

NEMZETI KÖZSZOLGÁLATI EGYETEM
ÁLLAMTUDOMÁNYI ÉS NEMZETKÖZI TANULMÁNYOK KAR

TUDOMÁNYOS DIÁKKÖRI KONFERENCIA
2024. ÉVI TAVASZI FORDULÓ

A DIGITÁLIS EGÉSZSÉGÜGYI
INFRASTRUKTÚRA KIBERVÉDELMI
KIHÍVÁSAI: KOCKÁZATELEMZÉS AZ
INTERNETRE CSATLAKOZTATHATÓ
ORVOSI ESZKÖZÖK VÉDELMEBEN

Szerző:

Gulyás László

Kiberbiztonsági TDK

Témavezető:

Dr. Bányász Péter

egyetemi docens

Budapest

2024. 04. 10.

**A DIGITÁLIS EGÉSZSÉGÜGYI
INFRASTRUKTÚRA KIBERVÉDELMI
KIHÍVÁSAI: KOCKÁZATELEMZÉS AZ
INTERNETRE CSATLAKOZTATHATÓ
ORVOSI ESZKÖZÖK VÉDELMEBEN**

2024. 04. 10.

Tartalomjegyzék

BEVEZETÉS.....	1
A téma aktualitása.....	1
A tudományos probléma megfogalmazása	1
Kutatási célkitűzések	2
Kutatási hipotézisek megfogalmazása	2
Kutatási módszerek.....	3
1 ÁTFOGÓ ÁTTEKINTÉS AZ EGÉSZSÉGÜGYI INFRASTRUKTÚRA VÁLTOZÁSAIRÓL	3
1.1 Az egészségügyi kritikus információs infrastruktúra: Az internetre csatlakoztatható orvosi eszközök és az AI alapú rendszerek szerepe	3
1.1.1 Az internetre csatlakoztatható orvosi eszközök.....	4
1.1.2 A mesterséges intelligencia alapú rendszerek szerepe	6
1.2 A COVID-19 hatása a digitalizációra az egészségügyben	7
1.2.1 Az egészségügyi digitalizáció felgyorsulása a pandémia idején	7
1.2.2 Kihívások a digitalizálódó egészségügyben a COVID-19 idején.....	9
1.3 Kibertér jogi szabályozásai: Az adatvédelem és a kibervédelem jogi keretei az egészségügyi szektorban.....	10
1.3.1 Adatvédelem az egészségügyi szektorban.....	10
1.3.2 Kibervédelem jogi keretei	11
KÖVETKEZTETÉSEK.....	12
2 KOCKÁZATELEMZÉS A Z E G É S Z S É G Ü G Y I K R I T I K U S I N F O R M Á C I Ó S I N F R A S T R U K T Ú R Á B A N.....	12
2.1 Bevezetés a kockázatelemzésbe.....	13
2.1.1 Kockázatelemzés alapjai.....	13
2.1.2 Az elemzés jelentősége az egészségügyi szektor aspektusából.....	14
2.2 A SecRam modell alkalmazási lehetősége	14
2.3 Az Octave modell alkalmazási lehetősége	17

KÖVETKEZTETÉSEK.....	21
3 AZ IOMT ESZKÖZÖK KOCKÁZATELEMZÉSE: AZ OCTAVE MÓDSZERTAN INTEGRÁLÁSA A BIZTONSÁGBAN.....	22
KÖVETKEZTETÉSEK.....	30
ÖSSZEGZETT KÖVETKEZTETÉSEK.....	31
Új tudományos eredmények	32
FELHASZNÁLT IRODALOM.....	34
ÁBRÁK JEGYZÉKE	39
TÁBLÁZATOK JEGYZÉKE	39
RÖVIDÍTÉSEK JEGYZÉKE	39

BEVEZETÉS

A téma aktualitása

A kiberbiztonság az egészségügy területén rendkívül aktuális és kritikus téma. A kutatási témám szempontjából releváns aspektus a biztonság, különösen az internetre csatlakoztatható eszközök kontextusában, amelyek elterjedése és használata kiemelt figyelmet igényel a lehetséges támadások hatékony megelőzése érdekében. Ahogy az internetre csatlakoztatható, ebből kifolyólag egymással kommunikálni képes rendszerek egyre nagyobb teret nyernek a digitalizációs folyamat során, exponenciálisan növekvő lehetőséget nyitnak a modern orvoslás terén. Az egészségügyi ellátási folyamat gördülékenységét segítik elő, a betegek ezáltal sokkal dinamikusabb és professzionálisabb ellátásban részesülnek, viszont meglehetősen sok biztonsági rést nyit a kibertérben a használatuk, amelyekre megfelelően kell reagálni.

2019-ben amikor is a COVID-19 pandémia kirobbant, a világban elősegítette, hogy az okoseszközök robbanásszerűen elterjedjenek. Ez a folyamat a társadalmi izolációval, mint például a karantén és távolságtartás, összefüggésben állt. A világijárvány terjedésének visszaszorítása érdekében a lakosságot karanténba kellett helyezni, a szeparáció érdekében, ami megnövelte az internetes eszközök és virtuális szolgáltatások iránti igényt mind a munkavégzés, mind a közoktatás területén. Ez volt az az időszak, amikor az emberek tömegesen álltak át a távmunkára és az online oktatásra. Az infrastruktúra rövid időn belül óriási térnyerésnek örvendett. Ez a strukturális változás tartós hatást gyakorol a társadalomra, és az online eszközök használatának növekedése a mai napig érezhető, ami alátámasztja annak jelentőségét a jelenlegi és jövőbeli társadalmi dinamikákban.

A kutatás jelentősége ebben a kontextusban kétségtelen. Egyrészt a technológia rohamos fejlődéséből, másrészt a kiberfenyegetések egyre növekvő számából adódóan a témával foglalkozni kell, mivel ez incidensek nem csak az adott szektorra gyakorolhatnak hatást, hanem közvetlenül érintik a páciensek egészségét, vagy akár az állam működését is megzavarhatják. Ezáltal a kiberbiztonsági fenyegetéseket és sebezhetőségeket azonosítani kell, majd stratégiákat és módszertanokat fejleszt ki ezek kezelésére. Ezért elengedhetetlen, hogy a kutatásomban nem csupán technikai kérdésekkel kell foglalkozni, hanem etikai és jogi problémákat is érinteni, mint például a betegadatok védelmét és a hozzáférés biztosítását.

A tudományos probléma megfogalmazása

A dolgozatom tudományos problémája a fentebb körülhatárolt változásokból eredeztethető. Az internetre csatlakoztatható eszközök széles spektruma megtalálható az egészségügyi

szektorban, amelyek használatából eredően biztonsági kockázat származik. Ezzel együtt számos lehetőséget nyújt a szektor innovációjában is.

A használatukból kifolyólag meglehetősen nagy az az eszközpark, ami rendszeresítve van, például a vérnyomás- és glükózmérők, valamint pacemakerek és defibrillátorok, amelyek egymástól eltérő módon és mértékben sebezhetőek egy kibertámadás során. Ez a fajta sokszínűség megnehezíti a biztonsági szabályozást azáltal, hogy az eszközöket nem kizárólag az egészségügyi intézményekben alkalmazzák, hanem a mindennapi élet során is, ha egy pacemakerről van szó a példa kedvéért. Ez az aspektus alátámasztja azt, hogy a kiberbiztonság szorosan összefonódott a mindennapi életünkkel is, mivel akár akarva, vagy akaratlan kívül is az elektronikus eszközök kölcsönhatásában élünk.

Bár egy állam gördülékeny működése sok pontból tevődik össze, kétségtelen, hogy az egészségügy az egyik legfontosabb eleme. Egy harmadik féltől érkező behatás erre olyan súlyos változásokat is okozhat, amivel teljesen átalakíthatja az ország berendezkedését. Emiatt fontosnak tartom, hogy a szuverenitás megőrzésében a kutatásom során minden behatást gyakorló aspektust együttesen vizsgáljak, ennek megfelelően az erre épülő kockázatokat és lehetőségeket, amelyek az internetre csatlakoztatható eszközökből ered.

Kutatási célkitűzések

A dolgozatom célja, hogy reflektorfénybe helyezzem az egészségügyi szférában, azon belül az internetre csatlakoztatható orvosi eszközök kihívásait, amelyek a kibertér sokféleségéből adódó fenyegetéseket hordoznak magukban. Továbbá vizsgálni fogom, hogy milyen lehetőségeket biztosít ezen okos eszközök használata különböző egészségügyi felhasználás keretein belül.

A téma sokszínűsége miatt a kutatásom másik céljaként tekintem azon fenyegetések azonosítását, amelyek az internetre csatlakoztatható orvosi eszközökből származnak. Azonosításukat követően azon biztonsági eljárások definiálása, amelyek alkalmazásával minimalizálható a kibertérből érkező fenyegetések.

Végezetül a dolgozat részcéljaként tartom annak meghatározását, hogy milyen formában, milyen intézményi keretrendszerben alkalmazható a kockázatelemzés módszertana a szektorban.

Kutatási hipotézisek megfogalmazása

A dolgozatban a kutatás során az alábbi hipotéziseket fogalmaztam meg:

H1: A kockázatelemzés alkalmazása hatékonyan csökkentheti a kibervédelem sérülékenységet az egészségügyi szektorban

H2: Az kockázatelemzés képes javítani az információbiztonságot és minimalizálni az emberi faktor kockázatát az egészségügyi kritikus információs infrastruktúra védelmében.

H3: A kockázatelemzés módszertana jelentős mértékben járulhat hozzá az egészségügyi kibervédelem hatékonyságához

H4: A modern egészségügy teljeskörű védelmében és a megfelelő betegellátás nyújtásának céljából a kockázatelemzés, mint módszertan minden esetben alkalmazásra kell kerüljön a védelmi stratégia kidolgozása során.

Kutatási módszerek

A kutatásom alapját a kockázatelemzés módszertana képezi. Viszont a dolgozat egy átfogó és strukturális folyamatként tekinthető, amely a hazai és nemzetközi szakirodalmak alapos áttekintésével és elemzésével kezdődik. Ebben a lépésben leszűkítettem majd azonosítottam a témát.

Ezt követően a kockázatelemzés módszertanát áttekintve az Octave Allegro metódus segítségével vizsgáltam meg az internetre csatlakoztatható eszközöket. Az elemzés a gyakorlati alapokon és a szakirodalmakon alapult, ami lehetővé tette a kiberbiztonsági kockázatok azonosítását és értékelését az ágazatban. A dolgozatom végére tehát egy teljeskörű elemzést értem el, ami a releváns hazai és nemzetközi szakirodalmakon és a módszertan sajátosságain alapul.

1 ÁTFOGÓ ÁTTEKINTÉS AZ EGÉSZSÉGÜGYI INFRASTRUKTÚRA VÁLTOZÁSAIRÓL

Mindennapi életünk gördülékenységét az egészségi állapotunk megfelelő szolgálata biztosítja. Szinte természetesnek tűnhet, hogy az egészségügyi szolgáltatások mindenhol és azonnal a rendelkezésre állnak, viszont a felszín alatt számos behatás érinti, amivel nap mint nap meg kell küzdenie. A világjárványok, nemzetközi szabályozások és a legújabb technológiai vívmányok komplex hatást gyakorolva alakítják a szektor működését.¹

1.1 Az egészségügyi kritikus információs infrastruktúra: Az internetre csatlakoztatható orvosi eszközök és az AI alapú rendszerek szerepe

Az Európai Unió tendenciák² alapján a társadalmunk megállíthatatlanul halad a digitalizáció és virtuális világ irányába, ami a modernizáció kulcsa, viszont ez az exponenciálisan növekvő virtuális térnyerés a magán és az állami szektort is számottevően érinti. Ebből kifolyólag, a terület számos kiaknázatlan lehetőséget rejt magában, viszont új kihívásokat és dilemmákat vet

¹ László, „KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK”. oldal: 6-16

² Hupont és mtsai., „Next Generation Virtual Worlds”. oldalak: 13-15

fel.³ A kritikus információs infrastruktúrák közül az egészségügy szektorban a kibertér és digitalizáció forradalmi megoldásokat rejtegetnek magukban. A páciensek visszajelzése alapján az ellátási minőséget határozottan javították a digitális eszközök alkalmazása és természetesen az adatáramlást is fölgyorsították.^{4 5}

1.1.1 Az internetre csatlakoztatható orvosi eszközök

Az elmúlt évek digitális egészségügyi fejlődésben kulcsfontosságú szerepet tölt be az internetre csatlakoztatható orvosi eszközök (Internet of Medical Things, továbbiakban IoMT) területe. Ezek az eszközök úgy kínálnak forradalmi megoldásokat a modern technológia és az egészségügyi ellátás ötvözésével, hogy jelentősen javítják a betegellátás minőségét és hatékonyságát. Ugyanakkor az alkalmazásuk lehetővé teszik a betegek állapotának távoli monitorozását, az életmentő adatok valós idejű áramlását és az orvosok gyorsabb, pontosabb diagnózisait.⁶ Ezen újítások révén a betegellátás sokkal dinamikusabb és interaktívabb, támogatva ezzel a betegek jobb kezelését és a gyógyulási folyamatok felgyorsítását.

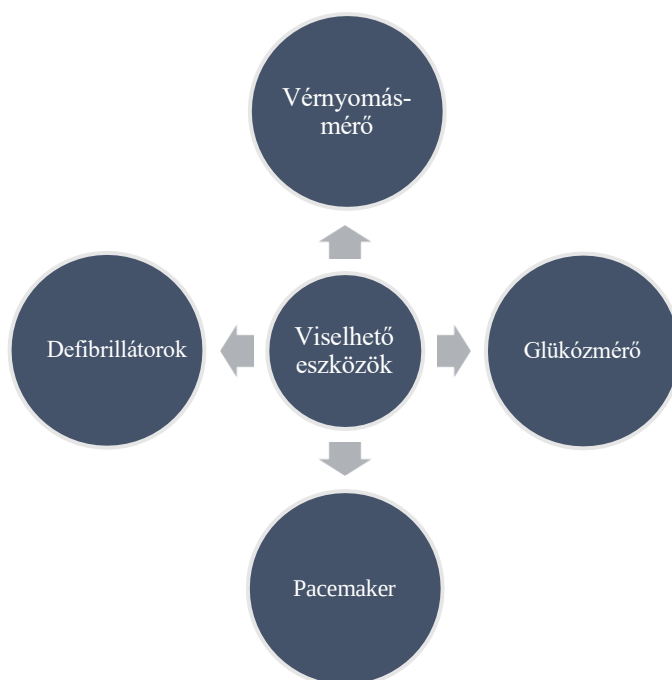
Napjainkban az IoMT eszközök, egyre fontosabb szerepet töltenek be a modern egészségügyi ellátásban. Ezek olyan eszközök, amelyek képesek a hálózatra csatlakozva adatokat gyűjteni, fogadni és továbbítani az ellátó rendszerek számára, ezzel lehetővé teszik az egészségügyi adatok valós idejű monitorozását és akkumulálását, ami jelentősen javíthatja a páciensek ellátásának minőségét és hatékonyságát. Az IoMT eszközök közé tartoznak az olyan hordható szenzorok, mint a vérnyomás- és glükózmérők, valamint az implantálható eszközök, például pacemakerok és defibrillátorok.

