Adatvezérelt Egészség Divízió
Egészségbiztonság Nemzeti Laboratórium

D2H

CYBERSEC 2023

Orvosi eszközök kiberbiztonsága

Dr. Palicz Tamás

2023. október 3.

Semmelweis Egyetem EMK Egészségügyi Menedzserképző Központ
MEMT Magyar Egészségügyi Menedzsment Társaság
NTP Neumann Technológiai Platform
RI
Széchenyi Terv Plusz Építsük együtt Magyarországot!
Magyarország Kormánya
Az Európai Unió finanszírozásával NextGeneration EU

Cybersecurity is not just a technical issue;
it’s a patient safety issue.*

2019. október 4.

Nil nocere! – Nem ártani!

Kiberbiztonság = betegbiztonság!

*https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals

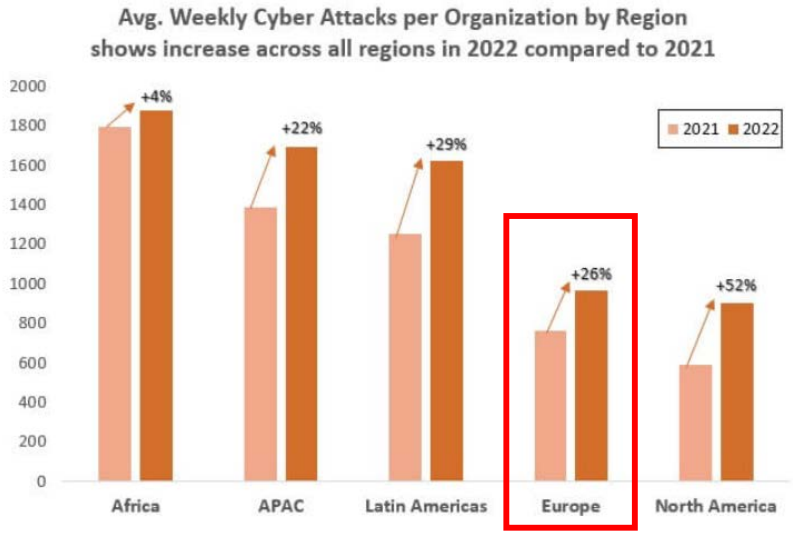
IoMT az egészségügyi rendszerben

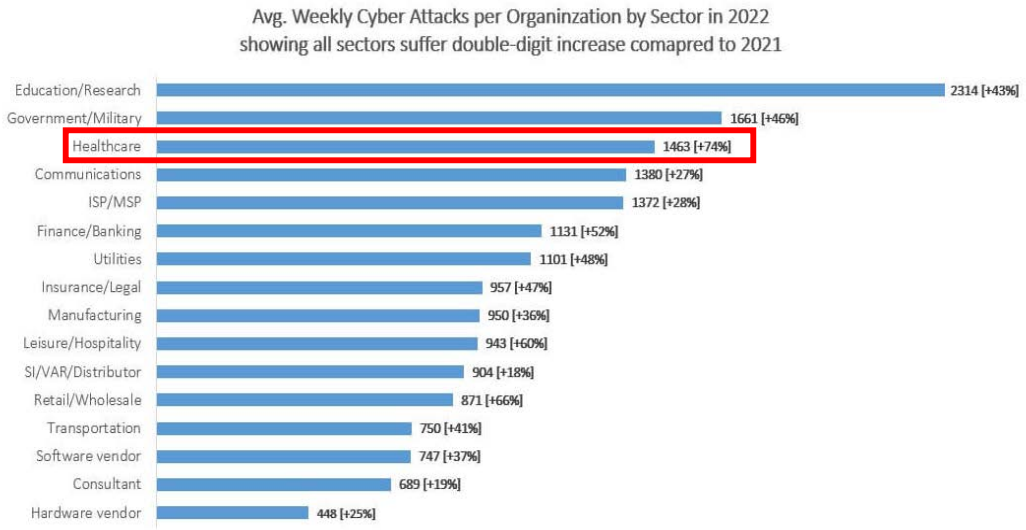
Adatvezérelt Egészség Divízió
Egészségbiztonsági Nemzeti Laboratórium

Semmelweis University
EMK
Health Services Management Training Centre

Egészségügyi kiberbiztonsági kihívások - 2023

A globális kibertámadások száma 2022-ben **38%-kal nőtt** 2021-hez képest. Ezeket a kibertámadások számá
kisebb, agilisabb hacker- és ransomware-bandák okozták, amelyek az otthoni munkakörnyezetekben haszn
együttműködési eszközök kiaknázására összpontosítottak, és megcélozták a **távoktatásra áttért oktatási intézményeket**. A globális kibertámadások számának ez a növekedése a hackerek **egészségügyi szervezete iránti érdeklődéséből is adódik, amelyek 2022-ben az összes többi iparághoz képest a legnagyobb mértékben növekedtek a kibertámadások számában**.





Healthcare cybersecurity predictions for 2023

Device security will be a major priority

The use of **IoT devices and connected medical devices** have always posed a **risk to healthcare** organisations,
[1] **due to poor security in the devices themselves** and because healthcare organizations generally don't take the necessary precautions to minimize the risk of a breach.
[2**]** **IoT device usage, however, is expected to increase** and as manufacturers pay attention to security, the onus of securing these devices and the
[3] **connecting networks** will fall on security department leaders
[4] **Remote care and telehealth services are also projected to increase**. This is offsite care that will still require ongoing monitoring and additional devices that can relay information wirelessly and also be part of a patient's overall treatment. Healthcare organisations shouldn't fall into the same trap as medical devices and ignore potential security harms, especially since an attacker may now be able to attack a patient's personal network, creating a new legal risk for healthcare providers.

Security leaders will need to handle an increasingly complex environment full of potentially insecure devices while also ensuring that new remote care and telehealth initiatives don't expose the company to cyber, compliance, or litigator risk.

https://www.expresshealthcare.in/blogs/guest-blogs-healthcare/healthcare-cybersecurity-predictions-for-2023/437858/

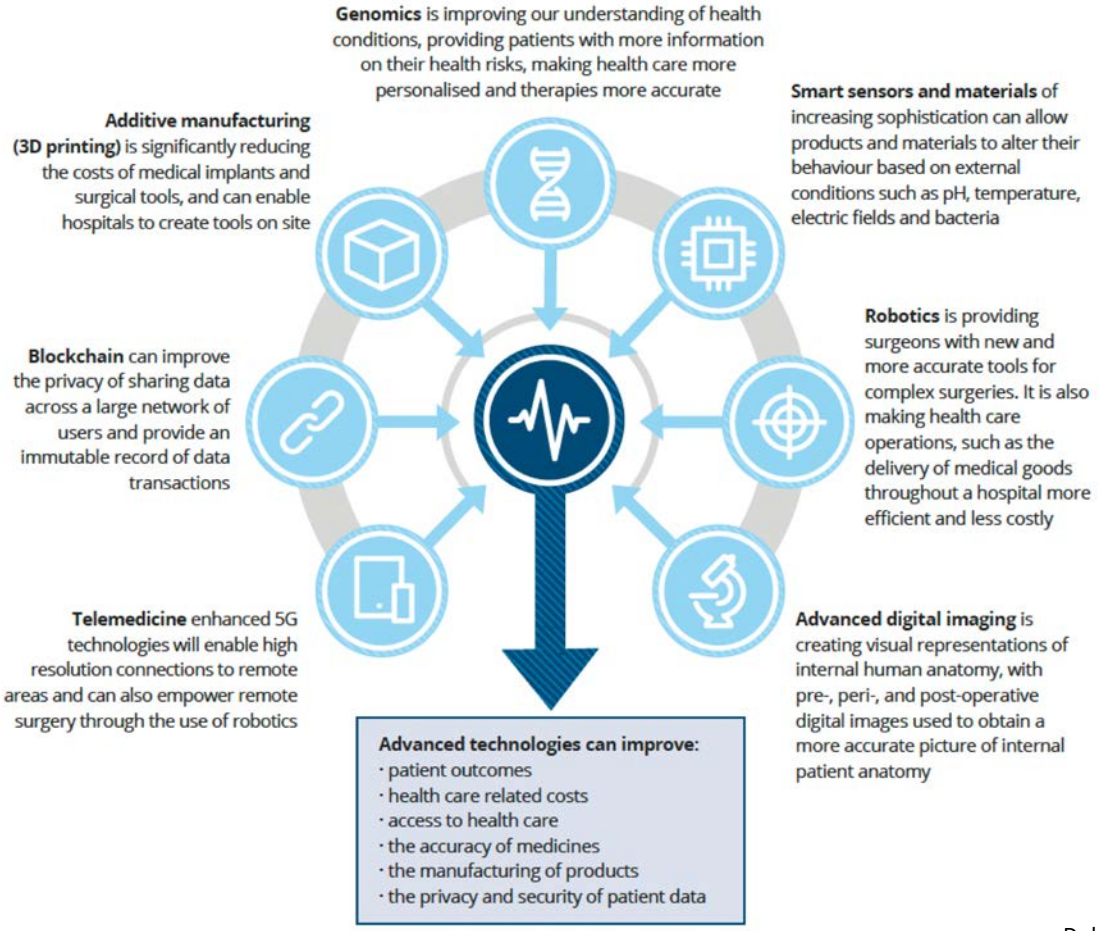
Egészségügyi digitális transzformációja
(digitalizálás, digitalizáció)

Adatvezérelt Egészség Divízió
Egészségbiztonsági Nemzeti Laboratórium

Semmelweis University
EMK
Health Services Management Training Centre

Egészségügyi technológiák - diszrupció

Figure 22: Disruptive technologies can improve the pulse of health care



Deloitte-Medtech and the Internet of Medical Things (2018)

