epidemiológiai vizsgálat, elemzés, az egészségügyi ellátás tervezése, szervezése, költségek tervezése, statisztikai vizsgálat, tudományos kutatás. (Eüak tv. 4.§ (2)) Az egészségügyi szakember-képzés céljából az érintett hozzájárulásával lehet jelen a gyógykezelés során orvos, orvostanhallgató, egészségügyi szakdolgozó, egészségügyi főiskola, egészségügyi szakiskola vagy egészségügyi szakközépiskola hallgatója, valamint tanulója (Eüak tv. 17.§ (1)). Az egészségügyi ellátóhálózat egészségügyi szakember-képzésre kijelölt intézményeiben az érintett hozzájárulására nincs szükség. Erről az érintettet fekvőbeteg-intézmény esetén legkésőbb az intézménybe történő beutaláskor, beutaló hiányában a felvételt közvetlenül megelőzően, az egészségügyi ellátó-hálózat egyéb intézményei esetén legkésőbb a gyógykezelés megkezdése előtt tájékoztatni kell. (Eüak tv. 17.§ (2)) Az egészségügyi ellátó hálózaton belül az egészségügyi és személyazonosító adat kezelésére jogosult a beteg gyógykezelésében résztvevő, az intézményvezető, az adatvédelmi tisztviselő, valamint az ellátásszervező adatelemzéssel megbízott alkalmazottja. Az adatkezelő, a megbízott adatfeldolgozó köteles az orvosi titkot megtartani. Az adatkezelő mentesül a titoktartási kötelezettség alól, ha az egészségügyi és személyazonosító adat továbbítására az érintett, illetve törvényes képviselője írásban hozzájárult, az abban foglalt korlátozásokon belül, valamint ha az egészségügyi és személyazonosító adat továbbítása törvény előírásai szerint kötelező. (Eüak tv. 17.§ (2))

Az egészségügyi szolgáltatónak nyilvántartást kell vezetni az érintettről felvett, a gyógykezelés érdekében szükséges egészségügyi és személyazonosító adatokról, valamint azok továbbításáról. Az adattovábbításról szóló feljegyzésnek tartalmaznia kell az adattovábbítás címzettjét, módját, időpontját, valamint a továbbított adatok körét. (Eüak tv. 28.§ (1)) Az egészségügyi dokumentáció a gyógykezelés érdekében szükséges egészségügyi és személyazonosító adatokat tartalmazza, beleértve az elvégzett diagnosztikai vizsgálatok eredményeit tartalmazó dokumentumokat is.

Tudományos közleményben nem szerepelhetnek egészségügyi és személyazonosító adatok oly módon, hogy az érintett személyazonossága megállapítható legyen, de tudományos kutatás céljából az intézményvezető vagy az adatvédelmi tisztviselő engedélyével a tárolt adatokba be lehet tekinteni. (Eüak tv. 21.§ (1)-(2)) Tudományos kutatás során nem készíthető olyan másolat a tárolt adatokról, amelyek személyazonosító adatot tartalmaznak. A betekintő személyekről, a betekintés céljáról és időpontjáról az egészségügyi szolgáltatónak nyilvántartást kell vezetni. A nyilvántartást 10 évig kell megőrizni. Az egészségügyi intézményen belül az egészségügyi és személyazonosító adatok védelméért, a nyilvántartás kezelésért az adatokat kezelő egészségügyi szolgáltató vezetője felel, ő jelöli ki az adatvédelmi tisztviselőt is. (Trócsányi, 2007)

3. Az e-health és a digitális adatkezelés

Az e-health eredetileg elektronikusan elérhető egészségügyi szolgáltatást jelent, amelyet az e-government részeként értelmeztek, de mára az e-egészségügy szinonímája lett. Az Európai Bizottság meghatározása szerint (Európai Bizottság, 2003) a megelőzés, a diagnosztizálás, a kezelés, a nyomon követés és az irányítás javítását segítő információs és kommunikációs technológiákat hasznosító eszközök és szolgáltatások összessége. Az európai egészségügy működését a magas költségek és a korlátozott források határozzák meg. Az e-egészségügy támogatja az egészségügyi rendszerek átalakulását, amely azért szükséges, hogy válaszoljon a demográfiai öregedés, az erőforrások szűkössége, az egészségügyi szakemberek hiánya, a krónikus betegségek növekedésének kihívásaira. Ennek egyik lehetséges módja, hogy fokozza az időszerű és megfelelő egészségügyi ellátást mindenki számára. Az információstechnológia (IT) Támogatja a szolgáltatások hatékonyabb felhasználását és az egészségügyi ágazat kapacitásainak jobb kihasználását. (WHO, 2005)