³ Gopal és mtsai., „Digital Transformation in Healthcare – Architectures of Present and Future Information Technologies”.

⁴ „Digital Transformation”.

⁵ „How the Digital Revolution Can Make Healthcare More Inclusive”.

⁶ Vishnu, Jino Ramson, és Jegan, „Internet of Medical Things (IoMT)-An Overview”.



1. ábra: A viselhető intelligens eszközök. (Saját szerkesztés, forrás: Ghubaish és mtsai. 2021⁷)

Ezek az eszközök folyamatos adatokat szolgáltatnak a páciens állapotáról, lehetővé téve az orvosok számára, hogy időben hozzanak döntéseket és beavatkozásokat. Ezenkívül, az IoMT fejlesztések segíthetnek a krónikus betegségek kezelésében, az egészségügyi költségek csökkentésében és a kezelési eredmények javításában.⁸ Azonban, ahogy az eszközök egyre inkább beépülnek az egészségügyi rendszerekbe, a biztonsági kockázatok is gyarapodnak, ezért az adatvédelem és a páciensek magánéletének biztosítása érdekében létfontosságú a megfelelő biztonsági intézkedések meghozatala.

<i>Előnyök</i>	<i>Hátrányok</i>
Jobb betegellátás	Biztonsági kockázatok növekedése
Valós idejű adatok áramlása	Adatvédelmi aggályok
Gyorsabb és pontosabb diagnózisok	Páciensek magánéletének kockázata
Dinamikusabb és interaktívabb ellátás	Szükségessé válik a megfelelő biztonsági intézkedések meghozatala

1. táblázat: Az intelligens eszközökkel járó előnyök és hátrányok a betegellátásban. (Saját szerkesztés, forrás: Chatterjee és mtsai. 2023⁹)

Ebből kifolyólag a fő kihívások közé tartozik az adatintegritás és a hálózati biztonság, mivel az ilyen eszközökből származó adatok illetéktelen hozzáféréseinek megakadályozása érdekében

⁷ Ghubaish és mtsai., „Recent Advances in the Internet-of-Medical-Things (IoMT) Systems Security”.

⁸ Ghubaish és mtsai.

⁹ Chatterjee és mtsai., „A systematic review and knowledge mapping on ICT-based remote and automatic COVID-19 patient monitoring and care”. 9. oldal

komplex titkosítási technikákra és megbízható hitelesítési protollokra van szükség. Egy másik kritikus aspektus a betegek adatvédelmi jogainak biztosítása. Sok IoMT eszköz által gyűjtött adat személyes és érzékeny információt tartalmazhat, ami a betegek magánéletének megsértéséhez vezethet, ha az információ illetéktelen kézbe kerül. A szolgáltatóknak biztosítaniuk kell, hogy eszközeik megfeleljenek a helyi és nemzetközi általános adatvédelmi rendeletnek (General Data Protection Regulation, továbbiakban: GDPR¹⁰). Ebből kifolyólag a megelőzés érdekében elengedhetetlen, hogy a megfelelő biztonsági követelményeknek eleget téve a rendszer mindig naprakész legyen és a személyzet is el legyen látva szakszerű információbiztonsági tudatossággal.¹¹

1.1.2 A mesterséges intelligencia alapú rendszerek szerepe

A mesterséges intelligencia (Artificial Intelligence, továbbiakban: AI¹²) az emberi fejlődés következő lépcsőfokaként¹³ jelentős változásokat hoz az egészségügyi rendszerekben is. A digitalizáció térnyerésével az AI egyre meghatározóbbá válik az egészségügyi infrastruktúrában, különösen az IoMT eszközök területén. Ezek az eszközök ma már gyakran alkalmaznak AI alapú megoldásokat az adatgyűjtés, adattovábbítás és a gyors kiértékelés érdekében. Ez a fejlesztés jelentősen felgyorsítja a diagnosztikai folyamatokat, ami kritikus jelentőségű a betegellátás hatékonysága szempontjából.

A fejlődés gyors tempója mellett az AI felhasználási területei folyamatosan bővülnek az egészségügyi szektorban, többek között a betegfigyelés, orvosi diagnosztika és szűrés, valamint az orvosi képalkotás területein. A beteg megfigyelésben az AI lehetővé teszi az állapotának folyamatos monitorozását, míg a diagnosztika és szűrés során a mesterséges intelligencia alapú rendszerek segítenek a betegségek korai felismerésében és a kezelési terv kidolgozásában. Az orvosi képalkotásban az AI segítségével a képek elemzése gyorsabb és pontosabb lehet, ami a diagnózis felállítását és a kezelési stratégiák megtervezését is jelentősen elősegíti.¹⁴

Ezáltal a mesterséges intelligencia (AI) és gépi tanulás (Machine Learning, továbbiakban: ML¹⁵) jelentős változásokat hoznak az egészségügyi terápiás folyamatokban. Az AI támogatásával működő orvosi képalkotó eszközök, mint az ultrahanggal operáló gépek,

¹⁰ 2018.05.25.-én az Európai Unió által hatályba lépő adatvédelmi és adatbiztonsági rendelet, amely védelmet nyújt a tagállamok polgárainak a személyes adataik kezelése során.

¹¹ Basatneh, Najafi, és Armstrong, „Health Sensors, Smart Home Devices, and the Internet of Medical Things”.

¹² Intelligens gépek, amelyek képesek érzékelni a környezetüket, döntéseket tudnak hozni, illetve olyan feladatokat tudnak megoldani, amihez eddig emberi képességeket igényeltek.

¹³ Taulli, „Cool AI Highlights At CES”.

¹⁴ V. Chamola et al., "A Comprehensive Review of the COVID-19 Pandemic and the Role of IoT, Drones, AI, Blockchain, and 5G in Managing its Impact", 2020. körülbelül 35-50. oldalak

¹⁵ Az AI olyan része, amelyben az adatokból tanul az algoritmus és anélkül fejleszti magát, hogy emberi behatás történne.

lehetővé teszik a betegségek gyorsabb és pontosabb felismerését, így segíti elő az eredmények javítását. Az AI-n alapuló rendszerek személyre szabott betegkezelést tesznek lehetővé, figyelembe véve a beteg egyedi jellemeit, ami csökkenti a mellékhatások kockázatát. Ezek az innovációk a betegfigyelést és értesítési rendszereket is magukban foglalják, amelyekkel elősegíthető a betegek állapotának folyamatos monitorozását és az időben történő beavatkozást. Az AI és ML alkalmazása így kulcsfontosságúvá válik a jövő egészségügyi rendszereinek fejlesztésében is, mivel a feljegyzések alapján ez a kulcs a diagnózisok pontosságának növelésére és a betegellátás minőségének javítására.¹⁶

Azonban az AI alkalmazása az egészségügyi kritikus infrastruktúrában számos kihívással is jár. Az IoMT eszközök és architektúrák felhőalapú rendszerek válaszüzeje, elérhetősége, biztonsága és felhasználó magánélete továbbra is kritikus kérdések maradtak.¹⁷ Az adatvédelem és a kiberbiztonság fokozott figyelmet igényel, hogy megvédjék az érzékeny betegadatokat és az egészségügyi infrastruktúrát. Az AI alapú rendszerek elfogultsága, a beteg és orvos közötti kommunikáció változásai, és a technológia által megkövetelt új készségek szintén fontos szempontok. Ezek mellett, a technológiai fejlesztések gyors üteme és az AI alkalmazások integrálása a meglévő egészségügyi rendszerekbe további kihívásokat jelent.¹⁸

1.2 A COVID-19 hatása a digitalizációra az egészségügyben

A COVID-19 világjárvány az egészségügyi szektort digitalizációs felgyorsulására kényszerítette, kihangsúlyozva az új generációs technikai eszközök és szoftverek jelentőségét a betegellátásban. Ezek a technológiák lehetővé tették a diagnosztika, a megelőzés és a terápia javítását, miközben csökkentették a költségeket. Azonban az egészségügyi rendszerek integrációjának hiánya és az adatbiztonsági aggodalmak továbbra is jelentős kihívásokat jelentenek mindenki számára. Az átmenet a vírus hatására felgyorsult digitalizáció felé kulcsfontosságú lehetőségeket kínál az egészségügyi kritikus infrastruktúra fejlesztésére és az AI alapú rendszerek széleskörű alkalmazására.¹⁹

1.2.1 Az egészségügyi digitalizáció felgyorsulása a pandémia idején

A 2019-ben kezdődő pandémia során az online konzultációk és a távorvoslás, más néven telemedicina területe jelentős fejlődésen ment keresztül, amit számos tényező magyaráz. Az

¹⁶ Qadri és mtsai., "The Future of Healthcare: Internet of Things - A Survey of Emerging Technologies", oldalak: 35-36.

¹⁷ Greco és mtsai., „Trends in IoT based solutions for health care”. oldalak: 346-353

¹⁸ Park és mtsai., „Identifying Challenges and Opportunities in Human-AI Collaboration in Healthcare”. oldalak: 86-88

¹⁹ Gopal, Gayatri, Suter-Crazzolara, Clemens, Toldo, Luca and Eberhardt, Werner. "Digital transformation in healthcare – architectures of present and future information technologies" *Clinical Chemistry and Laboratory Medicine (CCLM)*, vol. 57, no. 3, 2019, pp. 328-335

IoMT technológiák felhasználása lehetővé tette a klinikusok számára, hogy értékeljék, diagnosztizálják és kezeljék a betegeket anélkül, hogy fizikailag interakcióba kellene velük lépniük. Ez a gyakorlat különösen fontos volt egy olyan rendkívül fertőző betegség, mint a COVID-19 kitörése során, amikor a fizikai távolságtartás maximalizálása volt a kitűzött cél a vírus terjedésének megakadályozásához.²⁰

Időszak	Összes látogató	Telemedicina konzultációk	Jelenléti konzultációk	Új betegek	Visszatérő betegek
Pre-COVID	33976 fő	1200 fő	32776 fő	6719 fő	27257 fő
COVID	33706 fő	21251 fő	12455 fő	7509 fő	26197 fő

2. táblázat: A vírus hatása a telemedicina igénybevételére. (Saját szerkesztés, forrás: Kalwani et al. 2022²¹)

Az adatok azt mutatják, hogy a pandémia alatt a telemedicina használata exponenciálisan nőtt, ami lehetővé tette az új betegek ellátásának növelését és az egészségügyi ellátás folytonosságának fenntartását, miközben a visszatérő betegek látogatásai enyhén csökkentek. Ez a trend jelzi, hogy a pandémia alatt az egészségügyi szolgáltatások iránti igények jelentős részét távoli, digitális megoldásokkal sikerült kielégíteni, amelyek csökkentik a betegek és egészségügyi dolgozók közötti fizikai érintkezés szükségességét, ezzel redukálva a fertőzés terjedésének kockázatát.²²

A COVID-19 pandémia hatására jelentősen növekedett az egészségügyi adatok digitális megosztásának, kezelésének és tárolásának igénye, valamint a kibertámadások és adatszivárgások esélyének csökkentése. Az információs és kommunikációs technológiák elterjedése, különösen a felhőalapú megoldások és a mikroszolgáltatások, új lehetőségeket nyitottak meg az egészségügyi adatok kezelésében. A felhőszolgáltatások javították az infrastruktúra rugalmasságát, karbantarthatóságát és skálázhatóságát, lehetővé téve az orvosi adatok könnyű megosztását a különböző egészségügyi szolgáltatók között, akár nemzetközi szinten is. Az innovatív mikroszolgáltatások alkalmazása növelte a biztonságot és a magánélet védelmét, mivel korlátozták az egyes szolgáltatások által kezelt adatok hozzáférését, ezzel csökkentve a biztonsági kockázatokat.

Az egészségügyi adatok digitális kezelésének és megosztásának növekedését támogató technológiák közé sorolható a személyes egészségügyi nyilvántartások és az elektronikus egészségügyi nyilvántartások rendszere is. A személyes nyilvántartó rendszerek alapvetően

²⁰ Chamola és mtsai., „A Comprehensive Review of the COVID-19 Pandemic and the Role of IoT, Drones, AI, Blockchain, and 5G in Managing Its Impact”.

²¹ Kalwani és mtsai., „Changes in Telemedicine Use and Ambulatory Visit Volumes at a Multispecialty Cardiovascular Center during the COVID-19 Pandemic”.

²² Kalwani és mtsai.

lehetővé teszik az orvosi szenzitív információk megosztását több ellátó között, ami létfontosságú a páciens ápolásában való együttműködéshez a felek között, míg az elektronikusak a páciensek számára teszi lehetővé, hogy közvetlenül hozzáférjenek saját egészségügyi adataikhoz, javítva ezzel az egészségügyi ellátás átláthatóságát és a betegközpontúságot.²³

1.2.2 Kihívások a digitalizálódó egészségügyben a COVID-19 idején

A digitális korban a biztonság egyre nagyobb kihívást jelent, különösen a kiberbiztonságban, ahol az emberi tényező jelentős hatással van a biztonsági rések kihasználására. A COVID-19 pandémia kezdetétől számos emberi tulajdonság, mint például a félelem, kíváncsiság, információéhség, tudásvágy, ismerethiány, figyelmetlenség és kapkodás növelte a pszichológiai manipuláció, azaz a social engineering esélyét. Ezek a tulajdonságok, különösen az egészségügyben dolgozók körében, növelték a támadható felületet, mivel az alapvető hajlandóságuk az önzetlen segíteni akarás, a gyors problémamegoldás, valamint az új típusú feladatok megjelenése a szervezetben, a munkahelyi terhelés növekedésével együtt, tovább erősítette a sérülékenységet.²⁴

A pandémia alatt a támadási módszerek széles skáláját alkalmazták a kiberbűnözők, beleértve a zsarolóvírus-támadásokat, amelyek során az egészségügyi információs adatokat mindenki számára ellehetetlenítették, és ezzel kényszerítették ki a megtámadottaktól a fizetséget. Az egészségügyi dolgozókra gyakorolt nyomás, mint például a fáradtság, sietség, és a növekvő terhelés, közvetlenül összefüggésbe hozható a káros csatolmányokra történő kattintásokkal, amelyek növelték a sikeres támadások esélyét. Ezen felül, a COVID-19 alatti extrém munkakörülmények, mint a hosszú munkaórák és a speciális védőfelszerelésben végzett munka, tovább növelik a phishing támadásokra való kiszolgáltatottságot, hiszen a kimerült egészségügyi személyzet nagyobb valószínűséggel nyit meg egy kétes emailt vagy egy linket.²⁵

A támadás megelőzéséhez kulcsfontosságú a prevenció, ahol a személyzetet fel kell készíteni az új típusú támadásokra. Az Nemzeti Kibervédelmi Intézet részletes iránymutatást ad a teendőkkkel kapcsolatban, amelyek általánosak és nem csak az egészségügy specifikus problémáira vonatkoznak. Fontos, hogy adatokat elkülönített és fizikailag is leválasztható meghajtókon tárolják, a 3-2-1 biztonsági mentési elv alkalmazása, rendszeresen frissített operációs rendszerek és alkalmazások, valamint a naprakész vírusvédelmi megoldások alkalmazása. Emellett kiemelten fontos a biztonság tudatos internethasználat, különös

²³ Esposito és mtsai., „Security and privacy for cloud-based data management in the health network service chain”.