IoT – IoXT - IoMT

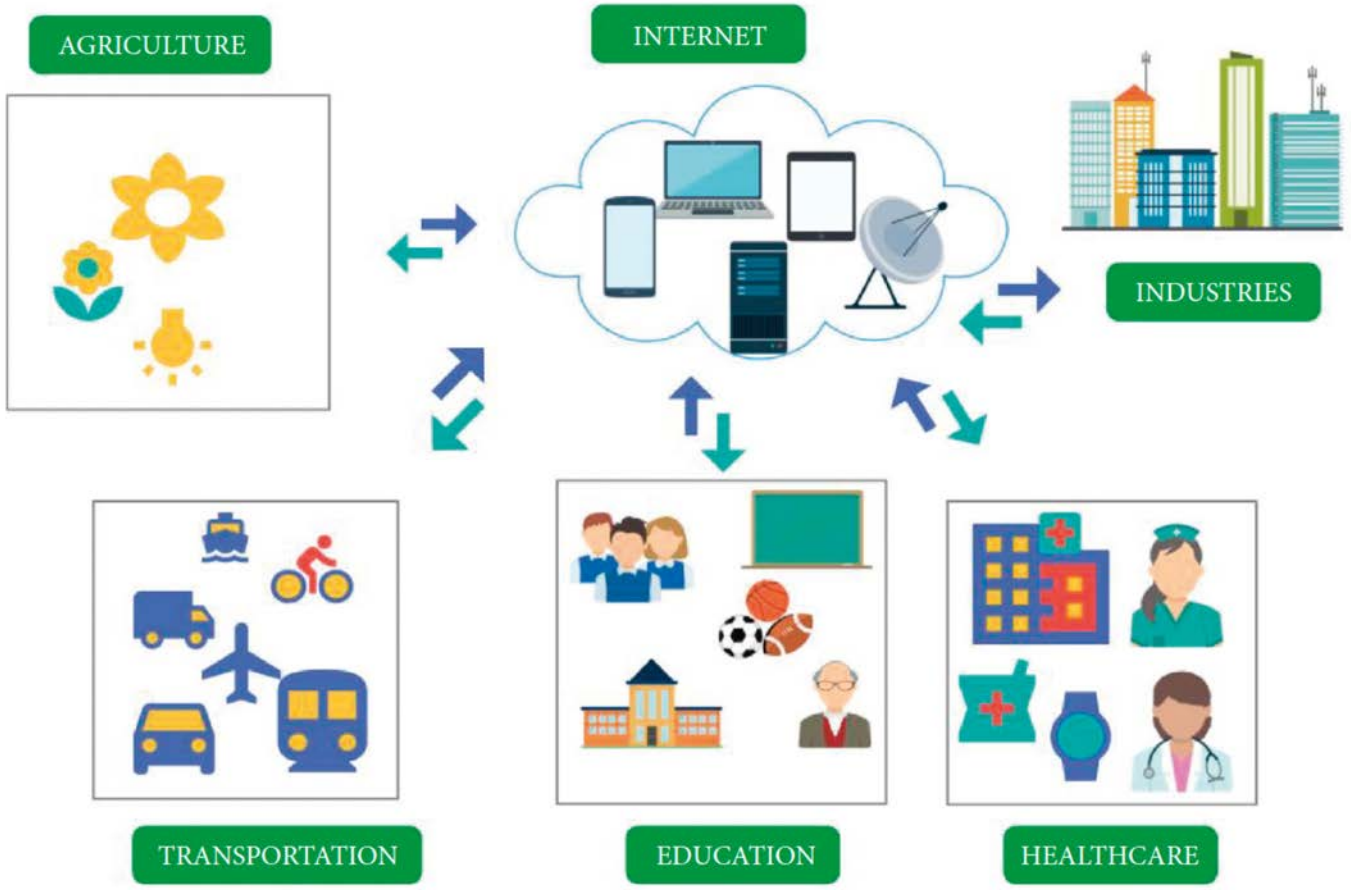


FIGURE 1: Overall view emphasizing the role of IoT in different domains.

https://doi.org/10.1155/2022/7218113

IoMT – definíció és típusok

IoMT, az orvosi eszközök hálózata az IoT technológiákkal (telemedicina, robotika) az egészségügyi ágazatban, amely magába foglalja az infrastrukturálisan és a hálózaton keresztül összekapcsolódó különböző orvosi eszközöket.

- Intelligens hordható eszközök
- Otthoni használatra szánt orvosi eszközök
- Beültethető eszközök
- Pontos gondozási készletek
- Vészhelyzeti reagáló rendszerek
- Virtuális otthoni asszisztens
- Kioszkok
- Szenzorok (RFID) gyógyszerészeti csomagolásban
- Mobil egészségügyi alkalmazások

ENISA – ICT security certification opportunities in the healthcare sector (2018)

IoMT – kategóriák

Table 4. A categorisation of the most common IoMT Devices.

Physiologic Monitoring	Medical Treatment	In-Hospital Connected	Ambient	Additional Devices
Motion sensors	Infusion pumps	MRI	Identification devices	Coordinators
Blood glucose device	ICPs	X-rays	Gyroscope sensors	Network devices
Blood pressure device	Cardiac rhythmic management	Surgical Robotics	Motion sensors	End user devices
Temperature sensor	Smart medical capsules	Prosthetic using Surgical Robotics	Vibration sensors	Databases
Pulse oximetry			Monitoring devices	Servers
Pacemakers			Alarm devices	
EEG sensors			Implantable device Charger	
ECG sensors				
Respiratory rate sensors				
Muscle activity sensors				
Implantable devices				
Pill-line sensors				
Aggregators				

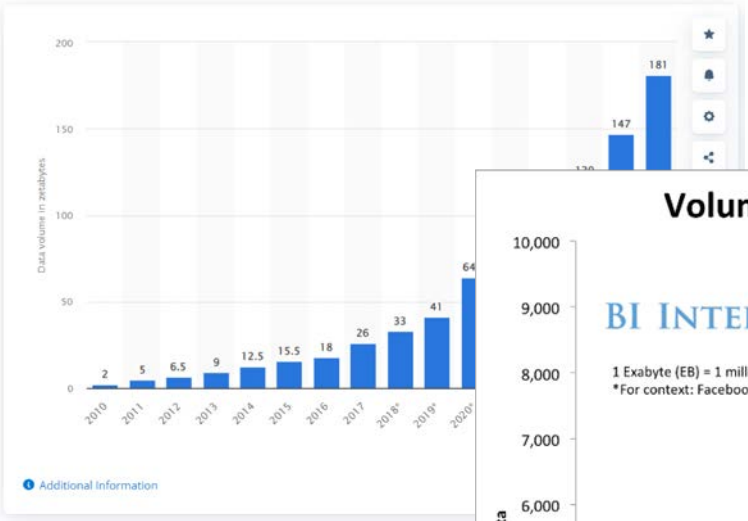
Table 1 **The types and characteristics of medical devices used in the IoMT system.**

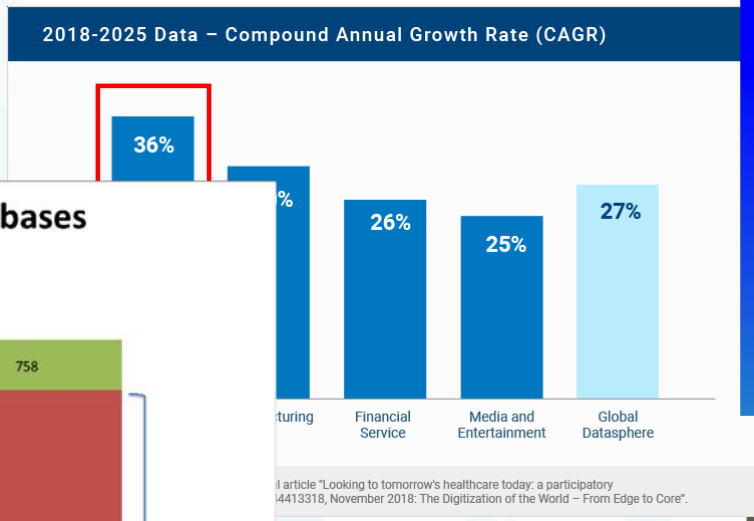
Device type	Placement	Example	Risk Value	References
Implantable	Within the human tissues	deep brain implants, heart pacemaker and insulin pump	High	*Santagati, Dave & Melodia (2020)*
Wearable	On the human body	smart watches, fitness devices	Low	*Tseng, Wu & Lai (2019)*
Ambient	Outside the human body	elderly monitoring devices in smart home	Low	*Pandey & Litoriya (2020)*
Stationary	Inside hospitals	medical image processing devices of MRI and CT-Scan	Low	*Nanayakkara, Halgamuge & Syed (2019)*, *Xu et al. (2019)*

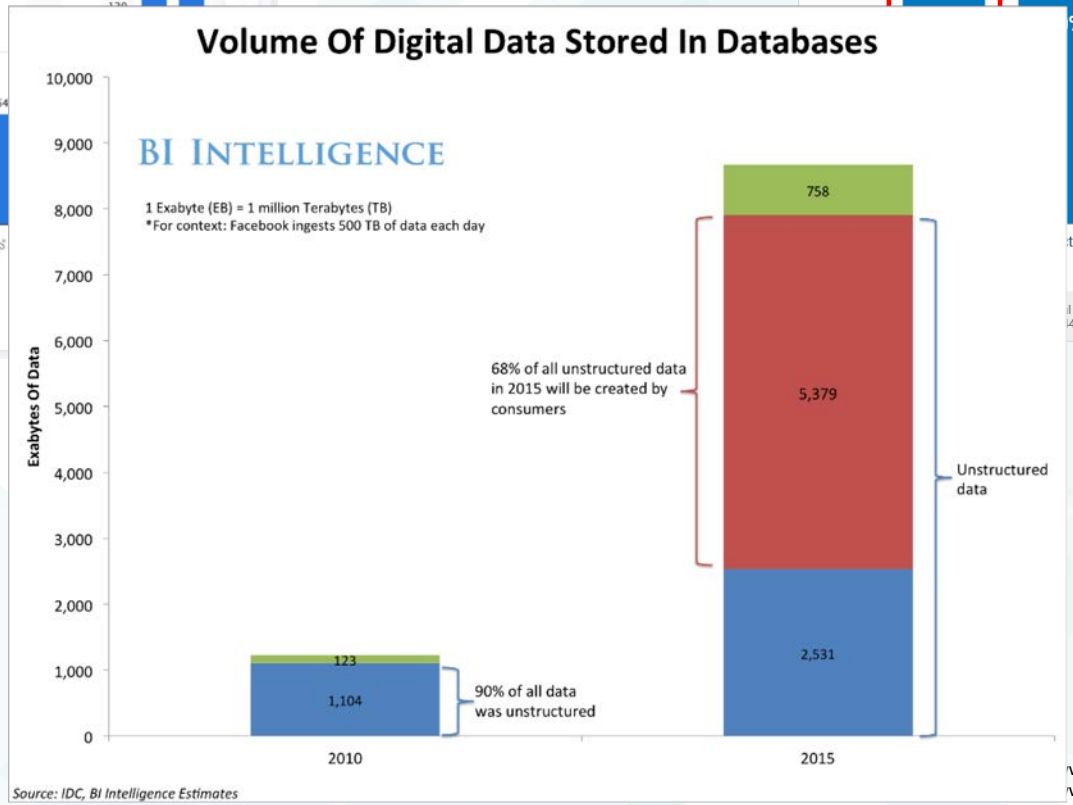
Note:
Each row represents a different type of medical device, and each column represents characteristics of that device.

Koutras et al (2020)

Az adat mennyisége







w.jdsupra.com/legalnews/what-is-data-volume-and-how-to-face-1804605/
w.businessinsider.com/social-medias-big-data-future-2014-3

Kórházak és hálózatok

20-25 ICT készülék/ágy – hálózat!!

Egészségügyi intézmények – hálózati eszközök

To asses the current connectivity status of healthcare devices, we surveyed the field of German hospitals and especially University Medical Center UMCs.