Az e-health legnagyobb vívmányai:

- A *telemedicina*: Legnagyobb vívmánya, hogy az orvos képes meglátni és megvizsgálni a tőle távol lévő beteget. Az egyidejű, kétirányú hang-, adat- és képkommunikáció (interaktív videó) jó alapot nyújt az egészségügyi szakemberek számára, akik ezzel azonnali segítséget tudnak nyújtani. Az IT eszközök, mint laptopok, notebookok, tabletek, mobileszközök, és egyéb adatbeviteli eszközök, a beteg kórtörténetét rögzítik, és ezek képesek a vonatkozó információkat elektronikus úton továbbítani egy fő adatbázisba. Egyre gyakoribb, hogy az egészségügyi szolgáltatók valós idejű orvosi berendezések nyomkövető rendszerét (pl. RFID = Radio Frequency IDentification) alkalmazzák a betegek azonosításához, a helymeghatározáshoz és a gyógyszeradagoláshoz.

- A *rugalmas és intelligens technológiákon alapuló rendszerek*, amelyek képesek az emberi testhez alkalmazkodni és amelyek integrálják az elektromos, optikai, kémiai és mechanikus érzékelők lehetőségeit. Képesek az azonnali betegellátáshoz biztosítani a technikai feltételeket. Például RFID implantátumok, amelyeket a bőr alá injektálnak. Ezek a rendszerek különféle paramétereket (biojelek, elhelyezkedés stb.) figyelnek, és szükség esetén biztonságosan kommunikálnak az egészségügyi szakemberekkel, valamint az intelligens támogatási rendszerekkel. A nyilvántartásokat rendszeresen frissítik, és a különböző egészségügyi szakemberek számára elérhetőek az ellátás során folyamatosan.

- *Nagy adattechnológiák (Big Data)*. A mesterséges intelligencia (AI) és a gépi tanulás (ML) elősegíti az e-health fejlődését. Az AI, vagyis az emberi intelligencia beépíthető a gépekbe, így ezek a gépek logikát és érvelést alkalmaznak a bemenetek elemzésére és a kognitív funkciók ellátására. „A mesterséges intelligencia intelligens viselkedésre utaló rendszereket takar, amelyek konkrét célok eléréséhez elemzik környezetüket és – bizonyos mértékű autonómiával – intézkedéseket hajtanak végre."(Európai Bizottság, 2018, 1.) Ez a definícó hamar átfogalmazásra került, mely szerint: a mesterséges intelligencia alapú rendszerek olyan, ember által tervezett szoftverek, amelyek meghatározott komplex célok elérése érdekében cselekszenek a fizikai vagy digitális dimenzióban, és elemzik környezetüket adatgyűjtés, az összegyűjtött rendszerezett vagy rendszertelen adatok értelmezése, tudásalapú érvelés vagy az információfeldolgozás által, majd a származtatott adatokból a legjobb, legmegfelelőbb cselekvést valósítják meg a meghatározott cél elérése érdekében. (European Commission, 2019)

Az egészségügyi szolgáltatónál végzett adatkezelések önálló adatkezelési rendszert alkotnak, a szolgáltatónál alkalmazott adatkezelési rendszereket pedig az intézményvezető határozza meg. (62/1997. NM rend. 1.§ (1)-(2)) Az elektronikus egészségügyi rendszereket úgy kell kialakítani, hogy a digitalizált egészségügyi dokumentumokat, a bennük szereplő személyes és különleges adatokat kizárólag az arra jogosultak tudják megismerni, valamint megfelelő szervezési és eljárási szabályok kialakításával kell az adatbiztonságról gondoskodni.