²⁴ Palicz, Bencsik, és Szócska, „Kiberbiztonság a koronavírus idején – a COVID-19 nemzetbiztonsági aspektusai”.

²⁵ Palicz és mtsai., „Magyar kórházakban előfordult zsarolóvírus támadások esetei”.

tekintettel az ismeretlen feladóktól érkező e-mailek mellékleteinek elkerülésére, valamint a hozzáférési jogok és felhasználói fiókok szigorú kezelésére. Bár a támadásokat nem mindig lehet megelőzni, de ezek a lépések jelentősen csökkentik a kiberbűnözők sikerének esélyét és segítenek a rendszer gyorsabb helyreállításában, így elkerülhető, hogy támadás esetén nemzetközi kihívássá eszkalálódjon a probléma.²⁶

A vírus idején tapasztalt kihívások rávilágítanak az emberi tényező jelentőségére a kiberbiztonság terén, és hangsúlyozzák a folyamatos oktatás, és a megfelelő munkakörülmények biztosításának szükségességét az ilyen típusú támadások elleni hatékony védekezés érdekében.

1.3 Kibertér jogi szabályozásai: Az adatvédelem és a kibervédelem jogi keretei az egészségügyi szektorban

A komplex és folyamatosan átalakuló világunkban elengedhetetlen, hogy mind mi, mind a jogi szabályozások is alkalmazkodjunk a változékony környezetünkhöz. A már tárgyalt pandémia rávilágított, hogy az emberi tényező kulcsfontosságú szerepet tölt be a kibertámadásokban, így a jogi szabályozások megfelelő értelmezése és betartása feltehetően a kulcs, a biztonságosabb egészségügyi környezet kialakításához.

1.3.1 Adatvédelem az egészségügyi szektorban

Az adatvédelem fontossága az egészségügyi szektorban különösen hangsúlyos a COVID-19 pandémia idején, amikor a gyorsan alkalmazott digitális technológiák, mint a kontakt-követési alkalmazások és a távmunka (home office) eszközök, jelentős adatvédelmi kihívásokat vetnek fel. A GDPR és általános adatvédelmi elvei, mint az arányosság, a célhoz kötöttség és az átláthatóság elvei kulcsfontosságúak a technológiák adatvédelmi törvényekkel való összhangjának biztosításában.²⁷ Ezek az elvek azt követelik meg, hogy az új vagy meglévő technológiák fejlesztői eleve beépítsenek adatvédelmi barát opciókat („privacy-by-design”), és biztosítsák, hogy ne dolgozzanak fel több személyes adatot, mint amennyi szükséges a vírus terjedésének megakadályozására, valamint, hogy az összegyűjtött adatok felhasználása átlátható legyen a felhasználók számára.²⁸ A GDPR ezenkívül megköveteli a felhasználóktól a hozzájárulást az egészségügyi adataik feldolgozásához (GDPR 9. cikk). Fontos viszont, hogy ezek az elvek nem tiltják a kormányok vagy egyéb szervezetek által jelenleg vett megfigyelési

²⁶ Palicz és mtsai., „»Pénzt Vagy Életet!« – Zsarolóvírusok Az Egészségügyi Informatikai Rendszerekben”.

²⁷ „AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/ 679 RENDELETE - (2016. április 27.) - a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/ 46/ EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)”.

²⁸ Newlands és mtsai., „Innovation under Pressure”.

intézkedéseket, hanem inkább biztosítják az adatok helyes kezelését a megváltozott körülmények között.

Az adatvédelem és a kiberbiztonság szoros összefüggést mutatnak, mivel mindkettő alapvető a biztonságos digitális környezet fenntartásához. A gyors digitalizáció és az online munkavégzés elterjedése fokozta a kiberfenyegetések kockázatát, különösen a kis- és középvállalkozások, valamint a kritikus infrastruktúrák, mint az egészségügyi intézmények, energiaellátó hálózatok és közszolgáltatások számára, ezért az EU-nak és tagállamainak sürgősen cselekedniük kellett a kibervédelem megerősítése céljából. Ez magában foglalja a kiberbiztonsági szakértelem és tudatosság növelését, valamint a kiberbiztonsági eszközök és irányelvek fejlesztését.²⁹

A kiberbiztonság nem csak technológiai kérdés, hanem alapvető emberi jogok és demokrácia védelmének eszköze is. A biztonságos kommunikációs csatornák és adatok biztosítása kulcsfontosságú a magánélet védelmében és a demokratikus folyamatok, például a választások integritásának megőrzésében. Az EU-nak folytatnia kell a kiberhigiénia és a kibertudatosság növelését célzó kezdeményezéseket, valamint elő kell segítenie a kiberbiztonsági ipar fejlődését, azáltal, hogy támogatja a szakértelem fejlesztését és a kiberbiztonsági megoldások bevezetését.³⁰

1.3.2 Kibervédelem jogi keretei

A kibervédelem jogi keretei az egészségügyben különösen fontosak, mivel az egészségügyi adatok és rendszerek védelme alapvető a betegek biztonsága és a szolgáltatások gördülékeny működése szempontjából. A kibertámadások elleni jogi védelem az egészségügyben azáltal valósul meg, hogy a szabályozások kötelezővé teszik az egészségügyi szervezetek számára a megfelelő kiberbiztonsági intézkedések alkalmazását. A kiberbiztonság jogi kerete az Európai Unióban jelentős átalakuláson ment keresztül az NIS 2 irányelv³¹ elfogadásával, amely kiterjeszti és megerősíti az előző NIS irányelv kereteit. Az új irányelv széles körben szabályozza azokat az intézkedéseket, amelyek az egészségügyi szektorban is kulcsfontosságúak a kibertámadások elleni védekezésben.³²

Az egészségügyi szervezetek, nemzetbiztonsági szakszervezetek felelőssége a kiberbiztonság terén megkérdőjelezhetetlen, tekintettel arra, hogy az egészségügyi adatok különösen érzékenyek és egyre vonzóbb célpontot jelentenek sebezhetőségük miatt a kiberbűnözők

²⁹ Tasheva, „Cybersecurity Post-COVID-19”.

³⁰ Kovács, *Kiberbiztonság és -stratégia*. oldalak: 25.

³¹ 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) (EGT-vonatkozású szöveg)

³² Kosutic, „What Is NIS2?”

számára. Az NIS 2 irányelv értelmében az "esszenciális entitások" közé sorolt egészségügyi szolgáltatóknak meg kell felelniük megszorított biztonsági és jelentésadási követelményeknek, hogy megvédjék az adatokat és az infrastruktúrát a kiberfenyegetésekkel szemben.³³ A jogi keret továbbá előírja, hogy az egészségügyi szektorban működő szervezeteknek proaktívan kell eljárniuk a kiberbiztonsági kockázatok kezelésében, beleértve a megelőző intézkedéseket, az incidensjelentést és az információmegosztást más releváns szervezetekkel. Ezen intézkedések betartása és betartatása nem csak a kiberbiztonsági események hatásának minimalizálására irányul, hanem a gyors reagálás és a helyreállítás elősegítésére is, amely létfontosságú az egészségügyi ellátás folytonossága szempontjából.³⁴

KÖVETKEZTETÉSEK

A fejezetben vizsgáltam az egészségügyi infrastruktúra változásait, specifikusabban a fejlődését és digitalizációját, az IoMT eszközök és az AI alapú rendszerek szerepét, valamint a COVID-19 pandémia digitalizációra gyakorolt hatását. Az exponenciálisan transzformálódó trendek és fejlődés igazolja a kutatások relevanciáját. Ezek az eszközök, mint a vérnyomásmérők, pacemakerek, valamint a mesterséges intelligencia és gépi tanulás alkalmazása, új dimenziókat nyitnak meg a diagnosztikában, a betegmonitorozásban és a terápiás beavatkozásokban, ami alátámasztja a kutatási szakterület multidiszciplináris megközelítésének fontosságát. Ez alapján igazoltam, hogy a betegellátás minőségét, hatékonyságát és elérhetőségét javítják ezen innovációk, azonban bevezetésük során kiemelt figyelmet kell fordítani a kiberbiztonsági kockázatok kezelésére is.

2 KOCKÁZATELEMZÉS AZ EGÉSZSÉGÜGYI KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁBAN

A létfontosságú rendszerelemek működéséhez kulcsfontosságúak a megfelelő vezetői döntések. Már az operatív szinttől egészen a stratégiai szintig terjedően előzetes elemzést kell végrehajtani, hogy számításba lehessen venni a potenciális hatást és eredményt az adott szervezet, intézmény működésére. Tekintettel arra, hogy az infrastruktúra kiszolgálja a polgári lakosság szükségleteit, ezért a mindegyik döntés jelentős hatást gyakorol minden tagjára.³⁵ Ebből kifolyólag kijelenthető, hogy mint személyes életünkben, úgy a kritikus rendszerek működésében is nélkülözhetetlen a kockázatelemzés.

³³ Ganzer, „Understanding EU’s NIS2 Cybersecurity Directive”.

³⁴ PECB, „A Comprehensive Guide”.

³⁵ Kiss Adrienn, „A kockázatelemzés rejtett számai”.

2.1 Bevezetés a kockázatelemzésbe

A kockázat³⁶ fogalma egyidős az emberiséggel³⁷, mivel alapvetően a döntéshozatal előtt – akár tudatosan, akár tudatalatt – az egyének mérlegelték a lehetséges scenáriókat. Ezen események valószínűség, hogy be fog-e következni tekintettel, hogy a többszörösen összetett és komplex világ, amiben élünk számtalan másik elemmel áll kölcsönös függésben.³⁸ Minden szervezetnek célja, hogy fenntartsák a befolyásolástól mentes működésüket és megőrizzék a szuverenitásukat azáltal, hogy időben felismerik az negatív végkifejletet és csökkentse az azok bekövetkezésének lehetőségét. Ezt a vezetők, döntéshozók kockázatelemzéssel érhetik el.

2.1.1 Kockázatelemzés alapjai

Ez a kifejezés valójában több tényezőből tevődik össze, többek között akár a különböző eseményekből fakadó veszélyek vagy potenciális károk időben történő felismeréséből és elemzéséből áll, amelyek egy szervezetnél a döntési folyamat részét képezik. Az elemzés lényege, hogy a vállalatok vagy szervezetek működése során felmerülő kockázatokat proaktívan kezeljük, mégpedig úgy, hogy csökkentjük a fenyegetések bekövetkezésének esélyét vagy az általuk okozott kár mértékét, mivel sajnos az esetek túlnyomó többségében a káresetet nem lehet elkerülni.³⁹

A kockázatkezelés folyamatában többféle lépésből tevődik össze, mint például a kockázatok azonosítása, értékelése és azok rangsorolása, majd egy olyan stratégia kidolgozása, amellyel minimalizálható a bekövetkezés.⁴⁰ Több módszertan is létezik, de a közös bennük, hogy standardizált keretrendszerre támaszkodnak szerkezeti felépítésükben, például a felmérésre a Nemzetközi Elektrotechnikai Bizottság irányelve: IEC 31010:2019 (International Electrotechnical Commission, továbbiakban: IEC⁴¹) és a kezelésre a Nemzetközi Szabványügyi Szervezet irányelve: ISO 31000:2018 (International Organization for Standardization, továbbiakban ISO⁴²) szolgál. A dolgozatban alkalmazott modellek - köztük a működési szempontból kritikus veszélyek, eszközök és sebezhetőség értékelése (Operationally Critical

³⁶ A kockázatokat biztonságot veszélyeztető tényezőként határozhatjuk meg, amelyek egy adott közösséget érő, negatív hatású, konkretizálható kimenetelű esemény eshetőségét jelentik. Ilyen esemény bekövetkeztekor a közösségi vagy nemzeti érdekek sérülhetnek, veszteségek keletkezhetnek. A kockázatnak van egy passzív (kedvezőtlen eshetőség) és egy aktív (kockázatos lehetőség) dimenziója is. „Kockázat - Közzszolgálati Online Lexikon”.

³⁷ „Garaczi Imre: Kockázati modellek és társadalmi mozgások”.

³⁸ Kiss Adrienn, „A kockázatelemzés rejtett számai”.

³⁹ Tünde, „Leggyakrabban használt kockázatkezelési modellek összehasonlítása”.

⁴⁰ Jain, „Mi az a kockázatelemzés”.

⁴¹ Az IEC egy nemzetközi szabványügyi szervezet, amely az elektrotechnika és elektronika területén dolgoz ki és ad ki szabványokat.

⁴² Az ISO egy független, nem kormányzati nemzetközi szervezet, amely szabványokat dolgoz ki és ad ki különböző iparágakban és tevékenységekben, hogy elősegítse a minőséget, biztonságot és hatékonyságot.

Threat, Asset, and Vulnerability Evaluation, továbbiakban: OCTAVE), valamint a biztonsági kockázatértékelési módszertan (Security Risk Assessment Methodology, továbbiakban: SecRam) - segítenek a vállalatoknak abban, hogy a különböző fenyegetések és veszélyek kockázatait tudatosan kezeljék, illetve, hogy az ellenük való hatékony védekezés megvalósítható legyen.^{43 44} Az OCTAVE egy keretrendszer az információbiztonsági kockázatok azonosítására és kezelésére, mely lehetővé teszi, hogy felderítsék azokat az információs eszközöket, amelyek fontosak a szervezet küldetéséhez, az ezeket fenyegető veszélyeket és az eszközöket fenyegető sebezhetőségeket. Továbbá a SecRam modell lényege, hogy azonosítja a kiberbiztonsági kockázatokat, forrásait és azt, hogyan lehet őket egy elfogadható szintre csökkenteni.

Egy-egy ilyen támadás esetén akár felbecsülhetetlen károk is keletkezhetnek, amelyek következtében az egészségügyi beteg- illetve dolgozói adatok sérülhetnek, a rendszerek huzamosabb időre leállhatnak, ami kritikus kockázathoz vezet. Ez viszont arra enged következtetni, hogy az egységes és átfogó kockázatkezelési modellek használata a 21. századi modern ellátásban esszenciális.