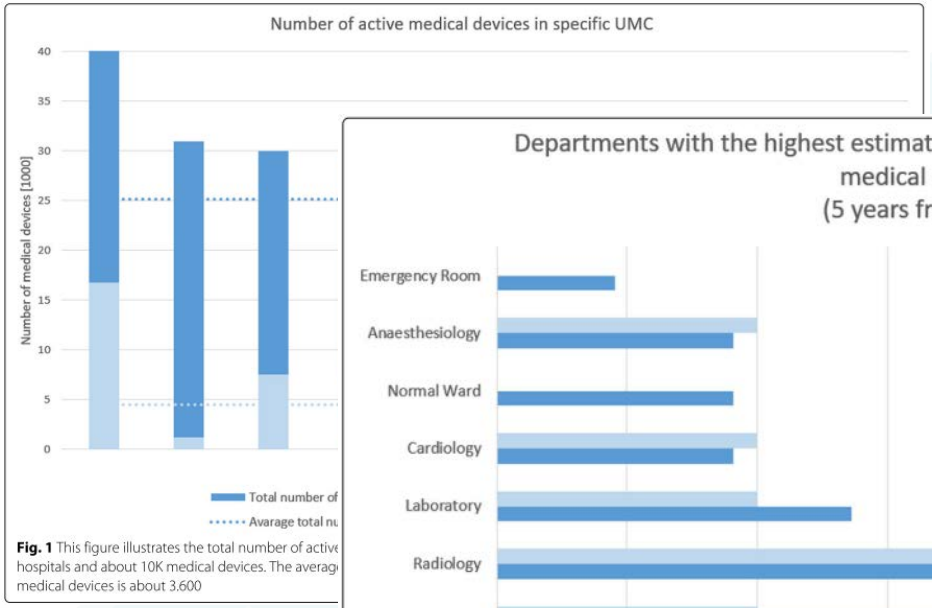
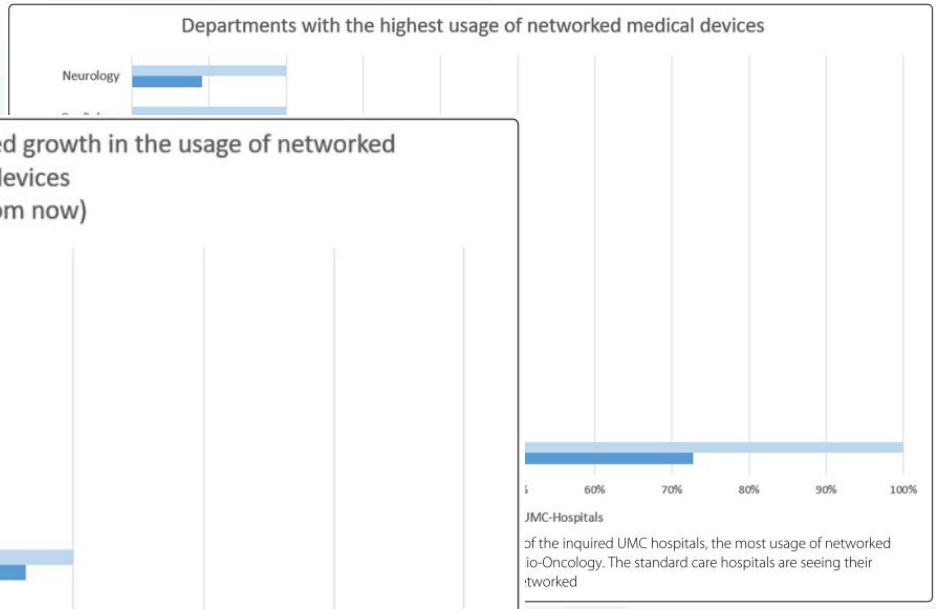


Fig. 1 This figure illustrates the total number of active hospitals and about 10K medical devices. The average medical devices is about 3.600



of the inquired UMC hospitals, the most usage of networked io-Oncology. The standard care hospitals are seeing their tworked

Fig. 5 Lowest usage of networked medical devices: This figure illustrates, that out of the inquired hospitals, the lowest usage of networked medical devices can be found in normal wards in basic care as well as in disciplines of Psych, and Dermatology

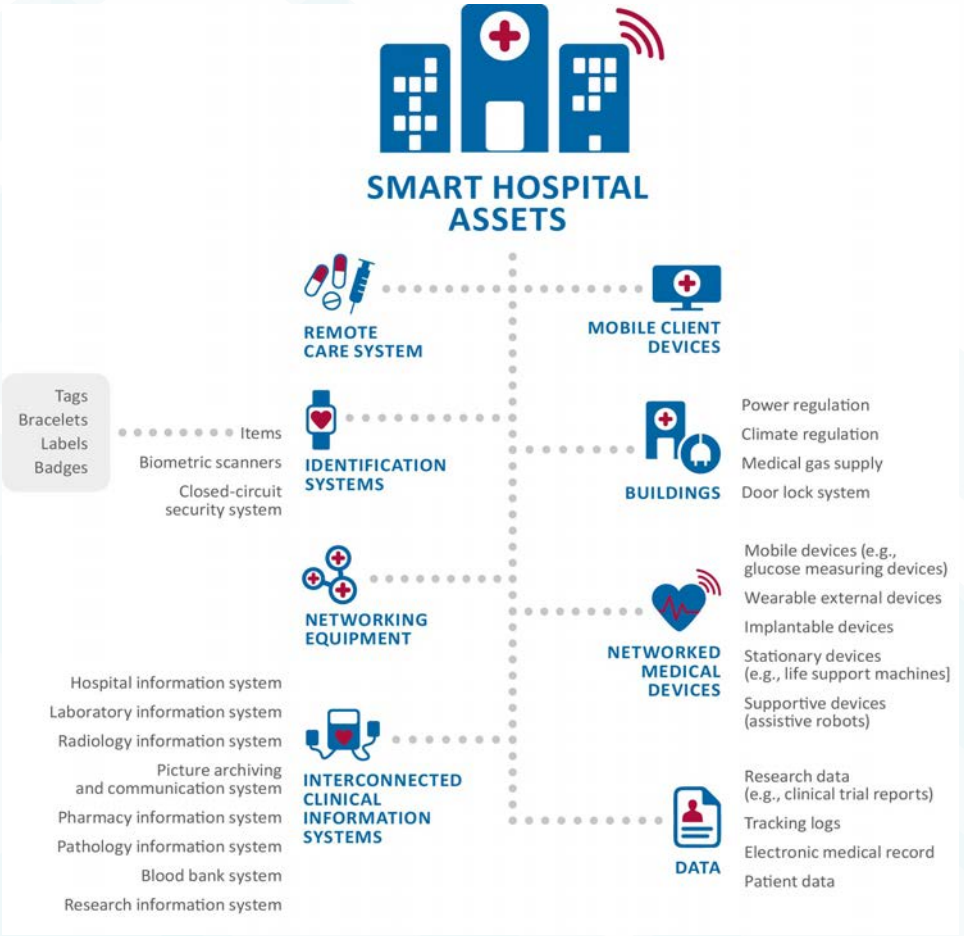
DOI: 10.1186/S12911-020-01259-Y

Adatvezérelt Egészség Divízió

Semmelweis University EMK Health Services Management Training Centre

SMART Hospital – kórházak és hálózatok

Az intelligens kórház az **összekapcsolt eszközök és az információs és kommunikációs technológiák (IKT) környezetére épülő optimalizált és automatizált folyamatokra** támaszkodó kórház, melynek célja a meglévő **betegellátási eljárások javítása és az új képességek** bevezetése.



https://www.enisa.europa.eu/news/enisa-news/diagnosing-cyber-threats-for-smart-hospitals/

Telemedicine in USA – AHA survey

DATA

97%

Patients satisfied with their first telehealth experience and would recommend the program

Source: Harvard Business Review

67%

Percentage of health system CEOs who said integration with clinical workflow is the most important factor when selecting a telehealth technology system from a vendor

Source: Center for Connected Medicine; The Health Management Academy

63%

Percentage of patients who reported "no difference" in the "overall quality of the visit" between a virtual and office visit with a physician

Source: American Journal of Managed Care

$1.41 Billion

2018 venture capital investment in on-demand health care services, including telemedicine

Source: Rock Health

$2,750

Health care providers saved almost $2,750 per patient when using telehealth instead of in-person physical therapy when discharged after knee-replacement surgery

Source: Veritas study, conducted by the Duke Clinical Research Group

80%

Emergency virtual visits wind up "resolving the episode of care" without a trip to the emergency department (ED) or another site of care.

Source: Jefferson Health

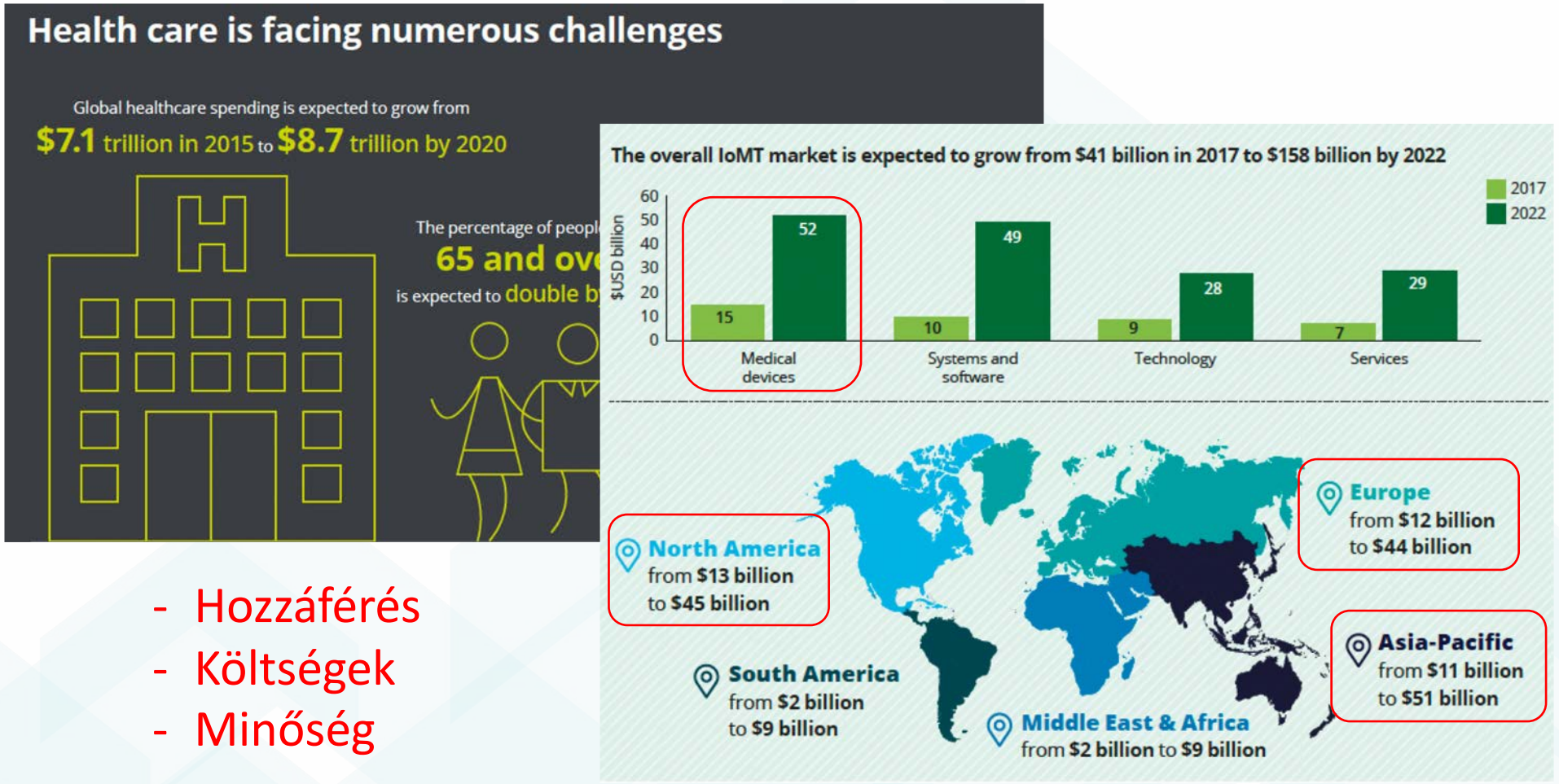
AHA CENTER FOR HEALTH INNOVATION

https://www.aha.org/center/emerging-issues/market-insights/telehealth

Adatvezérelt Egészségügy Divízió

Semmelweis University EMK Health Services Management Training Centre

IoMT és egészségpolitika



- Hozzáférés
- Költségek
- Minőség

Deloitte-Medtech and the Internet of Medical Things (2018)