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.) célként fogalmazza meg a hatálya alá tartozó (Ibtv. 2. §) elektronikus információs rendszerek és az azokban kezelt, tárolt és feldolgozott adatok zárt, teljes körű, folytonos és kockázatokkal arányos védelmének biztosítását. A 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.) általános tartalmú adatbiztonsági elvárásokat fogalmaz meg, a részletes szabályokat az egészségügyi szolgáltatók tevékenység specialitásaihoz igazodva az ágazati jogszabályok és az egyedileg kialakított intézményi adatbiztonsági szabályzatok tartalmazzák. Az Infotv. értelmében az adat mindaddig megőrzi személyes minőségét, amíg kapcsolata az érintettel az adatkezelő által helyreállítható, azaz az adatkezelő rendelkezik a helyreállítás technikai lehetőségével. Több technológiai, illetve eljárásrendi megoldás is létezik, melyekkel biztosítható az érintettel való kapcsolat helyreállíthatóságának kizárása. Az Infotv. az adatbiztonsági követelményekre vonatkozó előírások körében fogalmazza meg az ún. privacy by design, a tervezésbe épített adatvédelem követelményét. Ennek értelmében az érintettek magánszférájának védelmét szavatoló adatvédelmi biztosítékokat már a termékek, szolgáltatások, működési struktúrák és eljárások megtervezésekor érvényesíteni kell. (Infotv. 7. § (1)) Az eljárásrendi megoldások körébe tartozik például a kapcsolati kódok képzésével történő adatfelvétel, rögzítés és tárolás, míg technológiai megoldás lehet az adatok anonimizáló algoritmusokkal történő átdolgozása, vagy az adatállományok aggregálása. Ezen megoldások biztosítják, hogy az adat elveszti személyes jellegét. (Bocsok V. et al., 2015)

4. Az egészségügyi információs rendszerek sebezhetősége

A digitális egészségügyi eszközök számos előnyt jelentenek, lehetővé téve az állampolgárok biztonságának megőrzését, az egészségügyi szakemberek gyors hozzáférését az egészségügyi dokumentációhoz és a betegek számára dinamikus kapcsolatot az állami és magán egészségügyi

szolgáltatókkal. Az új digitális egészségügyi megoldások azonban új kihívásokkal és új előnyökkel járnak. A digitális biztonság szempontjából kulcsfontosságú a kiberbiztonsági fenyegetések és az azok által a betegadatokra jelentett kockázatok kezelése.

Európai Unió Kiberbiztonsági Ügynöksége (ENISA = European Union Agency for Cybersecurity) annak érdekében, hogy segítsen az egészségügyi szervezeteknek a magasabb szintű kiberbiztonság elérésében az általa összegyűjtött információk és a bevált gyakorlatok megosztásával lehetővé teszi az egészségügyi szolgáltatóknak a helyzetük javítását. (Drougkas, A., Liveri**,** D., 2020.) Mivel a kiberbiztonság egyre nagyobb prioritássá válik az egészségügyi szolgáltatók számára, elengedhetetlen, hogy az adatvédelem holisztikusan integrálódjon az egészségügyi ICT-ökoszisztémát befolyásoló különböző folyamatokba, összetevőkbe és szakaszokba. Az e-egészségügyben elsődleges adatvédelmi fenyegetettséget az egészségügyi információs rendszer működésével összefüggő technológiai, technikai problémák okozzák, úgy mint: a felhőszolgáltatásokat biztosító szolgáltató hibája, a hálózati szolgáltató hibája, áramellátás meghibásodása, az orvostechnikai eszközök gyártásával összefüggő meghibásodás. A felhőszolgáltatás igénybevétele egyre elterjedtebb az egészségügyi szolgáltatók körében, hiszen nem minden szolgáltatás és a vele járó adatforgalom, adattárolás található a szolgáltató központi szerverén. A könyvelés, a fizetések nyilvántartása, elszámolása, a készletellenőrzés kiszervezhető, és függ a harmadik fél felhőszolgáltatásaitól. A személyes IT orvosi eszközök szinte mindegyike a felhőben működik. Ezek a szolgáltatások, ha nincsenek megfelelően alátámasztva az off-line munkavégzéshez, súlyos zavarokat okozhatnak az orvosi szolgáltatások nyújtásában. A hálózati szolgáltató hibájából eredő hálózati meghibásodásnak pusztító hatása lehet. A redundancia és a topológia kialakítása döntő fontosságú az ilyen típusú fenyegetések enyhítésében. Az áramellátás meghibásodása esetén a biztonságos betegellátás érdekében az egészségügyi szolgáltatók alternatív eszközökkel biztosítják a működés folytonosságát. Az intenzív osztályokat, az operatív szobákat, a szervereket általában szünetmentes áramforrások vagy akkumulátorok védik, de más berendezések, például az MRI vagy a CT gépek is veszélybe kerülhetnek, amelyek védelméről szintén gondoskodni kell. Az orvostechnikai eszközök gyártásával összefüggő meghibásodás esetén ezek látens hibák, és bizonyos körülmények között a készülékek normál használata során is jelentkezhetnek. Valamennyi orvostechnikai eszköznél előfordulhat tervezési hiba a rendszerben.