2.1.2 Az elemzés jelentősége az egészségügyi szektor aspektusából

A szektor jövőjét garantálni csak úgy lehet, hogy minden kihívás megfelelően és időben van kezelve. Fel kell ismerni, hogy ebben a rendkívül összetett rendszerben sokféle potenciális veszély és kockázat lapul és a legkisebb is már beláthatatlan károkat képes generálni, illetve könnyen eszkalálódni, ha nem kezelik megfelelően. Ezen felül a hatékony kockázatkezelés egy másik kulcsfontosságú részhalmaza a meglévő ellenőrzési intézkedések értékelésének, hogy meghatározhassák azok hatékonyságát a kockázatok csökkentésében, mivel az intézményeknek meghatározott időközönként felül kell vizsgálniuk és aktualizálniuk kell a kockázatkezelési terveiket, hogy reagálni tudjanak a változó körülményekre és fenntartható biztonsági kultúrát alakíthassanak ki.⁴⁵

Az eredmény maximalizálásához kockázatelemzési modell, vagy modellek alkalmazása a legmegfelelőbb eszköz. A dolgozatban a SecRam és az Octave módszereken keresztül lesz a téma részletesebben megvizsgálva.

2.2 A SecRam modell alkalmazási lehetősége

Az adatintegritás, a hozzáférhetőség és a bizalmas információk, amellyel a modern egészségügy meglehetősen függésben áll. A fenyegetésekre válaszul alkalmazzák SecRAM-ot, amely

⁴³ „OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) - CIO Wiki”.

⁴⁴ „IT Security Risk Assessment Methodology”.

⁴⁵ Pascarella és mtsai., „Risk Analysis in Healthcare Organizations”.

eredetileg a légiforgalmi irányítás kontextusában jött létre, alapjáraton egy ISO 27005 alapú kockázatelemzési módszertan, ami arra lett kifejlesztve, hogy meghatározza a kiberbiztonsági kockázatok kontextusát, hatókörét és értékelési kritériumait. Az egészségügyi kritikus információs szektorban alkalmazva a SecRAM módszertan segít azonosítani a kritikus egészségügyi adatokat és eszközöket, valamint azokat a támogató eszközöket, amelyek ezek védelmében állnak.⁴⁶ Fontos kiemelni, hogy a prioritások között az adatok és eszközök állnak az első helyen.



2. ábra A SecRam általános alkalmazásának folyamata. (Saját szerkesztés, forrás: Asgari, Haines, és Waller.⁴⁷)

Az alkalmazási folyamatban a SecRam módszertan felbontható több lépésre. Első lépésben az egészségügyi alkalmazásokban a kockázatkezelési kontextust kell meghatározni és a vizsgálati területet, például az IoMT képző eszközök és AI-al működő eszközök kibervédelme a digitalizált egészségügyben. A folyamat magában foglalja az egészségügyi rendszer határainak kijelölését és a kapcsolódó rendszerektől való függőségek azonosítását. Ebben a szakaszban kritikus fontosságú a rendszer által kezelt adatok és szolgáltatások – mint prioritás – valamint az ezeket támogató fizikai eszközök és infrastruktúrák pontos azonosítása.⁴⁸

Az intézmény számára fontos, hogy azonosítsák a fenyegetéseket és a lehetséges támadási forgatókönyveket, ezek mellett a vagyont képző tárgyak, adatok teljeskörű beazonosítása. Ezzel

⁴⁶ Asgari, Haines, és Waller, „Security Risk Assessment and Risk Treatment for Integrated Modular Communication”.

⁴⁷ Asgari, Haines, és Waller.

⁴⁸ Asgari, Haines, és Rysavy, „Identification of Threats and Security Risk Assessments for Recursive Internet Architecture”.

lehetővé tehető, hogy felmérje, melyek azok a biztonsági rések és támadási vektorok, amik kockázatot jelenthetnek a rendszer integritására vagy akár a működésére. Ezt követően az egyes támadási forgatókönyvek hatásának értékelése révén meghatározható, hogy azok mennyire befolyásolják az adatok bizalmas jellegét, sértetlenségét és hozzáférhetőségét.⁴⁹

Ahogy az ábra is mutatja, a fenyegetések valószínűségének értékelése tovább finomítja a kockázati képet, lehetővé téve a kibervédelmi csapat számára, hogy megértsék, milyen gyakran fordulhatnak elő bizonyos támadások és milyen valószínűséggel érik el céljaikat. Ennek alapján, a SecRAM módszertan követi a kockázati szintek megállapítását, figyelembe véve a fenyegetések hatását és gyakoriságát.⁵⁰

A következő lépés a biztonsági kockázatok szisztematikus megközelítése és kategorizálása. Az azonosított kockázati szintű fenyegetések kezelése érdekében a SecRAM egy átfogó megközelítést biztosít a biztonsági ellenőrzések kiválasztásához és implementálásához. Az egészségügyi rendszerben ez magában foglalhatja az adatvédelmi irányelvek megerősítését, a hozzáférés-vezérlési mechanizmusok bevezetését, és a kommunikációs protokollok titkosítását és számos más metódus alkalmazását. Utolsó lépésekben a módszertan kockázati kezelési stratégiák validálása és a védelmi intézkedések hatékonyságának ellenőrzésére hívja fel a figyelmet. Ez magában foglalja az új biztonsági protokollok és gyakorlatok tesztelését vagy a régi aktualizálását, valamint az érintett személyzet kiképzését a kiberfenyegetésekkel szembeni hatékony reagálás érdekében, illetve megfelelő információbiztonsági tudatosságra oktatását.⁵¹ Összességében a modell használata teljesen átfogó megközelítést kínál az alkalmazása során a felhasználónak, így egy teljes képet nyújt a rendszer minden aspektusáról, a technikaitól kezdve az üzemeltetésig, amivel garantálható a sebezhetőségek időben történő felismerése. További előnyt jelent, hogy a modell elősegíti a jobb kommunikációt és megértést a különböző érdekelt felek között. Ezek által a felmerülő kockázatok és azok hatásai világosabb képet biztosítanak a döntéshozóknak, elősegítve a megfelelőbb információkon alapuló döntéshozatalt és hatékonyabb stratégia kidolgozását.

Nem szabad elismerni a tény mellett, hogy a felhasználásában nehézségek is adódhatnak. Egy teljeskörű kockázatelemzés bonyolult lehet, jelentős időt, szaktudást és erőforrást vehet igénybe, amelyek nem mindig állnak teljes egészében rendelkezésre minden szervezetben. Miközben a szakértői vélemény elengedhetetlen a kockázatok, hatások és végrehajtási folyamatok megítélésében, akár torzításokhoz vezethet. Mivel egyik modell sem kínál

⁴⁹ Ekelhart, Fenz, és Neubauer, „AURUM”.

⁵⁰ Korombel és Tworek, „Qualitative risk analysis as a stage of risk management in investment projects”.

⁵¹ Pascarella és mtsai., „Risk Analysis in Healthcare Organizations”.

tökéletesen átfogó rálátást, ezért fontos, hogy alkalmazásuk során fel kell ismerni a modell hiányosságait is.^{52 53}

2.3 Az Octave modell alkalmazási lehetősége

A működési szempontból kritikus veszélyek, eszközök és sebezhetőség értékelése egy olyan létfontosságú szektorban, mint az egészségügy esszenciális. A dolgozatban a másik kockázatelemzési modell, az Octave stratégia kerül alkalmazásra, amit az információbiztonsági kockázatok kezelésére dolgoztak ki. A célja, hogy az alkalmazó szervezet megértse az infrastruktúrájukhoz szükséges működésüknek az igényét azáltal, hogy összpontosít a kockázatalpú értékelésre. A vizsgálati folyamat többek között magába foglalja, az intézményi technológiai kérdések áttekintését, valamint azt, hogy hogyan használják az emberek a szervezetük számítástechnikai infrastruktúráját mindennapi munkájuk során.⁵⁴ A modellben elkülöníthetünk két alkalmazási területet.

Az első kategória az Octave-S, amelyet kis és közepes vállalatokra fejlesztettek ki, mivel ezek a vállalatok nem gyakorolnak bonyolult, formális adatgyűjtési tevékenységet. Viszont az egészségügy, komplexitásából, összetettségéből, valamint egy állam működésében létfontosságú szerepéből adódóan kritikus infrastruktúrának deklarálható.⁵⁵ Ebből adódóan a dolgozatban a másik kategória kerül alkalmazásra, amit Octave Allego-nak nevez a szakirodalom, viszont a dolgozatban csak Octave-ként lesz megnevezve. Ez a módszertan egy részletesebb, mégis átlátható és kezelhető megközelítést nyújt a vizsgálódás során. Az IoMT eszközök védelmére összpontosít úgy, hogy figyelembe veszi az információs eszközök használatát és a fenyegetések bekövetkezésének a valószínűségét.⁵⁶

⁵² Marotta és mtsai., „Applying the SecRAM Methodology in a CLOUD-Based ATM Environment”.

⁵³ Asgari, Haines, és Rysavy, „Identification of Threats and Security Risk Assessments for Recursive Internet Architecture”.

⁵⁴ „Introduction to the OCTAVE Approach”.

⁵⁵ „BM Országos Katasztrófavédelmi Főigazgatóság”.

⁵⁶ „Managing Information Security Risks”.



3. ábra: Az Octave általános alkalmazásának folyamata. (Saját szerkesztés, forrás: Vijayanto, Devyana, és Wang ⁵⁷)

Ahogy a mellékelt ábrán demonstrálja, a modell alkalmazása 8 fő lépésből áll. Metódusában és elvében hasonló, mint a SecRam, viszont az Octave egy sokkal átfogóbb és komplexebb elemzési lehelőseget ad a szervezet számára. Egy átfogó felmérés sokkal több időt és energiát igényel, de ezzel együtt az eredmény is sokkal átfogóbb lesz, ami bőven kifizetődő.

A folyamat első lépésében a kockázatkritériumok meghatározása történik. Ebben a fázisban az egészségügyi szervezet értékeli majd kategorizálja, hogy milyen behatások tekinthetők súlyos-, közepes-, vagy alacsony intenzitásúnak az információs eszközökre nézve, például pénzügyi veszteségek, a hírnév csorbulása, jogi következményekkel járó esetek vagy akár a működési hatékonyság csökkenését előidéző károk.⁵⁸ Ez a szakasz tekinthető tehát a legfontosabbnak, mivel a megfelelő kategorizálás hiányából fakadóan egy torz eredmény születne a kockázatelemzés eredményeként. Az információs vagyonprofil készítése során meg kell határozni azokat az információs vagyonelemeket, amelyek kritikusak a szektor működését tekintve. Ezt követően az információs vagyonokhoz kapcsolódó biztonsági követelményeket kell meghatározni, amelyek figyelembe veszik a vagyon értékét, valamint az adatok épségét és hozzáférhetőségét. Majd a következő lépésben lokalizálni, hogy hol és mikor használják ezeket, milyen módon kerülnek szállításra, és hol kerülnek feldolgozásra ezek az információk. Ez alatt

⁵⁷ Vijayanto, Devyana, és Wang, „Enhancing Is Risk Assessment through Using Combination Vector Matrix and Octave Methods”.

⁵⁸ „Lean Risk Assessment Based on OCTAVE Allegro – Compass Security Blog”.

értendő a fizikai helyszínek, mint például irodák vagy adatközpontok, valamint a hálózati infrastruktúrák és az alkalmazások.⁵⁹

Az aggodalomra okot adó területek azonosítása során a szervezetnek fel kell ismernie és dokumentálnia kell azokat a területeket, ahol az információs vagyont fenyegethetik olyan potenciális biztonsági rések, ahol a biztonsági intézkedések hiányosak vagy elégtelenek. Ezt követően fenyegetési forgatókönyveket kell készíteni, ahol reprezentálható több olyan szcenárió, hogy hogyan férhetnek hozzá illetéktelen személyek vagy csoportok az egészségügyi információs vagyonhoz. Nélkülözhetetlennek tekinthető ez a módszer, mivel segít megérteni a lehetséges biztonsági réseket és azokat a módszereket, amelyekkel a támadók kihasználhatják ezeket. A szervezet identifikálja ezt követően a meghatározott fenyegetések és sebezhetőségek kombinációjából adódó kockázatokat majd dokumentálja, hogy melyik lehetőség jelent a legnagyobb fenyegetést számára.

A kockázatelemzési folyamat az utolsó két lépésben érkezik el egy kulcsfontosságú állomáshoz, ahol az egyes fenyegetéseket és sebezhetőségeket a már meghatározott kockázatmérési kritériumok alapján végül sorrendbe lehet állítani, figyelembe véve a bekövetkezésük valószínűségét és potenciális hatásukat. A cél az, hogy az elemzés egyértelmű és mérhető módon reprezentálja a kockázatot, ami lehetővé teszi a vezetői és döntéshozói réteg számára, hogy szakszerű döntéseket hozzon, emellett a kommunikációt is megkönnyítse.

A folyamat utolsó lépésében már a stratégiai szakaszba érkezünk. A folyamat végén már csak ki kell választani a megfelelő kockázatsökkentő stratégiákat és enyhítési intézkedéseket a kiemelt kockázatok bekövetkezése esetén a kezelésére. Itt a kiválasztott enyhítési módszerek lehetnek különbözőek, annak függvényében, hogy az adott fenyegetést milyen mértékben kívánják csökkenteni, és nagyságrendben milyen erőforrások állnak rendelkezésre. Nem utolsó sorban, számításba kell venni a kockázattűrési szintet is. Az enyhítési stratégiák kidolgozása során kiemelt figyelmet kell fordítani a költség-haszon elemzésre, biztosítva, hogy a kiválasztott intézkedések gazdaságilag is indokoltak és fenntarthatóak legyenek az szervezet számára.⁶⁰

A folyamat végére körvonalazódik, hogy az Octave egy keretrendszer kínál a kockázatelemző számára, ezzel együtt kristálytiszta képet ad az elemzési folyamatok végére. Ahogy láthatjuk a stratégiai szint a piramis teteje, mivel a jól körül határtolt és beazonosított értékekre csak egy fenntartható stratégiával lehet létjogosultságot garantálni. Ezért hát nincs is más dolga a

⁵⁹ Prajanti és Ramli, „A Proposed Framework for Ranking Critical Information Assets in Information Security Risk Assessment Using the OCTAVE Allegro Method with Decision Support System Methods”.