IoMT – előnyök

Azonnali hozzáférés a tesztek eredményeihez vagy a képekhez
Valós idejű hozzáférés az orvosi adatokhoz
Könnyebb elemzés
Az adatok automatikus korrelációja
Egészségügyi figyelmeztetések
A krónikus betegségek távfelügyelete
Egyszerűbb gyógyszerkezelés
A betegek fokozott érdeklődése
Alacsonyabb egészségügyi költségek

ENISA – ICT security certification opportunities in the healthcare sector (2018)

IoMT – home care példa

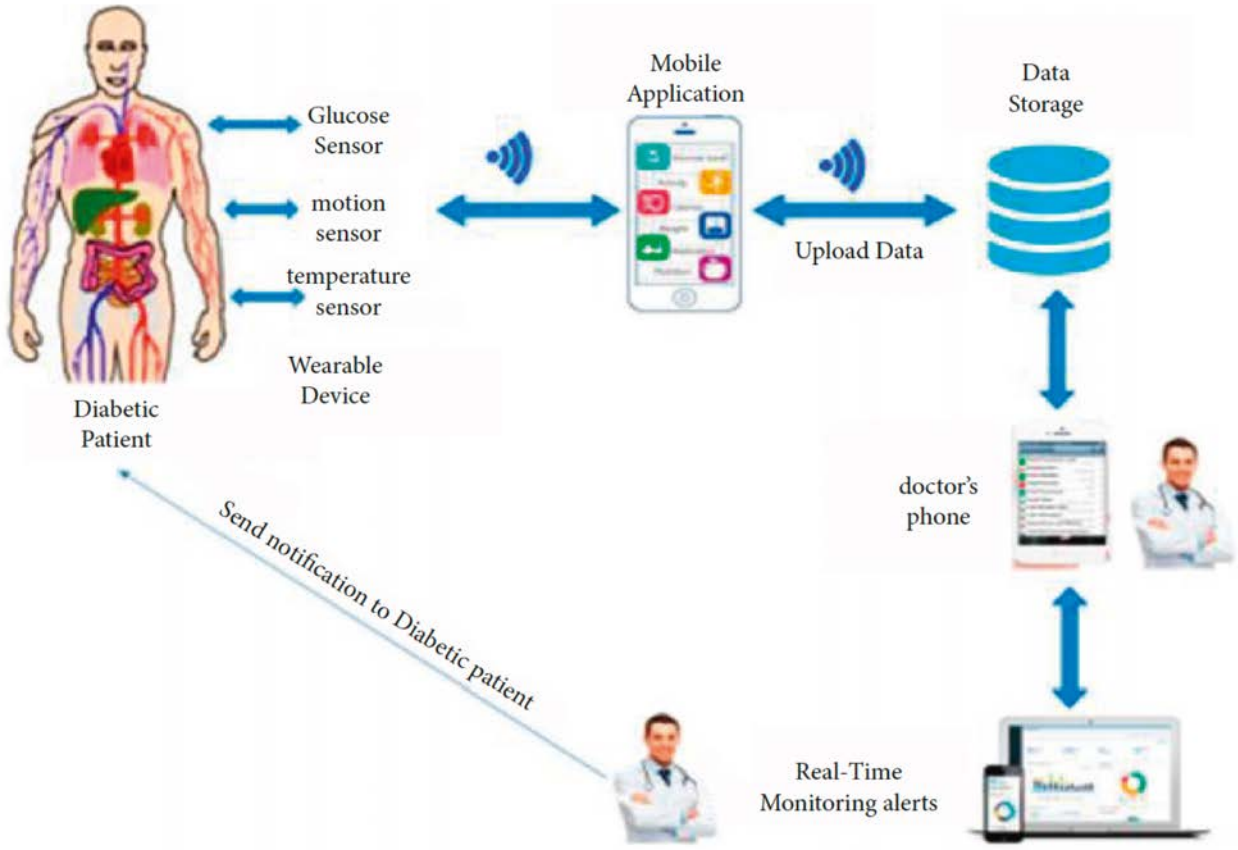
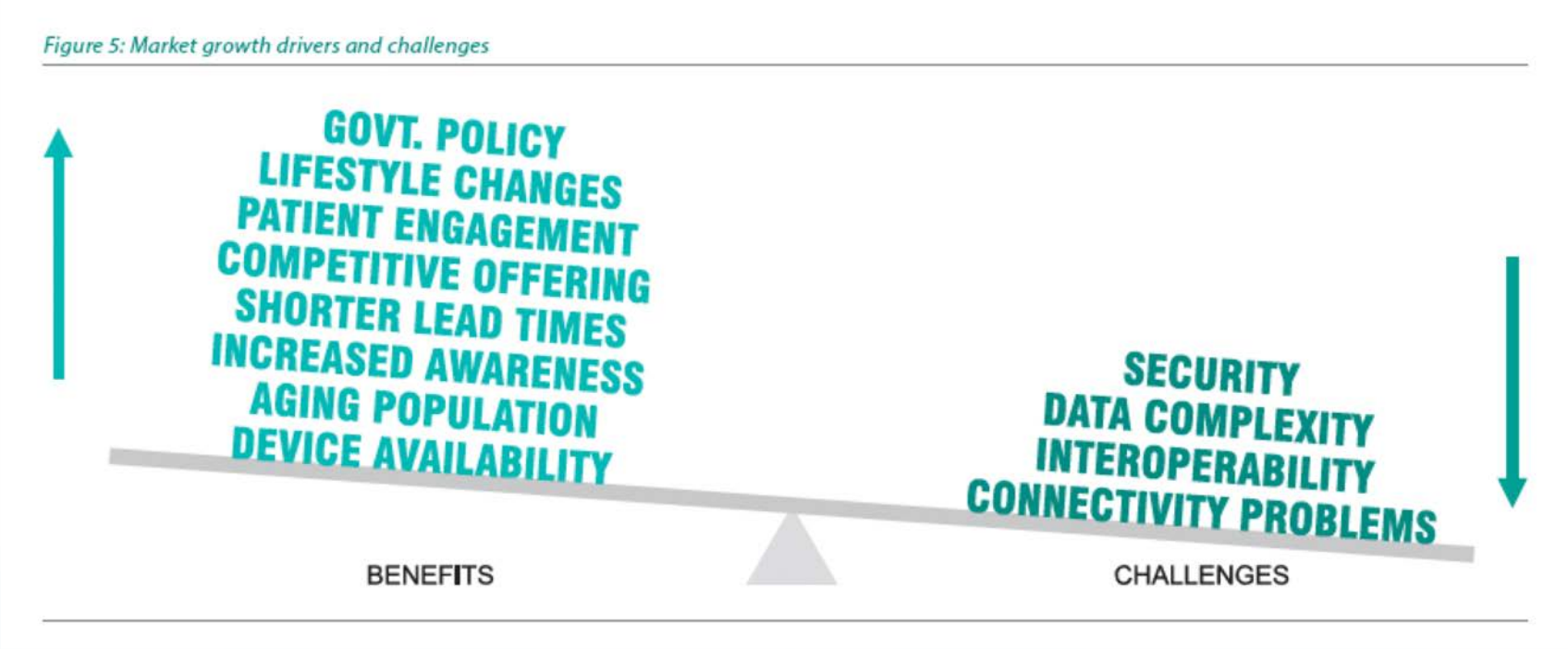


FIGURE 12: Home care example [8, 31].

https://doi.org/10.1155/2022/7218113

IoMT – benefits and challanges



Aranca – Internet of Medical Things (2019)

IoMT - challenges

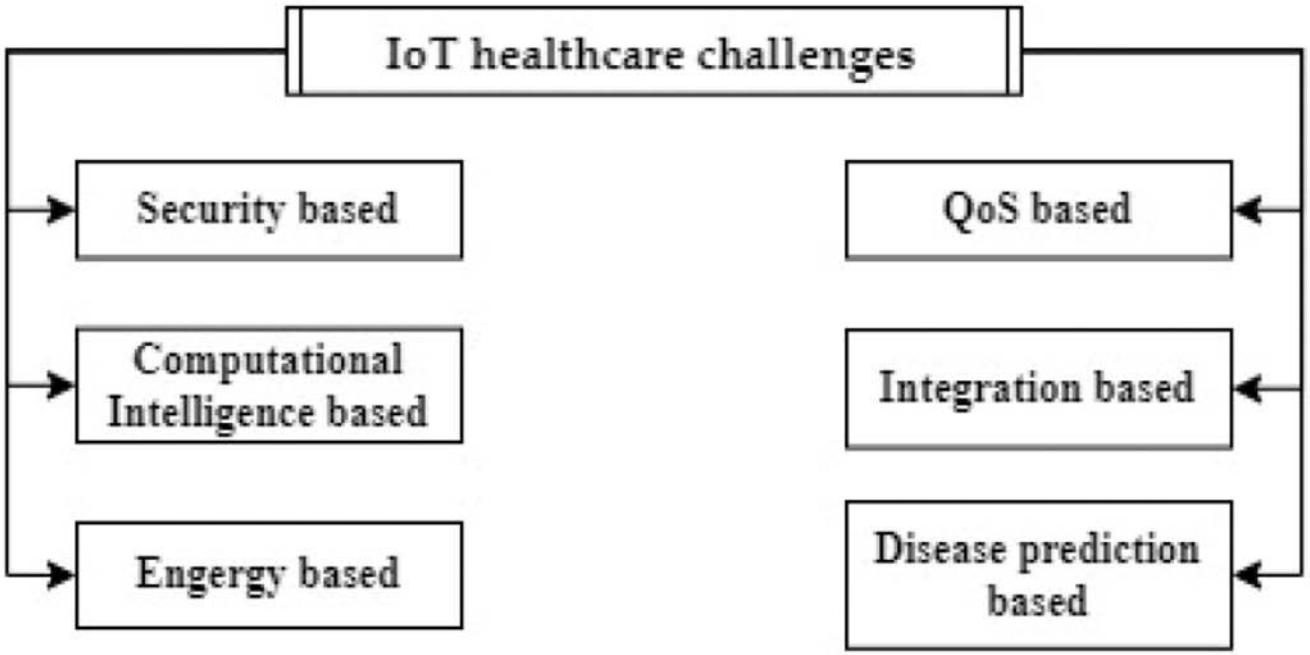
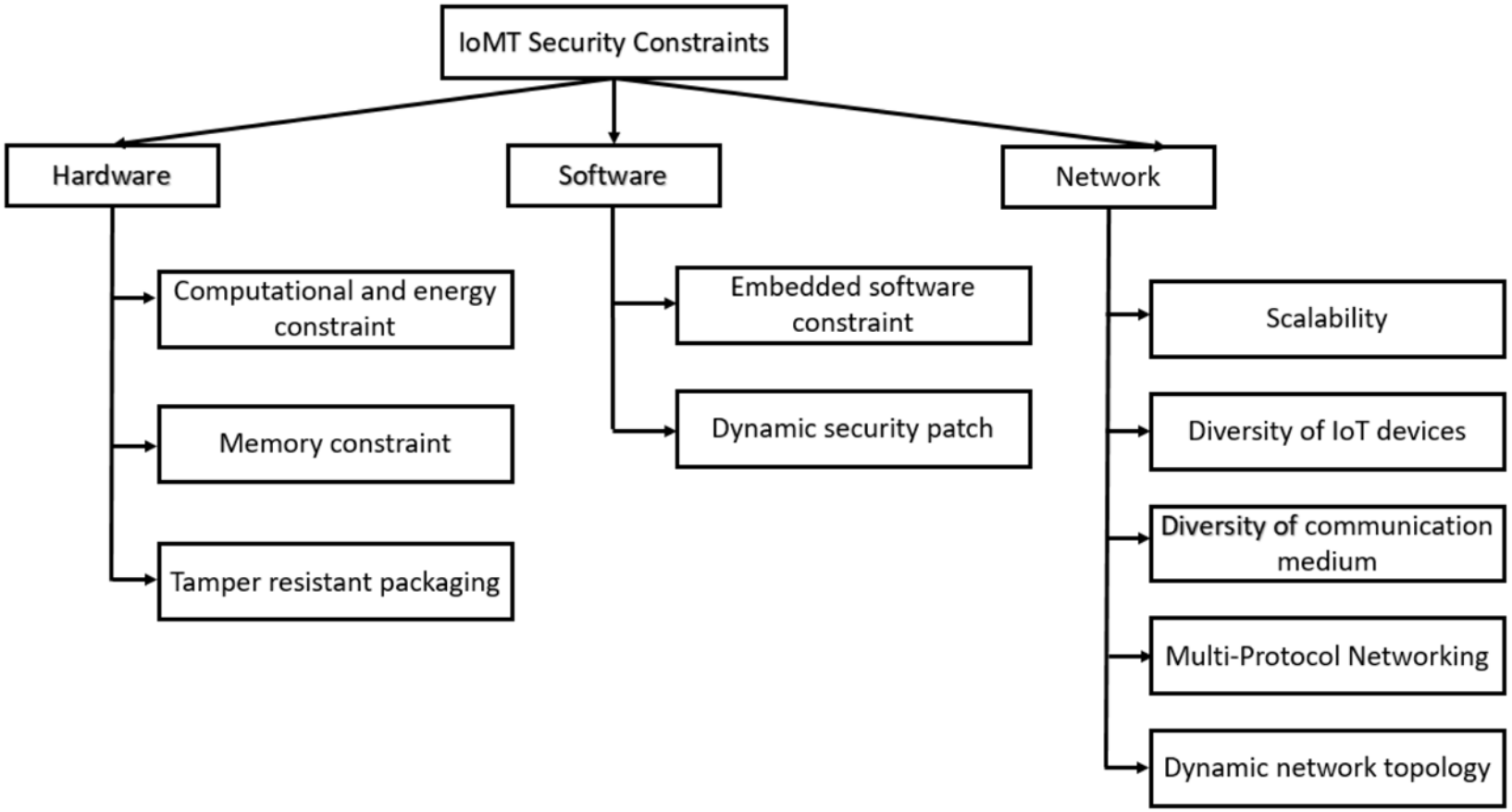