A fentiekben tárgyalt hibák mellett egyre nagyobb kiberbiztonsági fenyegetést jelentenek az informatikai rendszereket érő rosszindulatú támadások. Az egészségügyi szervezetekben az informatikai rendszerek szorosan összekapcsolódnak, és nehéz őket úgy elkülöníteni, leválasztani anélkül, hogy a szolgáltatás folyamata megszakadna. Ennek köszönhetően ezek a rendszerek optimális helyek a rosszindulatú programok számára. (Kruse, Clemens Scott et al., 2017.) A nagyon sok eszközzel rendelkező egészségügyi szolgáltatóknak nehézségeik lehetnek a licencek frissítésével, miután ezeknek jelentős költségei vannak. Az adware az egyik legegyszerűbb módszer a rosszindulatú programok terjesztésére, és a felhasználók ezt gyakran figyelmen kívül hagyják. A ransomware jelenti a legismertebb fenyegetést az egészségügyi szervezetek számára, főleg a Wannacry-eset miatt (A WannaCry egy zsarolóvírus, amely behatol egy felhasználó számítógépébe, titkosítja fájljait, és utasítja az áldozatot, hogy fizessen Bitcoin-ban a fájlok visszaszerzése érdekében.)

Az orvosi berendezéseknek általában valós idejű kommunikációra van szükségük, és a klinikusoknak is gyors válaszra várnak a rendszertől is, amikor a betegadatokat vagy a vizsgálati információkat keresnek. A processzor működési sebességére vagy a kommunikációs kapacitásra hatással van egy esetleges, kéretlen adatbányászat, a kriptopénz bányászatára való kényszerítés (cryptojacking, medjacking). Ez kihat a rendszer teljesítményére és természetesen az egészségügyi ellátásra is. A cryptojacking és a medjacking közötti különbség alapvetően az érintett hardver. Az első esetben általános célú informatikai infrastruktúráról, a másodikban

pedig informatikai alapú orvosi berendezésekről beszélünk. (Koppel, R. 2015.) Ez a módszer akkor is működik egy-egy kártékony weboldalon vagy appon keresztül, ha a készülékek rendszere teljesen védett és biztonságilag naprakész. (Welp, Annalena et al., 2019.) A social engineering az emberi tényező kihasználható tulajdonságaira, az emberi hiszékenységre építő támadási forma, olyan technikák és módszerek összessége, amely az emberek befolyásolására, manipulálására alapozva teszi lehetővé bizalmas információk megszerzését, vagy éppen egy kártékony program terjedését és működését. (adathalászat, baiting, eszközklónozás) További veszélyeket hordoz az eszközök/adatok lopása, a skimming, a szolgáltatás blokkolása a hálózaton keresztül. (Smith, Sean W. & Koppel, Ross, 2014.)