⁶⁰ Caralli és mtsai., „Introducing OCTAVE Allegro”.

szervezet vezetőinek, döntéshozóinak csak annyi, hogy megismerjék az ellenségüket és szándékait, illetve ezzel együtt a saját képességüket is felmérjék. Ezzel a tudással száz kihívásból mind a százszor pozitív végkimenetelre számíthat. Azonban, ha csak saját képességeit ismeri, az arányok egyenlőek lesznek és amennyiben meg egyiket sem ismeri, akkor soha nem számíthat pozitív eseményekre.⁶¹ Tehát, hogyha a kockázatokat alaposan elemzik és priorizálják, majd hatékony enyhítési stratégiákat dolgoznak ki, az egészségügyben látványosan javíthatják védelmi képességüket a kiberfenyegetésekkel szemben, miközben biztosítják, hogy erőforrásaikat a legkritikusabb területeken használják fel. Az itt meghozott döntések jelentősen befolyásolják az szervezet kockázatkezelési stratégiájának hatékonyságát és hosszú távú sikerét.⁶²

	OCTAVE	SecRam
Hatékony	x	
Gyors	x	
Cselekvésre kész	x	
Átfogó	x	
Leegyszerűsített		x

3. táblázat: Az Octave és SecRam módszertan tulajdonságainak összehasonlítása. (Saját szerkesztés, forrás: Praveen⁶³)

Az elhangzottak alapján, az Octave elsődleges előnye, hogy a szervezeti célokat az információs kockázatértékeléssel és sebezhetőségkezeléssel összekapcsolja, ami segít a megérteni és megfelelően kezelni az információs biztonsági kockázatokat az egészségügy működésében. A módszertan kiemeli az ismételhető módszereket, amelyek integrálhatóak a szektor folyamatos kockázatkezelési programjaiba, biztosítva az eredmények konzisztenciáját rendszeren belül. Magyarul effektív és gyors, emellett időt takarít meg azzal, hogy csökkenti a felesleges dokumentációt, és megbízható eszközközpontú nézetet nyújt az elemzőknek, valamint a módszer nagymértékű testreszabhatósága lehetővé teszi, hogy az aktuális szükségleteikhez igazítsák.⁶⁴

Fontos azonban megemlíteni, hogy az előnyei akár hátrányt is jelenthetnek más módszertanokhoz képest, például a túlzott egyszerűsítése és az alacsonyabb képzési és tudásigények csökkentése lehet, hogy nem nyújt elegendő mélységet és részletességet az egészségügyi szektor komplexitásának kezeléséhez, vagy a sebezhetőségi tesztelés hiánya

⁶¹ „Szun-Ce - A Háború Művészete PDF | PDF”.

⁶² „Managing Information Security Risks”.

⁶³ Praveen, „The Benefits of Utilizing the OCTAVE Threat Model”.

⁶⁴ Praveen.

jelentős aggályt vethet fel az egészségügyi intézmények számára, ahol a sebezhetőségek pontos és alapos azonosítása létfontosságú az érzékeny betegadatok védelme és a rendszerek integritásának megőrzése érdekében. Ez azt eredményezi, hogy lesznek kritikus biztonsági részek, amelyek felismeretlenül fognak maradni, ez viszont növeli az infrastruktúra támadhatóságának felületét. Ezek mellett az Octave nem feltétlenül szolgálja ki a nemzetközi szabályozások által lefektetett normákat, például a GDPR, ami megnehezítheti az egészségügyi intézmények számára, hogy biztosítsák szabályozási kötelezettségeik teljesítését.⁶⁵

Következtetésképpen, az Octave módszertan alkalmazása jelentős kihívásokat és korlátokat jelenthet a jövő egészségügyi kritikus információs szektorában. Miközben az egyszerűsített folyamat és az alacsonyabb erőforrás-igények előnyök lehetnek bizonyos aspektusokban, de az infrastruktúra komplex és folyamatosan változó igényei miatt egy módszertan alkalmazása nem tudja maximálisan biztosítani a kellő mélységet és specifikált a hatékony kockázatelemzéshez.⁶⁶ Ezért az ágazatban a kibertámadások tendenciája miatt fokozott figyelmet kell fordítani a védekezésre, és arra, hogy az egészségügyi intézmények személyzeti is biztonság tudatosak legyenek. Az egészségügyi adatok védelme közös fellépést, intézményi és személyi edukációt, valamint az adattudatosság erősítését igényli a megfelelő adatvédelmi és kiberbiztonsági intézkedések meghozatala mellett, mivel a támadások száma növekszik, és egyre több a zsarolóvírus, az adatlopás, valamint az ellátás folytonosságát veszélyeztető események. Ezentúl naponta több tízezer érzékeny adat keletkezik, amelyek védelme nélkülözhetetlen a betegek és a személyzet biztonságának megőrzése érdekében. Ezért szükség van egy jó stratégiára, mivel az nem csak a támadások megakadályozására összpontosít, hanem hatékony válaszokat is kínál a bekövetkezett eseményekre, ezáltal növelve a hatékonyságot és biztonságot a szektorban.^{67 68}

KÖVETKEZTETÉSEK

A fejezetben megvizsgáltam az egészségügyi infrastruktúra védelmének jelentőségét az egyre növekvő kibervédelmi kihívások és fenyegetések fényében. Továbbá, a kockázatelemzés fontosságát, két módszertan - a SecRam és az Octave – alkalmazását a szektor kockázatainak kezelésére. A leírtak szorosan kölcsönhatásba állnak az előző fejezetben megálapítottakkal, hiszen a megfelelő vezetői döntések, amelyek a kockázatelemzés eredményein alapulnak,

⁶⁵ Caralli és mtsai., „Introducing OCTAVE Allegro”.

⁶⁶ Putri és Riadi, „Analysis of Risk Management on Learning Management System Using Octave Allegro Framework”.

⁶⁷ „Stratégiai megállapodás a hazai egészségügy kiberbiztonságának javítása érdekében | Nemzeti Kibervédelmi Intézet”.

⁶⁸ PricewaterhouseCoopers, „Kiberbiztonság és adatvédelem”.

elengedhetetlenek az egészségügyi infrastruktúra hatékony védelméhez. Ebből kifolyólag megállapítható a kockázatelemzés interdiszciplináris jellege, ami magában foglalja, többek között az informatikai biztonságot, az egészségügyi tudományokat és a jogi előírásokat is. Arra a következtetésre lehet jutni ebből, hogy az egészségügy szuverenitásában aktív szerepet játszik a kockázatelemzés módszertana.

3 AZ IOMT ESZKÖZÖK KOCKÁZATELEMZÉSE: AZ OCTAVE MÓDSZERTAN INTEGRÁLÁSA A BIZTONSÁGBAN

Az előző fejezetekben áttekintett egészségügy digitális átalakulásából egyre nagyobb létjogosultságot nyerő IoMT eszközök védelme megkérdőjelezhetetlen. A növekvő igényük és jelentőségük az egészségügyi ellátásban új kérdéseket vetnek fel, viszont a válasz komplex. Figyelemmel kell kísérni, a korábban már említett a digitális átalakulás előnyeit és kockázatait, valamint az adatvédelmi és kibervédelmi jogi kereteket, mivel az elemek minimális egymásra gyakorolt hatása meglehetősen befolyásolja a kihívásokra adott választ. Az első és második fejezetben elhangzottak alátámasztják a jelentőségét annak, hogy igen is szükség van a folyamatosan megújuló és dinamikus formázható világban egy olyan stratégiára, ami alkalmazkodik a megváltozott nemzetközi környezethez.⁶⁹ Ezért indokolt a szükségessége, hogy részletesen foglalkozzunk az IoMT eszközök átfogó kockázatelemzésével, az Octave módszertant alkalmazva.

A metodológia meglehetősen fontos a szektor kiberbiztonsági kihívásainak kezelésében, mivel alkalmazásával azonosítható, értékelhető és csökkenthető a kiberfenyegetések által okozott kockázatok.⁷⁰ Ezt követően részletes elemzésre kerül, hogyan is vehető igénybe az IoMT eszközök kritikus infrastruktúrában való védelmére, figyelembe véve az egyedi operációs környezeteket és a kiberbiztonsági fenyegetések sajátos természetét.

1. lépés

A folyamat ezen lépésében körül kell határozni a kockázatomérési dimenziókat, típusait annak érdekében, hogy az eredmény átfogó legyen és ne torzuljon az elemzés során. Ez a lépés a keretrendszer alapja.⁷¹ Az első két fejezetben megállapítottak alapján a 4. táblázatot fogom használni, amiben 4 fő befolyásoló irányt kell megkülönböztetni, amelyek az adatvédelem,

⁶⁹ Kft, „1163/2020. (IV. 21.) Korm. Határozat Magyarország Nemzeti Biztonsági Stratégiájáról - Hatályos Jogszabályok Gyűjteménye”.

⁷⁰ Pascarella és mtsai., „Risk Analysis in Healthcare Organizations”.

⁷¹ Caralli és mtsai., „Introducing OCTAVE Allegro”.

rendszer rendelkezésre állás, sebezhetőségek kezelése és legvégül támadási vektorok tényező szerepel.

Kritérium	Leírás	Fontosság
Adatvédelem	A páciensek egészségügyi és személyes adatainak védelme.	Magas
Rendszer rendelkezésre állása	A pacemakerek állandó és megbízható működésének biztosítása.	Kritikus
Sebezhetőségek kezelése	Az eszközök sebezhetőségeinek azonosítása és orvoslása.	Magas
Támadási vektorok	Lehetséges külső és belső támadási források azonosítása.	Magas

4. táblázat: Kockázatomérési kritériumok (Saját szerkesztés, forrás: Zaldivar és mtsai.⁷²)

A mért kritériumok fontossága indokolt, ahogy azt a táblázat is mutatja, ugyan is az adatvédelem és integritás perspektívájából a pacemakerekben tárolt egészségügyi adatok védelme kulcsfontosságú. Ezek az adatok érzékeny információkat tartalmaznak, így azok biztonságának garantálása elengedhetetlen. Továbbá, a pacemakerek állandó működésének biztosítása létfontosságú, hiszen ezek az eszközök életmentő funkciókat látnak el, ezért is elengedhetetlen az állandó rendelkezésre állás. A pacemakerek hardveres és szoftveres sebezhetőségeinek azonosítása és kezelése fontos a kibertámadások kockázatának csökkentése érdekében, illetve azonosítani kell a lehetséges külső és belső fenyegetéseket, amelyek a pacemakereket érinthetik.^{73 74 75}

Egy gyakorlati példával szemléltetném a táblázatban is említett kritériumok és az IoMT eszközökkel kapcsolatos kockázatok kérdéskörét, pontosabban Dick Cheney az Amerikai Egyesült Államok 46. alelnökének esetét. 2007-ben az orvosai feltörési kockázatok miatt letiltották a pacemakerének a vezetéknélküli képességét. Ez a döntés egy új szintre emelte a kiberbiztonság és betegbiztonság kérdéskörét, mivel rávilágított arra, hogy igen is távoli támadások révén illetéktelenek is közvetlen hozzáférhetnek, akár módosíthatják az eszköz funkcióit is, ha biztonsági rés keletkezik a szektor működésének valamelyik területén. Emellett ez a döntés hangsúlyozta az IoMT eszközök körül kialakítandó szigorú biztonsági protokollok szükségességét a mind elméleti, mind konkrét fenyegetések elleni védelem érdekében.⁷⁶

A kockázatelemzés és a biztonsági stratégia kidolgozásában az értékelési módszerek megkerülhetetlenek. Ezért azonosítani majd prioritizálni kell a mért adatokat, amelyek az egészségügyi rendszert fenyegetik.

⁷² Zaldivar, Tawalbeh, és Muheidat, „Investigating the Security Threats on Networked Medical Devices”, 2020.

⁷³ Baranchuk és mtsai., „Cybersecurity for Cardiac Implantable Electronic Devices”, 2018.

⁷⁴ Patel és Makaryus, „Cardiac implantable electronic devices and cybersecurity”.

⁷⁵ Alexander, Haseeb, és Baranchuk, „Are implanted electronic devices hackable?”

⁷⁶ Peterson, „Yes, Terrorists Could Have Hacked Dick Cheney’s Heart”.

2. lépés

Az elemzés ezen stádiumában ki kell alakítani a pacemaker eszközök kritikus információs eszközprofilja. A már korábban is említett IoMT eszközök más más egyedi tulajdonságokkal, jellemzőkkel és értékkel rendelkeznek, ezért a vagyontprofil készítése során a módszertanhoz igazodva meg kell határozni, hogy melyik tárgy miért kritikus. Az alábbi fő információs profilokat azonosítottam, amelyek kiemelt fontosságúak az egészségügyi intézmények számára. A páciens egészségügyi adatai az egyik, mivel ezek az adatok magukban foglalják a betegek kezelésének teljes folyamatait, diagnózisokat, kezelési terveket, és egyéb személyes egészségügyi információkat. Ezek az egészségügyi adatok rendkívül értékesek, mivel megbízható és állandó személyes információforrást jelentenek, amelyek vonzó célpontot kínálnak a kiberbűnözők számára. Az elektronikus egészségügyi nyilvántartási rendszerek ezeket az adatokat tárolják, amelyek lehetővé teszik az egészségügyi szakemberek számára, hogy hozzáférjenek és kezeljék a páciens információkat.⁷⁷

Az egészségügyi információs rendszerek eszközparkjába tartoznak a már említett elektronikus egészségügyi nyilvántartás rendszerek, a diagnosztikai rendszerek és a betegmenedzsment rendszerek. Ezek használatából eredően új kiberbiztonsági sebezhetőségeket is megnyitnak. Az egészségügyi információs rendszerek gyakran tárolják és kezelik a páciens adatokat, valamint támogatják az egészségügyi szakemberek közötti kommunikációt és adatmegosztást.⁷⁸

Nem utolsó sorban a kommunikációs infrastruktúra, ami hardver és szoftver rendszerelemek közötti adatátvitelt segíti elő a hálózati infrastruktúrában. Az egészségügyi intézmények hálózatai és a távoli hozzáférésű szolgáltatások, mint például a felhőalapú tárolás és az elektronikus egészségügyi nyilvántartások, fokozott kiberbiztonsági kockázatokat jelentenek.

79

3. lépés

A folyamat ezen lépésében megállapítom, hogy az IoMT eszközök által biztosított adatok milyen formában kerülnek feldolgozásra, hol tárolódnak, illetve hogyan szállítják őket. Ezeket az 5. táblázatban demonstrálom. A tároló konténerek között megkülönböztetjük a fizikai, technikai konténereket, amelyek lehetnek szoftverek és hardverek is. A fizikai konténerek, mint

⁷⁷ Clarke és Martin, „Managing cybersecurity risk in healthcare settings”.

⁷⁸ Coventry és Branley, „Cybersecurity in healthcare”, 2018.