Figure 7. IoT healthcare challenges and open issues.

Abdulmalek et al (2022)

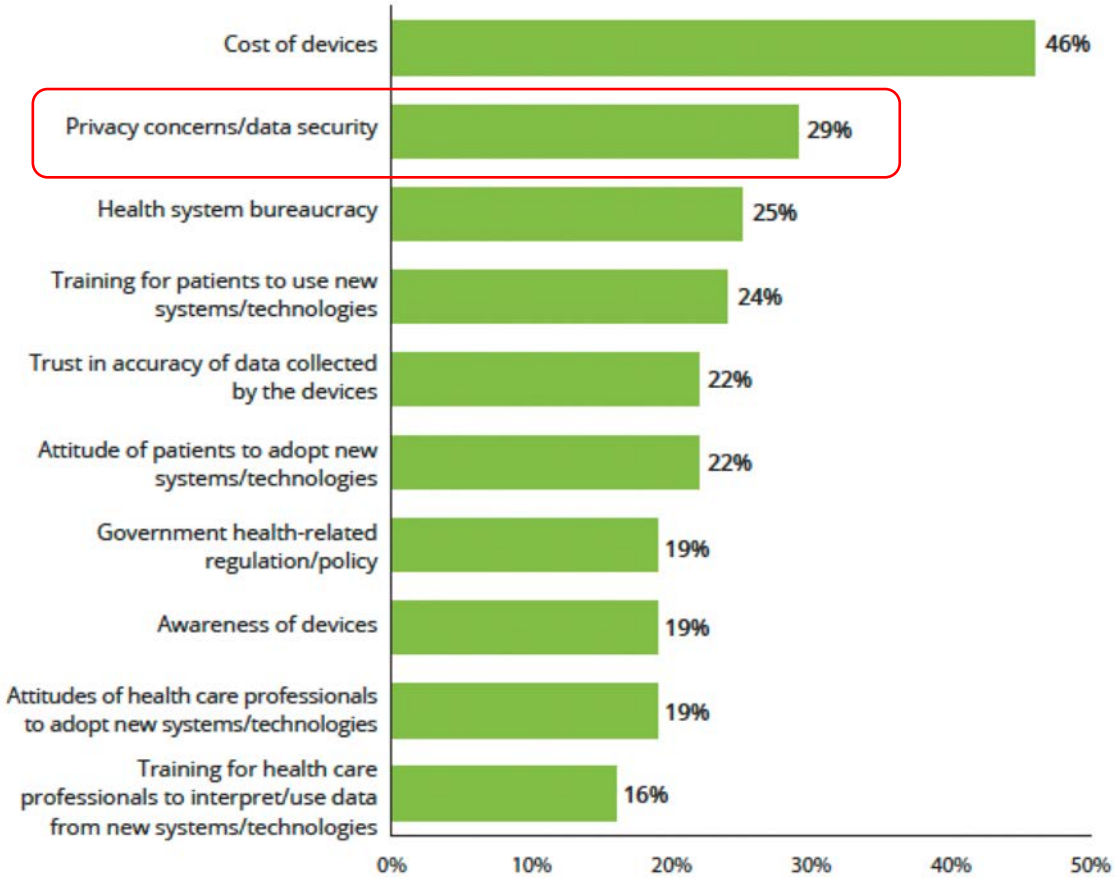
IoMT – security constrains



https://www.sciencedirect.com/science/article/pii/S0167739X19305680

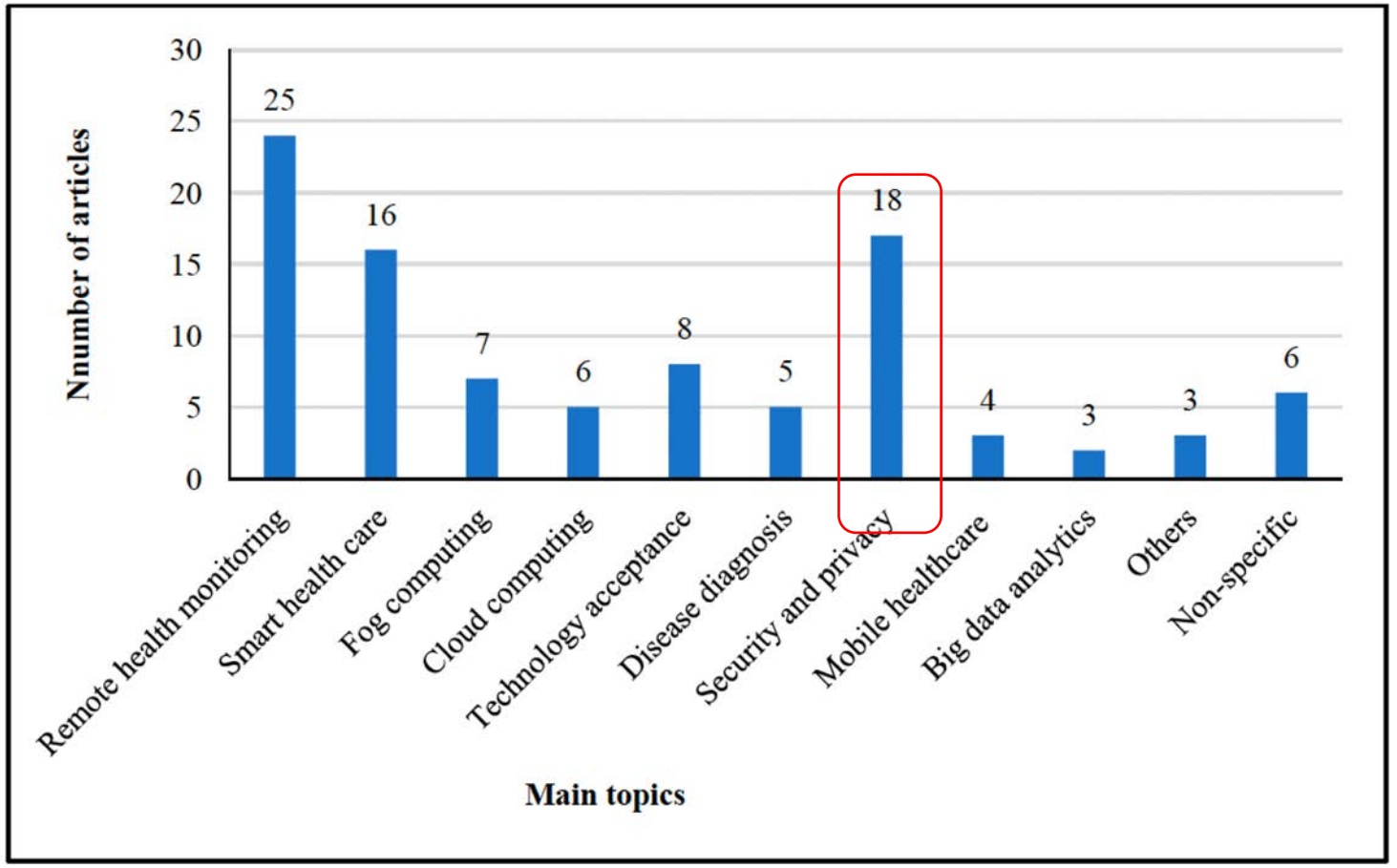
IoMT – akadályozó tényezők

Figure 15: Top ten perceived barriers to adoption of connected technology*



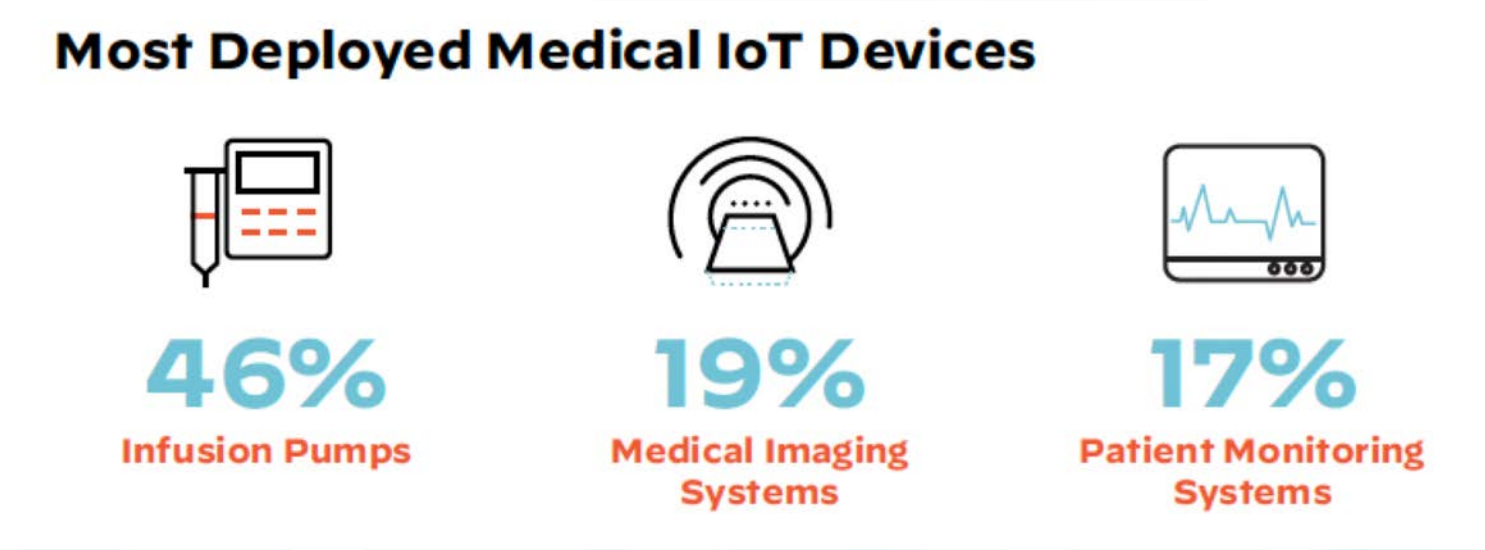
Deloitte-Medtech and the Internet of Medical Things (2018)

IoMT – main topics



Jawad et al (2022)

IoMT – security issues



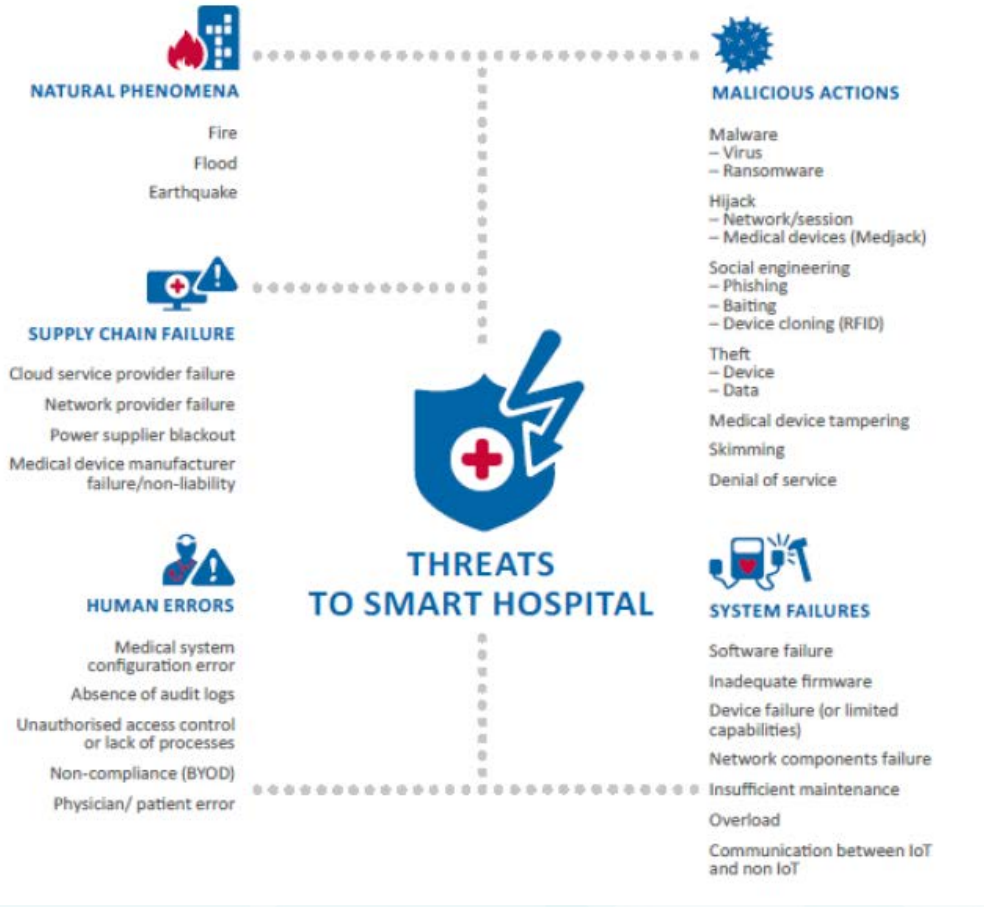
PaloAlto - The Healthcare CISO's Guide to IoT Security (2021)

IoMT – a biztonság a leggyengébb láncszem…

1. Láthatóság
2. Különböző gyártók
3. Nem javított eszközök
4. Régi infrastruktúra, sw
5. Kihasználható sebezhetőségek
6. Tulajdonjog
7. Laza biztonsági konfigurációk/gyakorlatok
8. A hálózati szegmentáció hiánya
9. BYOD a hálózaton, az informatikai szakemberek félelme, a kibertudatosság hiánya, élet-halál helyzetek

CyberTalk – Buyer's Guide to IoMT Security Solutions (2021)

SMART Hospital – fenyegetések



https://www.enisa.europa.eu/news/enisa-news/diagnosing-cyber-threats-for-smart-hospitals/

Kiberbiztonság és kórházi/rendszer működés

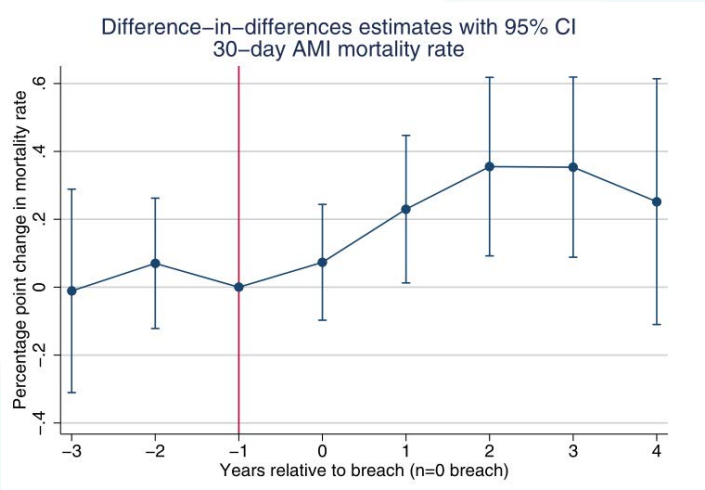
HSR HEALTH SERVICES RESEARCH
Impacting Health Practice and Policy Through State-of-the-Art Research and Thinking

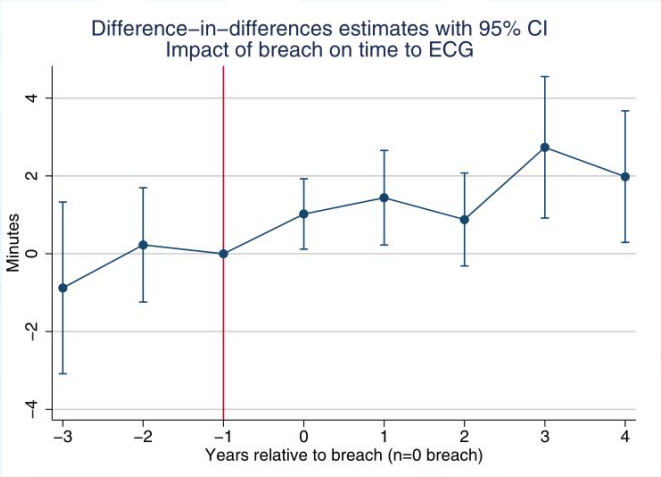
Data breach remediation efforts and their implications for hospital q

Sung J. Choi PhD M. Eric Johnson PhD Christoph U. Lehmann MD

2019. október

Data: 2012- 2016 , Department of Health and Human Services' (HHS) public database on hospital data breaches and Medicare Compare's public data on hospital quality measures, 3025 hospitals with 14 297 unique hospital-year





30 napon belüli AMI halálozás: +36/10 000 eset

Time-to ECG: +2,7 perc