Egy friss tanulmány a COVID-19 nyomán vizsgálta az egészségügyi és orvosi alkalmazásokat adatbiztonsági szempontból. Megállapította, hogy ezen alkalmazások 71%-ában van legalább egy olyan súlyos sebezhetőség, amely az orvosi adatok megsértéséhez vezethet. A tanulmányt az Intertrust (2020.) készítette, különösen a pandémiás helyzetre való tekintettel. Megállapították, hogy a COVID-19 nyomkövető alkalmazások 85% -a kiszivárogtatja az adatokat. Ezen kívül felhívja a figyelmet a következő biztonsági problémákra is:

- A tesztelt orvosi alkalmazások 71%-ában van legalább egy magas szintű biztonsági rés.
- Az orvosi alkalmazások túlnyomó többségében (91%) rosszul kezelik és / vagy gyenge a titkosítás, ami veszélyezteti őket az adatok kitettségének és az IP (szellemi tulajdon) lopásának.
- Az Android-alkalmazások 34%-a és az iOS-alkalmazások 28%-a sérülékeny a titkosítási kulcsok kibontása szempontjából.
- Ha kifejezetten a COVID-nyomkövető alkalmazásokat nézzük, 85% -uk kiszivárogtatja az adatokat.
- A felfedezett magas szintű fenyegetések 83%-át enyhíteni lehetett volna olyan alkalmazásvédelmi technológiákkal, mint a kód elhomályosítása, a manipuláció felderítése és a fehér dobozos kriptográfia.

5. Az orvosi eszközök kiberbiztonsági kérdései

Orvostechnikai eszköz lehet bármilyen eszköz, készülék, eszköz, gép, készülék, implantátum, in vitro felhasználásra szánt reagens, szoftver, anyag vagy más hasonló vagy kapcsolódó cikk, amelyet a gyártó önállóan vagy együttesen gyógyászati célra szán. (GHTF, 2012)

Az orvosi eszközök sebezhetősége szintén teret adhat adatvédelmi incidensek lehetőségére. Az eszközök gyártási folyamatait hagyományosan szigorúan az orvostechnikai eszközök beszállítói ellenőrzik, valójában nagyon gyakori, hogy az ellátási láncban harmadik féltől származó szoftver- és elektronikai eszköz, alkatrész van. Ennek eredményként a gyártóknak nemcsak az anyagokat, a tartósságot vagy a sterilizálást kell ellenőrizniük, hanem a szoftvereket és az elektronikát is tesztelniük kell, hogy megbízhatóak és biztonságosak legyenek. Különösen a drága egészségügyi felszerelések esetén szokás olyan eszközöket bérelni, amelyeket korábban más egészségügyi szervezetek is használhattak, és gyakran alapértelmezett beállítással érkeztek. Ezen beállítások megtartása fenyegetést jelenthez az egészségügyi rendszer számára.

Az orvosi berendezések általában nagyon drágák, így várhatóan ezek az eszközök hosszú évekig üzemben lesznek. Ennek a hosszú életciklusnak köszönhetően az egészségügyi szolgáltatónak néha nehézségei lehetnek a karbantartási támogatás biztosításában. Emiatt a kibertámadások kihasználhatják az informatikai rendszer sebezhetőségét.
Az orvosi berendezések kezelése és beállítása mindig összetett. Sem az orvosokat, sem az informatikai osztályt nem szokták kiképezni az új felszerelések telepítésére, karbantartására.

(Mccaffery, F., Coleman, G., 2007.) A szokásos eljárás az, hogy megvásárolt/bérelt a berendezést a szállító normál beállításban hagyja. Így az alapértelmezett jelszavak által a rendszer sebezhetősége és az ismeretlen funkciók aktiválása kihívás ebben a környezetben. Az eszközök operatív eljárásokat hajthatnak végre (pl. Dátum/idő kérések, műszaki és szolgáltatási adatok közlése a gyártóval, karbantartási kérések, automatikus frissítések, … stb.), amelyek a vevő számára ismeretlenek, és biztonsági riasztásokat indíthatnak el. (Kruse, Clemens Scott et al., 2017.)
A legújabb orvostechnikai eszközök általában távvezérléssel működnek. Ez lehetővé teszi a szolgáltatók számára a karbantartási költségek csökkentését és egyéb műveletek elvégzését. A távvezérléshez használt kommunikációs eszközök biztonsági beállítási, vezérlőszoftverei szintén sebezhetővé tehetik az egészégügyi információs rendszert. (Zorz, Z. 2020.) A kiberbiztonság egy lánc, amelyben az eszköz biztonságos működéséhez a lánc összes láncszemének biztosnak kell lennie. A támadók mindig azt a leggyengébb láncszemet keresik, amely adatbiztonság szempontjából a legsérülékenyebb.