⁷⁹ Singh és mtsai., „Guest Editorial”.

például a szerverek, adatközpontok és hordozható adattároló eszközök, létfontosságú infrastruktúrát biztosítanak az egészségügyi adatok tárolásához és védelméhez.^{80 81}

Technológia	Előnyök	Kihívások
Blocklánc	Decentralizált-, manipulációálló adattárolás	Bonyolult implementáció, nagy adatkezelési költségek
Felhőalapú tárolás	Rugalmasság, skálázhatóság, költséghatékonyság	Adatvédelmi és biztonsági aggályok
Interplanetáris fájlrendszer	Elosztott tárolás, magas rendelkezésre állás	Kezdeti technológiai korlátok, teljesítmény kérdések
Fizikai tárolás	Megnövelt biztonság, ellenőrzött hozzáférés	Magas költségek, fizikai sérülékenység

5. táblázat: Az egészségügyi adattárolási technológiák előnyei és kihívásai (Saját szerkesztés, forrás: Baskar és mtsai.⁸² és Gatkal és mtsai.⁸³)

A blokklánc technológia egyedülálló lehetőséget kínál az egészségügyi adatok biztonságos tárolására, mivel egy decentralizált, manipulációálló adatbázist hoz létre. Az adatokat blokkokban tárolja, amelyek kriptográfiai módon vannak összekapcsolva, így biztosítva az adatok integritását és nyomon követhetőségét. Ez a technológia lehetővé teszi a páciensek számára, hogy nagyobb ellenőrzést gyakoroljanak saját egészségügyi adataik felett, miközben lehetővé teszi az egészségügyi szolgáltatók számára az adatok biztonságos és átlátható megosztását és még központi felügyeletre sincs hozzá szükség.⁸⁴

A felhőalapú tárolás rugalmasságot, skálázhatóságot és költséghatékonyságot kínál az egészségügyi adatok kezelésében. Lehetővé teszi az egészségügyi intézmények számára, hogy nagy mennyiségű adatot tároljanak anélkül, hogy szükség lenne jelentős előzetes beruházásra a helyszíni infrastruktúrába. Az adatok távoli elérhetősége javítja az egészségügyi ellátás minőségét és hatékonyságát, lehetővé téve az egészségügyi szakemberek számára, hogy gyorsabban hozzáférjenek a szükséges információkhoz. Azonban a felhőalapú megoldások alkalmazása magában hordozza az adatvédelmi és biztonsági kockázatokat, amelyek kezeléséhez erős titkosítási és hozzáférés-kezelési protollokra van szükség.⁸⁵

⁸⁰ „Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks - Consensus”.

⁸¹ Coventry és Branley, „Cybersecurity in healthcare”, 2018.

⁸² Baskar, Ramar, és Shanmugasundaram, „Data Security in Healthcare Using Blockchain Technology”.

⁸³ Gatkal és mtsai., „Survey on Medical Data Storage Systems”.

⁸⁴ Baskar, Ramar, és Shanmugasundaram, „Data Security in Healthcare Using Blockchain Technology”.

⁸⁵ Gatkal és mtsai., „Survey on Medical Data Storage Systems”.

Az interplanetáris fájlrendszer⁸⁶ egy elosztott fájlrendszer, amely lehetővé teszi az adatok decentralizált tárolását és megosztását. Az említett rendszer, a betegdiagnosztikai jelentések tárolására szolgáló megoldás lehetőséget kínál az egészségügyi adatok gyors és hatékony hozzáférésére, miközben csökkenti a központi tárolási pontokon keresztül történő adatvesztés vagy manipuláció kockázatát. Ez a technológia javíthatja az adatbiztonságot és az adatmegőrzés hatékonyságát, különösen nagy adatmennyiségek esetében.⁸⁷

A fizikai konténerek, mint például a szerverek, adatközpontok és hordozható adattároló eszközök, létfontosságú infrastruktúrát biztosítanak az egészségügyi adatok tárolásához és védelméhez. Ezek a konténerek fizikai biztonsági intézkedésekkel, mint például hozzáférés-ellenőrzés és környezetvédelmi szabályozásokkal vannak felszerelve, hogy megvédjék az adatokat a fizikai fenyegetésektől.⁸⁸

4. lépés

Ebben a lépésben az előbbieken összegyűjtött eszközök, konténerek és információk alapján felvázolom az aggodalomra okot adó területeket, amelyek fenyegethetik az intézmény információs vagyonát.

1. Pacemakerek hálózati sebezhetőségei: Az egészségügyi eszközök, különösen a pacemakerek, egyre inkább csatlakoznak a hálózathoz, ami új sebezhetőségeket tárt fel. Ezek a sebezhetőségek lehetővé teszik a támadók számára, hogy távolról hozzáférjenek az eszközök beállításaihoz vagy manipulálják azok működését.⁸⁹
2. Adatvédelmi aggodalmak: A pacemakerek által gyűjtött egészségügyi adatok érzékeny információk, amelyek illetéktelen hozzáférés esetén kompromittálódhatnak. Az adatvédelmi aggályok középpontjában a páciensek személyes egészségügyi információinak védelme áll.
3. Rendszerek integrációjának hiányosságai: A különböző egészségügyi információs rendszerek közötti integráció hiányosságai további kibervédelmi kockázatokat jelenthetnek, különösen a pacemakerek és más kritikus eszközök esetében.⁹⁰

⁸⁶ Az interplanetáris fájlrendszer lehetővé teszi az adatok interneten történő tárolását és megosztását központi szerverek használata nélkül. Elképzelhető ez úgy, mint egy közös adattár, ahol mindenki tárolhat és elérhet információkat úgy, hogy az adatok nem egy helyen, hanem a világ számos pontján lévő számítógépeken vannak elosztva. Ez segít abban, hogy az információk gyorsabban és biztonságosabban legyenek elérhetők, valamint nehezebben lehessen őket támadni.

⁸⁷ Kumar, Marchang, és Tripathi, „Distributed Off-Chain Storage of Patient Diagnostic Reports in Healthcare System Using IPFS and Blockchain”.

⁸⁸ Argaw és mtsai., „Cybersecurity of Hospitals”.

⁸⁹ „Cybersecurity Threats Targeting Networked Critical Medical Devices - Consensus”.

⁹⁰ Coventry és Branley, „Cybersecurity in healthcare”, 2018.

5. lépés

Ebben a lépésben részletesen ki fogok térni arra, hogy mi történhet akkor, ha az aggodalomra okot adó események bekövetkezésre kerülnek, amelyeket a 4. lépésben dolgoztam ki. Ezt a legrészletesebben egy-egy forgatókönyvben lehet demonstrálni az eszközök, területek és konténerek együttes vizsgálatával. Ezek a forgatókönyvek a következők:

1. Pacemaker hálózati sebezhetőségein alapuló támadás: Egy támadó kihasználja a pacemaker hálózati kommunikációjának sebezhetőségét, hogy jogosulatlan hozzáférést szerezzen az eszközhöz. Ezáltal képes lehet megváltoztatni a pacemaker ütemezését, ami szívritmuszavarhoz vagy akár a pacemaker működésének teljes leállításához vezethet.⁹¹
2. Adatvédelmi hiányosságból eredő támadás: Egy biztonsági rést kihasználva, támadók hozzáférnek a pacemaker által gyűjtött és tárolt érzékeny egészségügyi adatokhoz, beleértve a páciens szívritmus adatait és személyes azonosító információkat. Az ilyen típusú adatszivárgás nemcsak a páciens magánéletét sérti meg, hanem potenciálisan zsaroláshoz is felhasználható.⁹²
3. Rendszerek integrációjaikból eredő támadás: Egy egészségügyi intézmény rendszerei közötti integrációs hiányosságok miatt a pacemaker adatok nem megfelelően védettek, amikor a különböző rendszerek között továbbításra kerülnek. Egy támadó kihasználhatja ezt a sebezhetőséget a rendszeren belüli mozgásra, hogy hozzáférjen a pacemakert kontrolláló infrastruktúrához, lehetővé téve számára, hogy manipulálja az eszköz beállításait vagy akár kiiktassa annak működését.⁹³

6. lépés

Tovább haladva, az előző lépésben meghatározottak kiválóan alátámasztják a szükségességét annak, hogy megvizsgálásra kerüljenek a támadásból eredő kockázatok az intézmény számára.

1. A hálózati sebezhetőségek kihasználásából eredő kockázatok egyike, hogy a pacemaker funkcióinak jogosulatlan manipulálásából a támadók képesek lehetnek a pacemaker ütemezését megváltoztatni, ami aritmiához, szívritmuszavarhoz vagy akár a pacemaker funkciójának teljes leállításához vezethet. Emellett a páciens egészségét közvetlen veszélyezteti, ha a pacemaker beállításait megváltoztatják, mivel végzetes egészségügyi

⁹¹ Alexander, Haseeb, és Baranchuk, „Are implanted electronic devices hackable?”

⁹² Patel és Makaryus, „Cardiac implantable electronic devices and cybersecurity”.

⁹³ Zaldivar, Tawalbeh, és Muheidat, „Investigating the Security Threats on Networked Medical Devices”, 2020.

következményekkel is járhat, beleértve az életveszélyes állapotok kialakulását, bekövetkezését. Végül a beteg elveszti a bizalmát az egészségügyi technológiával szemben. Ezen kockázat erodálhatja a páciensek bizalmát az ilyen típusú eszközök biztonságosságával-, vagy akár az egészségügyi szakemberekkel kapcsolatban is.⁹⁴

2. A személyes és egészségügyi adatok kiszivároghatnak. A támadók által ellopott vagy illetéktelenül hozzáférhetővé tett adatok súlyos adatvédelmi jogsértést jelentenek. Illetve a kiszivárgott adatok felhasználhatók azonosságlopásra, ami további jogi és pénzügyi következményekkel járhat a páciensek számára, de még az egészségügyi intézmények számára a pacemaker adatok kiszivárgása súlyos hírnév károsodást is okozhat, ami ismét csak tovább csökkenti a betegek bizalmát és potenciálisan pénzügyi veszteségeket okoz.⁹⁵
3. A rendszer integrációs hiányosságai miatt a pacemaker és az egészségügyi rendszerek közötti adatátvitel során az adatok manipulálhatók vagy eltorzíthatók lehetnek. Ez adatintegritás- és hitelesség veszélyeztetést eredményez. Továbbá ami növeli még az adatvédelmi és biztonsági kockázatokat az, hogy integrációs problémák miatt még több nem jogosult személyek is hozzáférhetnek a pacemaker adataihoz.⁹⁶

7. lépés

A következő táblázatban a kockázatok elemzését demonstrálom az Octave keretrendszer alapelveit követve, ahol részletesen értékelem a pacemakerekkel kapcsolatos kiberbiztonsági kockázatokat. Az értékelés során a kockázatokat bekövetkezési valószínűségük és a generált hatásuk alapján rangsoroltam egy skálán, ahol az értékek 1-től 5-ig terjednek. Az 1-es jelenti a legkevésbé valószínű vagy súlyos hatást, míg az 5-ös jelenti a legmagasabb határfokot vagy bekövetkezési valószínűséget, ahol a hatás azt jelzi, hogy egy adott kockázat mennyire súlyos következményekkel járhat a páciensek egészségére és biztonságára nézve, míg a bekövetkezési valószínűség azt mutatja meg, hogy egy adott kockázat mennyire valószínűleg fog bekövetkezni. Ez lehetővé teszi az összkockázat számszerűsítését és segít priorizálni azt. Emellett a táblázatban megállapítom a kockázati szintet, a lehetséges csökkentő intézkedéseket, és azt, hogy a kockázat elfogadható-e. Az elfogadhatóság oszlop segít eldönteni, hogy mely kockázatokat kell tovább kezelni, és melyeket lehet feltételek mellett elfogadni.

⁹⁴ Baranchuk és mtsai., „Cybersecurity for Cardiac Implantable Electronic Devices”, 2018.

⁹⁵ Saxon és mtsai., „Factors Influencing the Decision to Proceed to Firmware Upgrades to Implanted Pacemakers for Cybersecurity Risk Mitigation.”

⁹⁶ Patel és Makaryus, „Cardiac implantable electronic devices and cybersecurity”.

Sorszám	Kockázat leírása	Bekövetkezési valószínűség	Hatás	Kockázati szint	Kockázat csökkentő intézkedés	Kockázat elfogadható?
1	Adatvédelmi hiányosságok és adatszivárgás	4	4	Magas	Erősített felhasználói hitelesítés, oktató kampányok	Nem
2	Rendszerek integrációjának hiányosságai	3	3	Közepes	Redundáns rendszerek kiépítése, katasztrófa helyreállítási tervek	Igen, feltételekkel
3	Hálózati sebezhetőségek	5	5	Nagyon Magas	Folyamatos rendszerfrissítések, behatolás tesztelés	Nem

6. táblázat: A kockázati mátrix (Saját szerkesztés, forrás: Baranchuk és mtsai. & Patel és Makaryus⁹⁷)

8. lépés

Az utolsó pontban meghatározom, hogy az intézmény számára az azonosított kockázatok közül melyek igényelnek mérséklést és fokozott figyelmet a kapott értékek alapján. Ez az állomás kulcsfontosságú szerepet tölt be az elemzés keretstruktúrájában, mivel a konklúzió befolyásolja az enyhítési stratégia kidolgozását is.

Kockázati terület	Relatív kockázat (bekövetkezés x hatás)	Kockázati szint
Hálózati sebezhetőségek	25	Nagyon magas
Adatvédelmi hiányosságok és adatszivárgás	16	Magas
Rendszerek integrációjának hiányosságai	9	Közepes

7. táblázat: Relatív kockázati mátrix (Saját szerkesztés, forrás: Baranchuk és mtsai. & Patel és Makaryus⁹⁸)

Az relatív kockázati értéket úgy kaphatjuk meg legegyszerűbben, hogy a bekövetkezési valószínűség és a hatás pontszámainak szorzatát vesszük. Nagyon magas kockázati szinttel

⁹⁷ Baranchuk és mtsai., „Cybersecurity for Cardiac Implantable Electronic Devices”, 2018; Patel és Makaryus, „Cardiac implantable electronic devices and cybersecurity”.

⁹⁸ Baranchuk és mtsai., „Cybersecurity for Cardiac Implantable Electronic Devices”, 2018; Patel és Makaryus, „Cardiac implantable electronic devices and cybersecurity”.

rendelkeznek a hálózati sebezhetőségekkel kapcsolatos kihívások, mivel közvetlenül veszélyeztetik a páciensek egészségét és biztonságát. A hálózati sebezhetőségek mérséklésére folyamatos rendszerfrissítéseket és behatolásteszteket javaslok. Ez a kockázat nem elfogadható, azonnali cselekvést igényel. Az illetéktelen hozzáférés és a pacemaker működésének manipulálása közvetlenül veszélyezteti a páciensek életét és egészségét.

Magas besorolást kapott a relatív pontszámok alapján az adatvédelmi hiányosságok és adatszivárgás problémája. Ez a kihívás jelentősen befolyásolja a szervezet működését és egyáltalán nem elhanyagolható a kérdéskör. Leginkább a felhasználói hitelesítés erősítésével, valamint az információbiztonsági tudatosság növelésével és oktatással lehet javítani rajta. A kockázat szintén nem elfogadható.

A rendszerek integrációjának hiányosságai relatív pontszáma alapján közepes besorolást kap. Ez befolyásolhatja a szervezetet, de kezelhető megfelelő tervezéssel és erőforrás-allokációval. A közepes besorolású területek kezelését nem kell azonnal megkezdeni, de nem is hanyagolhatók el.