http://www.hsr.org/hsr/abstract.jsp?aid=54980728757
https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks/

IoMT kiberbiztonság - példák

Adatvezérelt Egészség Divízió
Egészségbiztonsági Nemzeti Laboratórium

Semmelweis University
EMK
Health Services Management Training Centre

Kiberbiztonság és beültethető eszközök

Doctors disabled wireless in Dick Cheney's pacemaker to thwart hacking

22 OCT 2013 3

- 1978-2010: öt szívinfarktus, 4x bypass surgery, 2007-ben defibrillátor beültetés
- 2013. október: Dick Cheney bejelenti, hogy a a pm hackelést reális veszélynek gondolták, ezért kikapcsolták a radiofrekvenciás befolyásolás lehetőségét

https://abcnews.go.com/US/vice-president-dick-cheney-feared-pacemaker-hacking/story?id=20621434
https://nakedsecurity.sophos.com/2013/10/22/doctors-disabled-wireless-in-dick-cheneys-pacemaker-to-thwart-hacking

FDA recalls close to half-a-million pacemakers over hacking fears

Security concerns over connected health devices are once again in the spotlight.

Saqib Shah, @eightiethmnt
08.31.17 in Security

4
Comments

1587
Shares

Qubit.

2019. március 22

MEGHEKKELHETŐ DEFIBRILLÁTOROK MIATT ADOTT KI RIASZTÁST AZ USA HADÜGYMINISZTÉRIUMA

03.22. | ♥ 44 — TECH

„Biztonsági rés tátong a Medtronic gyógyászati segédeszközöket gyártó cég által alkalmazott Conexus **kommunikációs protokollban**, figyelmeztetett csütörtökön az **amerikai védelmi minisztérium**. A hiba összesen nagyjából **750 000 készüléket** érinthet, amelyek között **defibrillátor-implantátumok is találhatók**. Több mint húsz típusra adtak ki riasztást, a hackerek a monitorok és a defibrillátorok közti kommunikációt zavarhatják meg, így akár **szívrohamot** is előidézhetnek a betegeknél. ”

„A minisztérium ennek ellenére (nem volt betörés, közelben kell tartózkodni) a **veszélyt egy tízes skálán 9,3-asra értékelte**” - !!!!