6. Összefoglalás

Az adatokat az információbiztonság hármas követelményével (bizalmasság, sértetlenség, rendelkezésre állás) megegyezően különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen kell védeni. A 29. cikk szerinti Munkacsoport a tagállami szakértők bevonásával folyamatosan dolgozik az új technológiák sajátosságai által generált szabályozási feladatokon.. Az új digitális egészségügyi megoldások azonban új kihívásokkal és új előnyökkel járnak. A digitális biztonság szempontjából kulcsfontosságú a kiberbiztonsági fenyegetések és az azok által a betegadatokra jelentett kockázatok kezelése.

Hivatkozások

1997. évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről. Forrás: https://net.jogtar.hu/jogszabaly?docid=99700047.tv letöltési idő: 2020.11.02.

1997. évi CLIV. törvény az egészségügyről. Forrás: https://net.jogtar.hu/jogszabaly?docid=99700154.tv letöltési idő: 2021.02.12.

2010. évi CLVII. törvény a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről. Forrás: https://net.jogtar.hu/jogszabaly?docid=a1000157.tv letöltési idő: 2021.02.12.

2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról. Forrás: https://net.jogtar.hu/jogszabaly?docid=a1100112.tv letöltési idő: 2021.02.12.

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról. Forrás: https://net.jogtar.hu/jogszabaly?docid=a1300050.tv letöltési idő: 2021.02.12.

62/1997. (XII. 21.) NM rendelet. Forrás: https://net.jogtar.hu/jogszabaly?docid=99700062.nm letöltési idő: 2021.02.12.

Bestsennyy, Oleg, Gilbert, Greg, Harris, Alex and Rost, Jennifer: Telehealth: A quarter-trillion-dollar post-COVID-19 reality? May 29, 2020. Forrás: https://www.mckinsey.com/industries/healthcare-systems-and-services/our-insights/telehealth-a-quarter-trillion-dollar-post-covid-19-reality letöltési idő: 2020.11.20.

Bocsok Viktor, Boldizs Péter Ferenc, Loós Csaba, Major Tamás (2015): A dolgok internete. Technológiai háttér, információbiztonsági és adatvédelmi aspektusok. Forrás: https://nmhh.hu/cikk/192604/A_dolgok_internete letöltési idő:2020.11.24.

Chi, Y.; He, D.; Han, S.; Jiang, J. (2018): What Sources to Rely on: Laypeople's Source Selection in Online Health Information Seeking. In Proceedings of the 2018 Conference on Human Information Interaction & Retrieval, New Brunswick, NJ, USA, 11–15 March 2018; ACM: New York, NY, USA; 233–236. o. Forrás: https://www.researchgate.net/publication/326293339_What_sources_to_rely_on_Laypeople's_source_selection_in_online_health_information_seeking letöltési idő: 2020.11.26.

Drougkas, Dr. Athanasios; Liveri, Dimitra, Zisi, Antigone, Kyranoudi, Pinelopi: Procurement Guidelines For Cybersecurity In Hospitals. Good practices for the security of Healthcare services. Feb. 2020. ISBN 978-92-9204-312-4, DOI 10.2824/943961 Forrás: https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services letöltési idő: 2021.03.10.

E-egészségügy (2015) Infojegyzet 2015/62. 2015. november 18. Forrás: https://www.parlament.hu/documents/10181/303867/2015_62_E_egeszsegugy/3d69ec52-210a-4f81-b935-d1eb1a663c39 letöltési idő: 2020.11.20.