KÖVETKEZTETÉSEK

A fejezetben megvizsgáltam az IoMT eszközöket, specifikusabban az implantálható egészségügyi pacemakereket az Octave kockázatelemzési keretrendszer alkalmazásán keresztül. Az első két fejezetben a vizsgálódásaim alátámasztották, hogy egyre növekvő jelentőséggel bír az egészségügyi szektor az állam működésében. Ahogy a világunk komplexitásának fokozódása beigazolódott, úgy az újabb aggodalomra okot adó területek megjelenése is a felszínre kerül, akár csak az implantálható eszközök kérdésköre, mivel ezek az IoMT eszközök jelentősége egyre növekszik az ellátásban, ezzel együtt a kiberbiztonsági kockázatok is növekvő tendenciát mutatnak. A kockázatelemzés során észrevettem, hogy a keretrendszer egy átfogó perspektívát ad az eszközök minden aspektusát tekintve, beleértve a dimenzióit, magukat az eszközöket és az általuk gyűjtött adatok tárolását és továbbhaladva, a működésükből adódó kockázatokat is. Ezen felül egy scenáriót is felvázoltam, amelyek közvetlenül és közvetve is bekövetkezhetnek függetlenül az eszköztől. A biztonsági hálón beszivárgó bűnözők hatalmas problémát tudnak generálni mind a társadalomnak, mind a szektornak és az államnak is, ha ezeket a hiányosságokat nem vizsgálják frekvencián felül a szakemberek és nem foltozzák be a biztonsági réseket. Az IoMT eszközök kockázatelemzése elengedhetetlen a modern egészségügyben, ezért tehát egy átfogó víziót, tervet kell az elemzés után felvázolni, hogy az azonosított kihívásokra gyors, rugalmas és hatékony választ tudjon adni a szektor.

ÖSSZEGZETT KÖVETKEZTETÉSEK

A dolgozatomban az egészségügyi kritikus információs infrastruktúra kibervédelmét vizsgáltam. A kutatásomat az indokolta, hogy a szektor jelentősége kulcsfontosságú szerepet tölt be minden ember életében és kardinális szerepet tölt be az állam működésében is. Számos modern eszközt, valamint digitális, internetre csatlakoztatható orvosi eszközt alkalmaznak a betegek ellátásában, ezért tehát kijelenthető, hogy az egészségügy a technológiai innováció terepe. A minőségi fejlődés hatalmas méreteket ölt a szektor falai között és ezzel egy új fejezetet is nyit az orvoslásban, de ki kell emelnem, hogy ez egy kétélű penge is egyben. Az innováció egyben rendkívül erős nyomást gyakorol a biztonsági szakemberekre, mivel olyan lehetőségeket nyitnak a kibertérben tevékenykedő bűnözők számára, amire eddig nem volt precedens.

Az első fejezetben az egészségügyi infrastruktúra változásait tekintetem át. Megállapítottam, hogy a szektor exponenciálisan gyorsuló fejlődésen megy keresztül, különösen az IoMT eszközök, mint a vérnyomás- és glükózmérők, pacemakerek, és defibrillátorok, valamint az AI alapú rendszerek alkalmazásán át. A gyorsuló folyamatnak egy lendületet adott a Covid-19 világjárvány, amikor is a pandémia során a távmunka és a telemedicina segítségével még inkább az online tér felé orientálódtak az emberek. Ez a folyamat előidézett új adatvédelmi és kibervédelmi kihívásokat. A kihívásokra válaszok kellene, ezeket a legjobban és legrészletesebben a GDPR és az NIS 2 irányelvek ismertették, amelyek fontos szerepet játszanak az egészségügyi adatok és infrastruktúrák védelmében.

A vizsgálódások alátámasztották, hogy a második fejezetben részletesebben áttanulmányozzam az IoMT eszközöket. Alapvetően a téma komplexitásából kifolyólag a legalaposabban szerettem volna tanulmányozni, ezért a kockázatelemzés módszertanait áttekintve megállapítottam, hogy az egészségügyi kritikus információs infrastruktúra védelmében a kockázatelemzés alapvető eszközként szolgál. A SecRam és az Octave Allegro kockázatelemzési modellek alkalmazásának lehetőségeit értékelve azt az eredményt kaptam, hogy a szektor méreteiből és komplexitásából kifolyólag az Octave módszertannal lehet a leginkább átfogó eredményt kapni a kockázati stratégiák kidolgozásához. A fejezet végén hangsúlyoztam a kockázatelemzés kritikus szerepét az egészségügyi szektorban, kiemelve, hogy az átfogó és hatékony kockázatkezelési folyamat elengedhetetlen az egészségügyi infrastruktúra védelmében és a biztonságos betegellátás biztosításában.

A harmadik fejezetben az Octave kockázatelemzés keretrendszerét alkalmazva megvizsgáltam az IoMT eszközöket. Az Octave segítségével az egészségügyi szervezetek felmérhetik és kezelhetik az IoMT eszközökkel kapcsolatos kiberbiztonsági kockázatokat. A dolgozatom ezen

szakaszában körvonalazódott, hogy a legnagyobb kockázatot az implantálható IoMT eszközök jelentik a szektorban. Az elemzés során felvázoltam, hogy az implantáló eszközök mely aspektusai hordoznak olyan kihívásokat magukban, amelyek később egy rést nyithatnak a kibertérben tevékenykedő bűnözők számára. Ezekből felvázoltam egy aggodalomra okot adó területeket, illetve scenáriókat, majd a relatív kockázati mátrix segítségével kiszámoltam az egyes területek relatív pontszámait. A számok alapján priorizáltam a területeket, majd azonosítottam, hogy melyek igényelnek moderálást. Emellett hangsúlyos, hogy az emberi tényező jelentős a kockázatelemzés- és kezelés folyamatában, kiemelve, hogy mind a felhasználók, mind az egészségügyi dolgozók biztonság tudatos magatartása kulcsfontosságú az IoMT eszközökkel kapcsolatos kiberfenyegetések megelőzésében. Hogy biztosítsák az IoMT eszközök biztonságos használatát és a szektor gördülékeny működését, megelőző intézkedéseket, incidensreagálási terveket és folyamatos felülvizsgálatot kell fenntartani. Úgy vélem, a szektor rendkívüli összetettsége miatt a biztonság komplex áttekintést igényel, ahol egyetlen aspektust sem szabad figyelmen kívül hagyni. Még a legjelentéktelenebbnek tűnő hiba is komoly problémákat okozhat, ezért kiemelten fontos a biztonság fenntartásának folyamatos biztosítása.

Új tudományos eredmények

T1: Megállapítottam, hogy a kockázatelemzés alkalmazásával az IoMT eszközöknél hatékonyan fel lehet fedni a sérülékenységeket és ezáltal javítható a szektor védelme és a betegellátás minősége is.

T2: A dolgozatomban és az elemzés során látható, hogy a legnagyobb kockázati tényezőt a számítógép és a szék között kell keresni, ami maga az ember. Viszont megfelelő edukálással jelentősen lehet redukálni a faktort.

T3: Azonosítottam, hogy olyan átfogó és komplex keretrendszer alkalmazásával, mint az Octave módszertan megállapítható, hogy jellegéből és metódusából adódóan könnyen lehet szűrni azokat a biztonsági réseket, amelyek felismerésével hatékonyan javítható a kibervédelem az egészségügyi szektorban.

T4: Meghatároztam, hogy a fenntartható egészségügynek szüksége van egy átfogó kiberbiztonsági megközelítésre, amely integrálja a legújabb technológiai fejlesztéseket, figyelembe veszi az adatvédelmi és jogi kereteket, és alkalmazkodik a folyamatosan változó kiberfenyegetésekhez. A kockázatelemzés és kockázatkezelési stratégiák kulcsszerepet játszanak az egészségügyi szektor kiberbiztonságának javításában. A dolgozatomban eredményei megerősítik, hogy a kockázatkezelési folyamat folyamatos figyelmet és adaptációt igényel a technológiai és társadalmi környezet változásaihoz.

A kutatásom megadta az alapot annak, hogy a következő dolgozatomban részletesebben foglalkozzak az IoMT eszközök kiberbiztonságának megerősítésével. Ez magában foglalhatja új kriptográfiai technikák és protokollok fejlesztését, amelyek kifejezetten az IoMT eszközök egyedi jellemzőire és kihívásaira összpontosítanak. Emellett további kutatásra van szükség a mesterséges intelligencia és a gépi tanulás alkalmazásai kapcsán, mivel ez a kiforratlan terület számtalan lehetőséget és kihívást hordoz magában a szektorra vetítve.

FELHASZNÁLT IRODALOM

- Kiss Adrienn, „A kockázatelemzés rejtett számai”. Ludovika.hu, 2022. november 15. <https://www.ludovika.hu/blogok/cyberblog/2022/11/15/a-kockazatelemzes-rejtett-szamai/>.
- Alexander, B., Sohaib Haseeb, és A. Baranchuk. „Are implanted electronic devices hackable?” *Trends in cardiovascular medicine*, 2019. <https://doi.org/10.1016/j.tcm.2018.11.011>.
- Argaw, Salem T., J. Troncoso-Pastoriza, Darren Lacey, Marie-Valentine Florin, F. Calcavecchia, Denise Anderson, Wayne Burleson, és mtsai. „Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks”. *BMC Medical Informatics and Decision Making* 20 (2020). <https://doi.org/10.1186/s12911-020-01161-7>.
- Asgari, Hamid, Sarah Haines, és Ondrej Rysavy. „Identification of Threats and Security Risk Assessments for Recursive Internet Architecture”. *IEEE Systems Journal* 12, sz. 3 (2018. szeptember): 2437–48. <https://doi.org/10.1109/JSYST.2017.2765178>.
- Asgari, Hamid, Sarah Haines, és Adrian Waller. „Security Risk Assessment and Risk Treatment for Integrated Modular Communication”. In *2016 11th International Conference on Availability, Reliability and Security (ARES)*, 503–9. Salzburg, Austria: IEEE, 2016. <https://doi.org/10.1109/ARES.2016.6>.
- „AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/ 679 RENDELETE - (2016. április 27.) - a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/ 46/ EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)”, é. n.
- Baranchuk, A., M. Refaat, K. Patton, M. Chung, Kousik Krishnan, V. Kutyifa, G. Upadhyay, John D. Fisher, és D. Lakkireddy. „Cybersecurity for Cardiac Implantable Electronic Devices: What Should You Know?” *Journal of the American College of Cardiology* 71 11 (2018): 1284–88. <https://doi.org/10.1016/j.jacc.2018.01.023>.
- Basatneh, Rami, Bijan Najafi, és David G. Armstrong. „Health Sensors, Smart Home Devices, and the Internet of Medical Things: An Opportunity for Dramatic Improvement in Care for the Lower Extremity Complications of Diabetes”. *Journal of Diabetes Science and Technology* 12, sz. 3 (2018. május 1.): 577–86. <https://doi.org/10.1177/1932296818768618>.
- Baskar, Sandhiya, K. Ramar, és Hariharan Shanmugasundaram. „Data Security in Healthcare Using Blockchain Technology”. *2021 International Conference on Decision Aid Sciences and Application (DASA)*, 2021, 354–59. <https://doi.org/10.1109/DASA53625.2021.9682300>.
- „BM Országos Katasztrófavédelmi Főigazgatóság”. Elérés 2024. március 12. <https://www.katasztrofavedelem.hu/109/kritikus-infrastrukturak-vedelmevel-osszefuggo-hatosagi-feladatok-jogszabalyok>.
- Caralli, Richard A., James F. Stevens, Lisa R. Young, és William R. Wilson. „Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process”: Fort Belvoir, VA: Defense Technical Information Center, 2007. május 1. <https://doi.org/10.21236/ADA470450>.
- Chamola, Vinay, Vikas Hassija, Vatsal Gupta, és Mohsen Guizani. „A Comprehensive Review of the COVID-19 Pandemic and the Role of IoT, Drones, AI, Blockchain, and 5G in Managing Its Impact”. *IEEE Access* 8 (2020): 90225–65. <https://doi.org/10.1109/ACCESS.2020.2992341>.
- Chatterjee, Ayan, Andreas Prinz, Michael A. Riegler, és Jishnu Das. „A systematic review and knowledge mapping on ICT-based remote and automatic COVID-19 patient monitoring and care”. *BMC Health Services Research* 23, sz. 1 (2023. szeptember 30.): 1047. <https://doi.org/10.1186/s12913-023-10047-z>.

- Clarke, M., és Kevin Martin. „Managing cybersecurity risk in healthcare settings”. *Healthcare Management Forum* 37 (2023): 17–20. <https://doi.org/10.1177/08404704231195804>.
- Coventry, L., és D. Branley. „Cybersecurity in healthcare: A narrative review of trends, threats and ways forward.” *Maturitas* 113 (2018): 48–52. <https://doi.org/10.1016/j.maturitas.2018.04.008>.
- „Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks - Consensus”. Elérés 2024. március 30. https://consensus.app/papers/cybersecurity-hospitals-discussing-challenges-working-argaw/4af5e3523d4d50acb405984f488c3cfc/?utm_source=chatgpt.
- „Cybersecurity Threats Targeting Networked Critical Medical Devices - Consensus”. Elérés 2024. március 31. https://consensus.app/papers/cybersecurity-threats-targeting-networked-critical-gaukstern/baef144a2917558f9a54220c6f2fae92/?utm_source=chatgpt.
- Deloitte Insights. „Digital Transformation”. Elérés 2024. március 4. <https://www2.deloitte.com/us/en/insights/industry/health-care/digital-transformation-in-healthcare.html>.
- Ekelhart, A., S. Fenz, és T. Neubauer. „AURUM: A Framework for Information Security Risk Management”. In *2009 42nd Hawaii International Conference on System Sciences*, 1–10, 2009. <https://doi.org/10.1109/HICSS.2009.82>.
- Esposito, Christian, Aniello Castiglione, Constantin-Alexandru Tudorica, és Florin Pop. „Security and privacy for cloud-based data management in the health network service chain: a microservice approach”. *IEEE Communications Magazine* 55, sz. 9 (2017. szeptember): 102–8. <https://doi.org/10.1109/MCOM.2017.1700089>.
- Ganzer, Meghan. „Understanding EU’s NIS2 Cybersecurity Directive”. Verve Industrial, 2023. június 6. <https://verveindustrial.com/resources/whitepaper/nis2-cybersecurity-directive-for-eu/>.
- „Garaczi Imre: Kockázati modellek és társadalmi mozgások”, é. n.
- Gatkal, Suyog, Pune India Jspm Narhe Technical Campus, V. Dhage, Dhanashree Kalekar, és Sanket Ghadge. „Survey on Medical Data Storage Systems”. *International Journal of Soft Computing and Engineering*, 2021. <https://doi.org/10.35940/ijscce.a3528.0911121>.
- Ghubaish, Ali, Tara Salman, Maede Zolanvari, Devrim Unal, Abdulla Al-Ali, és Raj Jain. „Recent Advances in the Internet-of-Medical-Things (IoMT) Systems Security”. *IEEE Internet of Things Journal* 8, sz. 11 (2021. június 1.): 8707–18. <https://doi.org/10.1109/JIOT.2020.3045653>.
- Gopal, Gayatri, Clemens Suter-Crazzolara, Luca Toldo, és Werner Eberhardt. „Digital Transformation in Healthcare – Architectures of Present and Future Information Technologies”. *Clinical Chemistry and Laboratory Medicine (CCLM)* 57, sz. 3 (2019. március 1.): 328–35. <https://doi.org/10.1515/cclm-2018-0658>.
- Greco, Luca, Gennaro Percannella, Pierluigi Ritrovato, Francesco Tortorella, és Mario Vento. „Trends in IoT based solutions for health care: Moving AI to the edge”. *Pattern Recognition Letters* 135 (2020. július 1.): 346–53. <https://doi.org/10.1016/j.patrec.2020.05.016>.
- Hupont, TORRES Isabelle, Vasiliki Charisi, PRATO Giuditta De, Katarzyna Pogorzelska, Sven Schade, Alexander Kotsev, Maciej Sobolewski, és mtsai. „Next Generation Virtual Worlds: Societal, Technological, Economic and Policy Challenges for the EU”. JRC Publications Repository, 2023. június 27. <https://doi.org/10.2760/51579>.
- „Introduction to the OCTAVE Approach”, 2003. augusztus 1. <https://insights.sei.cmu.edu/library/introduction-to-the-octave-approach/>.
- „IT Security Risk Assessment Methodology: Qualitative vs Quantitative | UpGuard”. Elérés 2024. március 9. <https://www.upguard.com/blog/risk-assessment-methodology>.