https://www.engadget.com/2017/08/31/fda-pacemakers-abbott-hacking/

Adatvezérelt Egészség Divízió
Egészségbiztonsági Nemzeti Laboratórium

Semmelweis University
EMK
Health Services Management Training Centre

Kiberbiztonság az inzulinpumpákban

Security

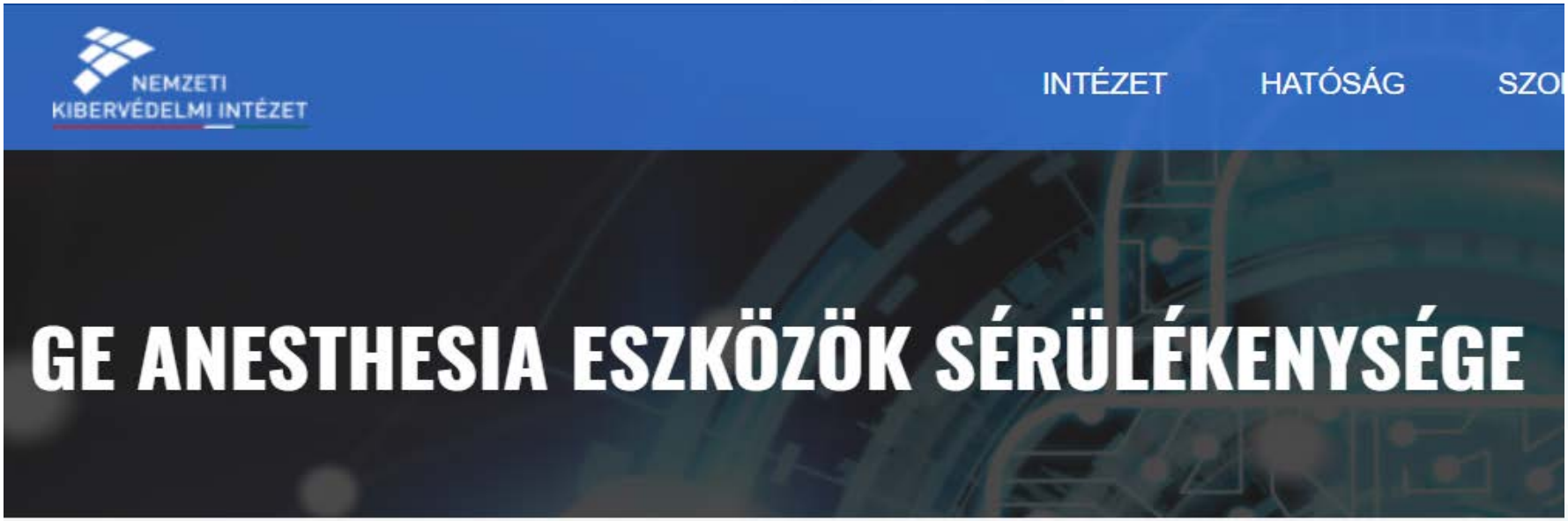
Insulin pump hack delivers fatal dosage over the air

Sugar Blues, James Bond style

By Dan Goodin 27 Oct 2011 at 06:23 90 SHARE ▼

- 2011-ben egy MacAffee szakértő (**Barneby Jackson**) demonstrálta, hogy hogyan hekkelhető meg egy inzulinpumpa akár több száz méter távolságról is…..
- A gyártási szám ismerete nélkül, a 25 egység helyett 300 egységet tudott beadni úgy, hogy **a pumpa nem jelezte az eltérést**

Kiberbiztonság és anesztézia



CH azonosító: CH-14654

Cím: GE Anesthesia eszközök sérülékenysége

Angol cím: GE Aestiva and Aespire Anesthesia

Publikálás dátuma: 2019.07.10.

achines/

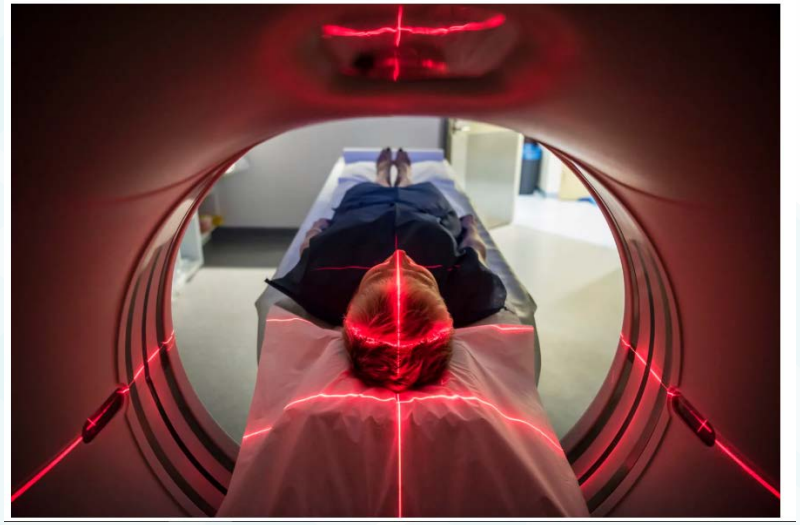
Kiberbiztonság és képalkotás

The Washington Post
Democracy Dies in Darkness

2019. április 3

Hospital viruses: Fake cancerous nodes in CT scans, created by malware, trick radiologists

Researchers in Israel created malware to draw attention to serious security weaknesses in medical imaging equipment and networks.



CT-GAN: Malicious Tampering of 3D Medical Imagery using Deep Learning

Yisroel Mirsky[1], Tom Mahler[1], Ilan Shelef[2], and Yuval Elovici[1]
[1]Department of Information Systems Engineering, Ben-Gurion University, Israel
[2]Soroka University Medical Center, Beer-Sheva, Israel
yisroel@post.bgu.ac.il, mahlert@post.bgu.ac.il, shelef@bgu.ac.il, and elovici@bgu.ac.il

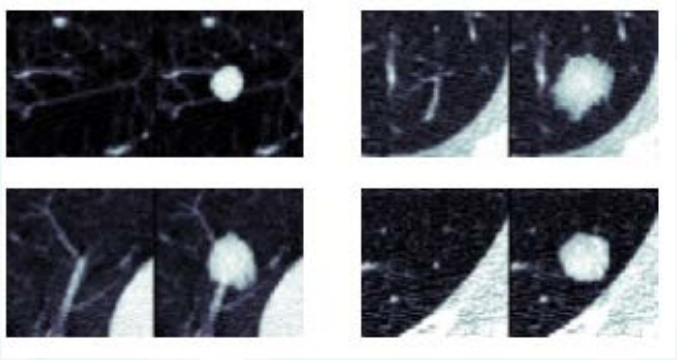
D2+ Adatvezérelt Egészség Divízió
Egészségbiztonság Nemzeti Laboratórium

Semmelweis University EMK Health Services Management Training Centre

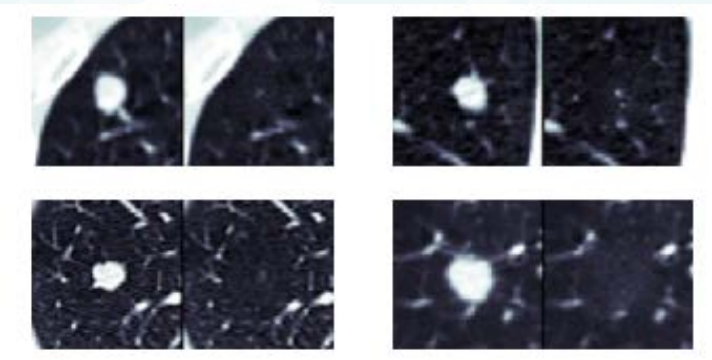
Kiberbiztonság és képalkotás

- Izraeli kutatók kifejlesztettek egy rosszindulatú szoftvert, hogy felhívják a figyelmet a diagnosztikai eszközök és hálózatok biztonsági hiányosságaira
- Mellkas CT felvételek manipulálása (tüdőrákos elváltozás elhelyezése és eltávolítása)
- Nem csak elméleti felvetés: 3 tapasztalt radiológust sikerült megtéveszteni
- Beláthatatlan következmények: **félrekezelések, klinikai vizsgálatok szabotálása, választások befolyásolása…**

Injection



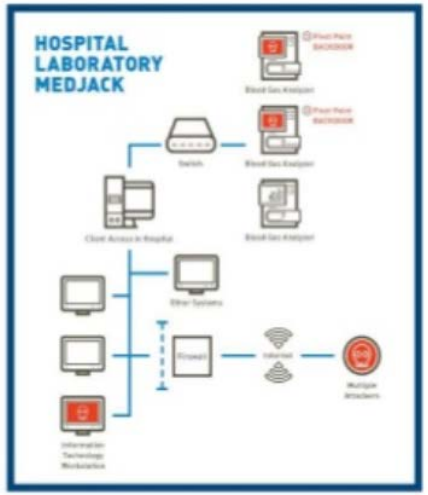
Removal



Forrás: Mirsky Y, Mahler T, Shelef I et al.: CT-GAN: Malicious Tampering of 3D Medical Imagery using Deep Learning, arXiv:1901.03597 [cs.CR], 3. April 2019

Kiberbiztonság és a laboratóriumok

Incidents Case Study



The customer had a very strong industry suite of cyber products. This included a strong firewall, intrusion detec (heuristics based), endpoint security and anti-virus and

Infection of one of the hospital IT department's workstati identified this infection point separately and we do susp connected.

Attacker has established a backdoor within our target bl analyzer, or any other medical device, almost any form manipulation of the unencrypted data stored and flowing device is possible.

MEDJACK attack vector has the potential to distort or internal data

The malware (net.sah.worm.win32.kino.kf) has been im re-manufacturing (packing, polymorphism and junk cod and encryption such that the signatures are no longer ob

EGÉSZSÉGÜGYI KUTATÓKÖZPONTOK UTÁN KÉMKEDNEK A KÍNAI HACKERCSOPORTOK

augusztus 23. 08:04

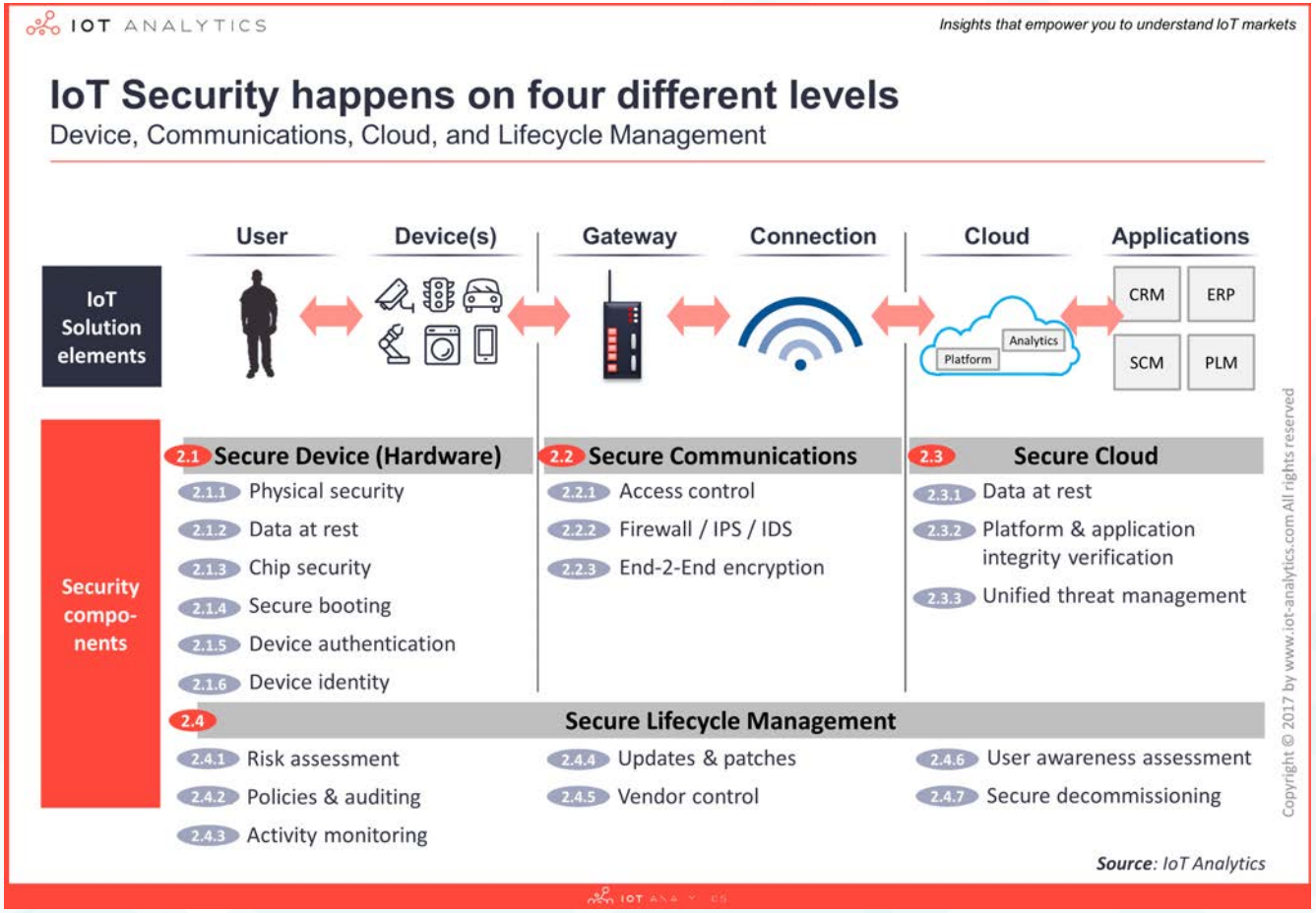
A FireEye egy a héten kiadott jelentése szerint továbbra is az egészségügyi kutatásokban résztvevő szervezetek, azok közül is leginkább...