Európai Bizottság (2018): Mesterséges intelligencia Európa számára – A Bizottság közleménye az Európai Parlamentnek, az Európai Tanácsnak, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának. COM (2018) 237 final/2 (a továbbiakban: COM(2018) 237 final/2). Brüsszel, 2018. 06. 26., 1. Forrás: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52018DC0237R(01) letöltési idő: 2021.03.10.

European Commission. Ministerial Declaration. Brussels. 22. May 2003. Forrás: http://bme2.aut.ac.ir/~towhidkhah/MI/seminar83/Eslami/HIS%20%20%20%20EHR---%20Documents%20of%20Classmates/F.R.Eslami/HIS--In%20%20Uropean%20Countries%20--%20E-References--%20%20Eslami/min_dec_22_may_03.pdf letöltési idő: 2019.11.20.

European Comission (2019): Independent High-Level Expert Group on Artificial Intelligence: A Definition of AI: Main Capabilities and Disciplines. Brussels, 2019. 04. 08. 6 Forrás: https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines letöltési idő: 2021.03.05.

GHTF: Definition of the Terms 'Medical Device' and 'In Vitro Diagnostic (IVD) Medical Device' Study, Group 1 Final Document GHTF/SG1/N071:2012, May 16 th, 2012. Forrás: http://www.imdrf.org/docs/ghtf/final/sg1/technical-docs/ghtf-sg1-n071-2012-definition-of-terms-120516.pdf#search= letöltési idő: 2021.03.10.

Intertrust: 85% of COVID-19 tracking apps leak data (2020). Forrás: https://www.helpnetsecurity.com/2020/09/30/covid-19-tracking-apps-leak-data/ letöltési idő: 2020. 12. 01.

Koppel R, Smith S, Blythe J, Kothari V. : Workarounds to computer access in healthcare organizations: you want my password or a dead patient? Stud Health Technol Inform. 2015;208:215-20. Forrás: https://pubmed.ncbi.nlm.nih.gov/25676976/ letöltési idő: 2021.03.10.

Kruse, Clemens Scott et al., 'Cybersecurity in Healthcare: A Systematic Review of Modern Threats and Trends', Technology and Health Care 25, no. 1 (21 February 2017): 1–10, Forrás: https://doi.org/10.3233/THC-161263. letöltési idő: 2021.03.10.

Mccaffery, Fergal & Coleman, Gerry. (2007). Developing a configuration management capability model for the medical device industry. IJISCM. 2. 139-154. 10.1504/IJISCM.2007.015117. Forrás: https://www.researchgate.net/publication/220343325_Developing_a_configuration_management_capability_model_for_the_medical_device_industry letöltési idő: 2021.04.18.

Smith, Sean W. and Koppel, Ross: 'Healthcare Information Technology's Relativity Problems: A Typology of How Patients' Physical Reality, Clinicians' Mental Models, and Healthcare Information Technology Differ', Journal of the American Medical Informatics Association 21, no. 1 (January 2014): 117–31. o., Forrás: https://doi.org/10.1136/amiajnl-2012-001419. letöltési idő: 2021.03.10.

Trócsányi Sára: Egészségügyi adatok kezelése a gyakorlatban. Válogatás az adatvédelmi biztos eseteiből. Infokommunikáció és jog. 2007. 3. sz. 93-97. o. Forrás: https://infojog.hu/wp-content/uploads/pdf/200719_TrocsanyiSara.pdf letöltési idő: 2020.11.20.

Zorz, Zeljka: How to build up cybersecurity for medical devices. (IN)Secure Magazin. Reducing risk. 72-77. o. ISSUE 67. 2020 nov. Forrás: https://img2.helpnetsecurity.com/dl/insecure/INSECURE-Mag-67.pdf letöltési idő: 2021.03.15.

Welp, Annalena et al.: 'Teamwork and Clinician Burnout in Swiss Intensive Care: The Predictive Role of Workload, and Demographic and Unit Characteristics', Swiss Medical Weekly, 24 March 2019, Forrás: https://doi.org/10.4414/smw.2019.20033 letöltési idő: 2021.03.10.

WHO: eHealth. Report by the Secretariat. 7 April 2005, Forrás: https://apps.who.int/iris/handle/10665/20303 letöltési idő: 2020.11.20.