- Jain Anushtha. „Mi az a kockázatelemzés: meghatározás és eszközök | Teljes útmutató”. *Visure Solutions* (blog). Elérés 2024. március 9. <https://visuresolutions.com/hu/blog/kock%C3%A1zatelemz%C3%A9s/>.
- Kalwani, Neil M, Esli Osmanliu, Vijaya Parameswaran, Lubna Qureshi, Rajesh Dash, Paul A Heidenreich, David Scheinker, és Fatima Rodriguez. „Changes in Telemedicine Use and Ambulatory Visit Volumes at a Multispecialty Cardiovascular Center during the COVID-19 Pandemic”. *Journal of Telemedicine and Telecare*, 2022. február 2., 1357633X211073428. <https://doi.org/10.1177/1357633X211073428>.
- Kft, Wolters Kluwer Hungary. „1163/2020. (IV. 21.) Korm. Határozat Magyarország Nemzeti Biztonsági Stratégiájáról - Hatályos Jogszabályok Gyűjteménye”. Elérés 2024. március 18. <https://net.jogtar.hu/jogszabaly?docid=A20H1163.KOR&txtreferer=00000001.txt>.
- „Kockázat - Közzolgálati Online Lexikon”, 2022. november 30. <https://lexikon.uni-nke.hu/szocikk/kockazat/>.
- Korombel, Anna, és Piotr Tworek. „Qualitative risk analysis as a stage of risk management in investment projects: Advantages and disadvantages of selected methods-theoretical approach”. „*AD ALTA: Journal of Interdisciplinary Research*” 2011, Vol. 1, Issue 2, pp. 51-54. 1 (2011. június 1.): 51–54.
- Kosutic, Dejan. „What Is NIS2? An Easy-to-Understand Guide | Advisera”, 2024. január 22. <https://advisera.com/articles/what-is-nis2/>.
- Kovács L á s z l ó . *Kiberbiztonság és - stratégia*. Dialóg Campus Kiadó, 2018. <https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/12639>.
- Kumar, Randhir, N. Marchang, és Rakesh Tripathi. „Distributed Off-Chain Storage of Patient Diagnostic Reports in Healthcare System Using IPFS and Blockchain”. *2020 International Conference on COMMunication Systems & NETWORKS (COMSNETS)*, 2020, 1–5. <https://doi.org/10.1109/COMSNETS48256.2020.9027313>.
- Kovács László. „KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK”, é. n.
- „Lean Risk Assessment Based on OCTAVE Allegro – Compass Security Blog”, 2013. április 11. <https://blog.compass-security.com/2013/04/lean-risk-assessment-based-on-octave-allegro/>.
- „Managing Information Security Risks: The OCTAVE Approach”, 2002. július 9. <https://insights.sei.cmu.edu/library/managing-information-security-risks-the-octave-approach/>.
- Marotta, Antonio, Gabriella Carrozza, Luigi Battaglia, Patrizia Montefusco, és Vittorio Manetti. „Applying the SecRAM Methodology in a CLOUD-Based ATM Environment”. In *2013 International Conference on Availability, Reliability and Security*, 807–13, 2013. <https://doi.org/10.1109/ARES.2013.108>.
- Newlands, Gemma, Christoph Lutz, Aurelia Tamò-Larrieux, Eduard Fosch Villaronga, Rehana Harasgama, és Gil Scheitlin. „Innovation under Pressure: Implications for Data Privacy during the Covid-19 Pandemic”. *Big Data & Society* 7, sz. 2 (2020. július 1.): 2053951720976680. <https://doi.org/10.1177/2053951720976680>.
- „OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) - CIO Wiki”. Elérés 2024. március 9. [https://cio-wiki.org/wiki/OCTAVE_\(Operationally_Critical_Threat,_Asset_and_Vulnerability_Evaluation\)](https://cio-wiki.org/wiki/OCTAVE_(Operationally_Critical_Threat,_Asset_and_Vulnerability_Evaluation)).
- Palicz, Tamás, Balázs Bencsik, és Miklós Szócska. „Kiberbiztonság a koronavírus idején – a COVID–19 nemzetbiztonsági aspektusai”. *Scientia et Securitas* 2, sz. 1 (2021. július 30.): 78–87. <https://doi.org/10.1556/112.2021.00001>.
- Palicz, Tamás, Tibor Sas, Zoltán Szabó, Tamas Toth, József Tisóczki, Balázs Bencsik, és Tamas Joo. „Magyar kórházakban előfordult zsarolóvírus támadások esetei”. *IME - Az*

- egészségügyi vezetők szaklapja* 20 (2021. január 1.): 32–38.
<https://doi.org/10.53020/IME-2021-105>.
- Palicz, Tamás, Tibor Sas, József Tisóczki, Balázs Bencsik, és Tamás Joó. „»Pénzt Vagy Életet!« – Zsarolóvírusok Az Egészségügyi Informatikai Rendszerekben”. *Orvosi Hetilap* 161, sz. 36 (2020. szeptember 1.): 1498–1505.
<https://doi.org/10.1556/650.2020.31788>.
- Park, Sun Young, Pei-Yi Kuo, Andrea Barbarin, Elizabeth Kaziunas, Astrid Chow, Karandeep Singh, Lauren Wilcox, és Walter S. Lasecki. „Identifying Challenges and Opportunities in Human-AI Collaboration in Healthcare”. In *Companion Publication of the 2019 Conference on Computer Supported Cooperative Work and Social Computing*, 506–10. Austin TX USA: ACM, 2019. <https://doi.org/10.1145/3311957.3359433>.
- Pascarella, Giacomo, Matteo Rossi, Emma Montella, Arturo Capasso, Gianfranco De Feo, Gerardo Botti, Antonio Nardone, és mtsai. „Risk Analysis in Healthcare Organizations: Methodological Framework and Critical Variables”. *Risk Management and Healthcare Policy* 14 (2021. július 8.): 2897–2911. <https://doi.org/10.2147/RMHP.S309098>.
- Patel, Bhakti, és A. Makaryus. „Cardiac implantable electronic devices and cybersecurity”. *Expert Review of Medical Devices* 18 (2021): 69–77.
<https://doi.org/10.1080/17434440.2021.2007075>.
- PECB. „A Comprehensive Guide: Understanding the NIS 2 Directive”. Elérés 2024. március 4. <https://pecb.com/article/a-comprehensive-guide-understanding-the-nis-2-directive>.
- Peterson, Andrea. „Yes, Terrorists Could Have Hacked Dick Cheney’s Heart”. *Washington Post*, 2021. december 6. <https://www.washingtonpost.com/news/the-switch/wp/2013/10/21/yes-terrorists-could-have-hacked-dick-cheney-s-heart/>.
- Prajanti, Anisa Dewi, és Kalamullah Ramli. „A Proposed Framework for Ranking Critical Information Assets in Information Security Risk Assessment Using the OCTAVE Allegro Method with Decision Support System Methods”. In *2019 34th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC)*, 1–4, 2019. <https://doi.org/10.1109/ITC-CSCC.2019.8793421>.
- Praveen. „The Benefits of Utilizing the OCTAVE Threat Model”. *Cybersecurity Exchange* (blog), 2022. szeptember 4. <https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/octave-threat-model-benefits/>.
- PricewaterhouseCoopers. „Kiberbiztonság és adatvédelem”. PwC, 2023. május 4. https://www.pwc.com/hu/hu/szolgaltatasok/vallalati_kockazatkezeles/kiberbiztonsag-es-adatvedelem.html.
- Putri, Tristania Setianingrum Dandhung, és Imam Riadi. „Analysis of Risk Management on Learning Management System Using Octave Allegro Framework”. *International Journal of Computer Applications* 184, sz. 34 (2022. október 31.): 18–23.
<https://doi.org/10.5120/ijca2022922410>.
- Saxon, L., N. Varma, L. Epstein, L. Ganz, és A. Epstein. „Factors Influencing the Decision to Proceed to Firmware Upgrades to Implanted Pacemakers for Cybersecurity Risk Mitigation.” *Circulation*, 2018.
<https://doi.org/10.1161/CIRCULATIONAHA.118.034781>.
- Scribd. „Szun-Ce - A Háború Művészete PDF | PDF”. Elérés 2024. március 13. <https://www.scribd.com/document/473169172/Szun-ce-A-haboru-m%C5%B1veszete-pdf>.
- Singh, Ashutosh Kumar, Abhinav Kumar, Zahid Akhtar, és Muhammad Khurram Khan. „Guest Editorial: Cybersecurity Intelligence in the Healthcare System”. *IEEE Transactions on Industrial Informatics* 19 (2023): 809–12. <https://doi.org/10.1109/TII.2022.3202828>.
- „Stratégiai megállapodás a hazai egészségügy kiberbiztonságának javítása érdekében | Nemzeti Kibervédelmi Intézet”, 2023. május 16.

- <https://nki.gov.hu/intezet/kozlemenyek/strategiai-megallapodas-a-hazai-egeszsegugy-kiberbiztonsaganak-javitasa-erdekeben/>.
- Tasheva, Iva. „Cybersecurity Post-COVID-19: Lessons Learned and Policy Recommendations”. *European View* 20, sz. 2 (2021. október 1.): 140–49. <https://doi.org/10.1177/17816858211059250>.
- Taulli, Tom. „Cool AI Highlights At CES”. *Forbes*. Elérés 2024. március 6. <https://www.forbes.com/sites/tomtaulli/2019/01/13/cool-ai-highlights-at-ces/>.
- Jenei Tünde. „Leggyakrabban használt kockázatkezelési modellek összehasonlítása”. *International Journal of Engineering and Management Sciences* 1 (2016. július 13.): 1–11. <https://doi.org/10.21791/IJEMS.2016.1.22>.
- Vijayanto, R.M., Devyana, és G. Wang. „Enhancing Is Risk Assessment through Using Combination Vector Matrix and Octave Methods”. *International Journal of Advanced Trends in Computer Science and Engineering* 8, sz. 6 (2019): 3140–46. <https://doi.org/10.30534/ijatcse/2019/77862019>.
- Vishnu, S., S.R. Jino Ramson, és R. Jegan. „Internet of Medical Things (IoMT)-An Overview”, 101–4, 2020. <https://doi.org/10.1109/ICDCS48716.2020.243558>.
- World Economic Forum. „How the Digital Revolution Can Make Healthcare More Inclusive”, 2021. szeptember 27. <https://www.weforum.org/agenda/2021/09/how-digital-revolution-can-make-healthcare-more-inclusive/>.
- Zaldivar, David, L. Tawalbeh, és Fadi Muheidat. „Investigating the Security Threats on Networked Medical Devices”. *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*, 2020, 0488–93. <https://doi.org/10.1109/CCWC47524.2020.9031212>.

ÁBRÁK JEGYZÉKE

1. ábra: A viselhető intelligens eszközök. (Saját szerkesztés, forrás: Ghubaish és mtsai. 2021)	
.....	Hiba! A könyvjelző nem létezik.
2. ábra A SecRam általános alkalmazásának folyamata. (Saját szerkesztés, forrás: Asgari, Haines, és Waller.)	15
3. ábra: Az Octave általános alkalmazásának folyamata. (Saját szerkesztés, forrás: Vijayanto, Devyana, és Wang)	18

TÁBLÁZATOK JEGYZÉKE

1. táblázat: Az intelligens eszközökkel járó előnyök és hátrányok a betegellátásban. (Saját szerkesztés, forrás: Chatterjee és mtsai. 2023).....	5
2. táblázat: A vírus hatása a telemedicina igénybevételére. (Saját szerkesztés, forrás: Kalwani et al. 2022).....	8
3. táblázat: Az Octave és SecRam módszertan tulajdonságainak összehasonlítása. (Saját szerkesztés, forrás: Praveen)	20
4. táblázat: Kockázatmérési kritériumok (Saját szerkesztés, forrás: Zaldivar és mtsai.).....	23
5. táblázat: Az egészségügyi adattárolási technológiák előnyei és kihívásai (Saját szerkesztés, forrás: Baskar és mtsai. és Gatkal és mtsai.)	25
6. táblázat: A kockázati mátrix (Saját szerkesztés, forrás: Baranchuk és mtsai. & Patel és Makaryus).....	29
7. táblázat: Relatív kockázati mátrix (Saját szerkesztés, forrás: Baranchuk és mtsai. & Patel és Makaryus).....	29

RÖVIDÍTÉSEK JEGYZÉKE

Rövidítés	Magyar nyelvű kifejezés	Idegen nyelvű kifejezés
AI	Mesterséges intelligencia	Artificial Intelligence
GDPR	Általános adatvédelmi rendelet	General Data Protection Regulation
IEC	Nemzetközi Elektrotechnikai Bizottság	International Electrotechnical Commission
IoMT	Internetre csatlakoztatható orvosi eszközök	Internet of Medical Things

ISO	Nemzetközi Szabványügyi Szervezet	International Organization for Standardization
OCTAVE	Működési szempontból kritikus veszélyek, eszközök és sebezhetőség értékelése	Operationally Critical Threat, Asset, and Vulnerability Evaluation
ML	Gépi tanulás	Machine Learning
SecRam	Biztonsági kockázatértékelési módszertan	Security Risk Assessment Methodology