https://nki.gov.hu/it-biztonsag/hirek/egeszsegugyi-kutatokozpontok-utan-kemkednek-a-kinai-hackercsoportok/
https://www.slideshare.net/vdesibabu/cybersecurity-medical-devices

Adatvezérelt Egészség Divízió

Semmelweis University EMK Health Services Management Training Centre

IoT security issues and attack



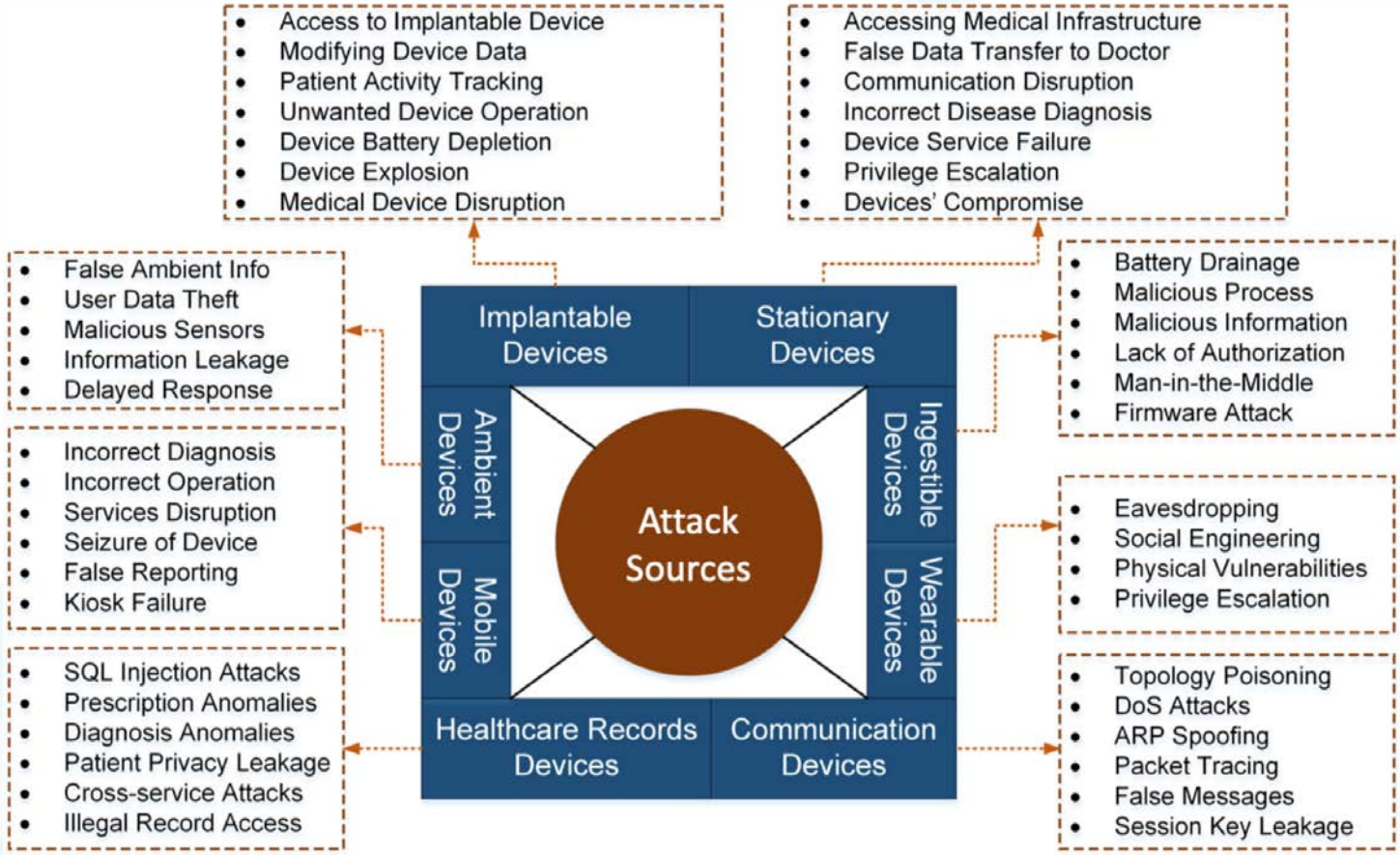
https://iot-analytics.com/5-things-to-know-about-iot-security/

IoMT security issues and attack - layers

Architectural Layers	Core Components	Major Functionalities	Common Security Issues
Device sensing layer	Smart sensors, actuators, RFID tags	Data sensing, data acquisition	Authentication, authorization and access control.
Network management layer	Wired, wireless networks, big data repositories	Data aggregation, QoS scheduling	Unauthorized access, modification of routing paths.
Service composition layer	Middle-ware technology, heterogeneous objects	Analysis and processing of data	Service (or group) authentication, data confidentiality.
Application layer	Various applications e.g., smart home, smart city	Determines massage passing protocols	Unauthorized access, privacy leakage, integrity.
User interface layer	Users	Export services to the end-users	Authentication and authorization, data confidentiality.

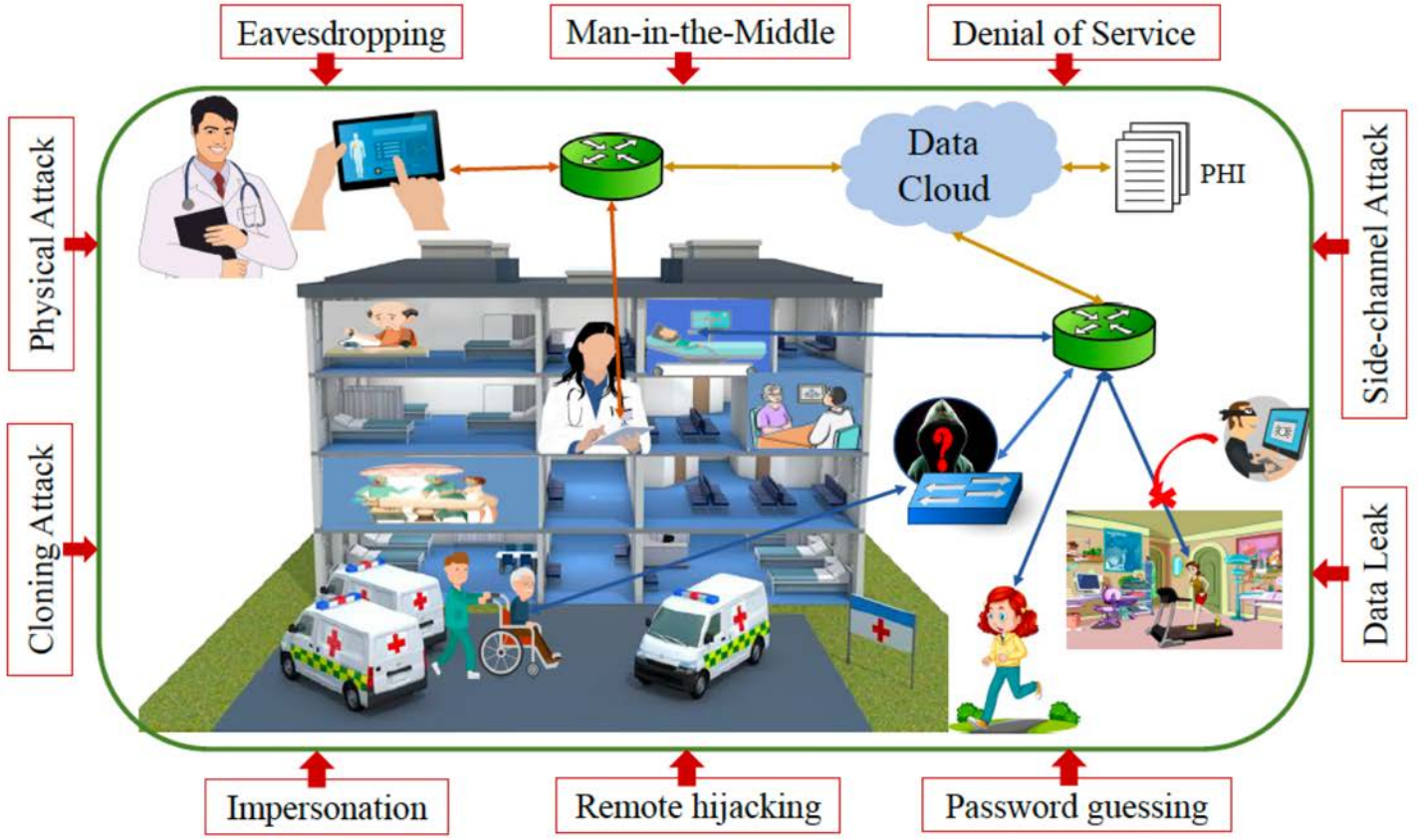
Pal et al (2020)

IoMT security issues and attack - devices



https://www.sciencedirect.com/science/article/pii/S1084804522000017

IoMT security issues and attack - ecosystem



Sadhu et al (2022)

IoMT szabályozás, ajánlások

Adatvezérelt Egészség Divízió
Egészségbiztonsági Nemzeti Laboratórium

Semmelweis University
EMK
Health Services Management Training Centre

Medical device regulations

United States Congress just before the end of 2022 aproved a bill that compel companies that make internet-connected medical devices to ensure the security of their products. The bill provides the health and human services authority the power to issue requirements and regulations relevant to the cybersecurity of connected medical devices.

The **European Union** has its MDR, IVDR, NIS22, CRA, which mandate cybersecurity requirements for IoT products including medical devices.

Japan's Ministry of Health, Labor and Welfare (MHLW) updated its regulations for medical devices in early 2022 to emphasize cybersecurity.

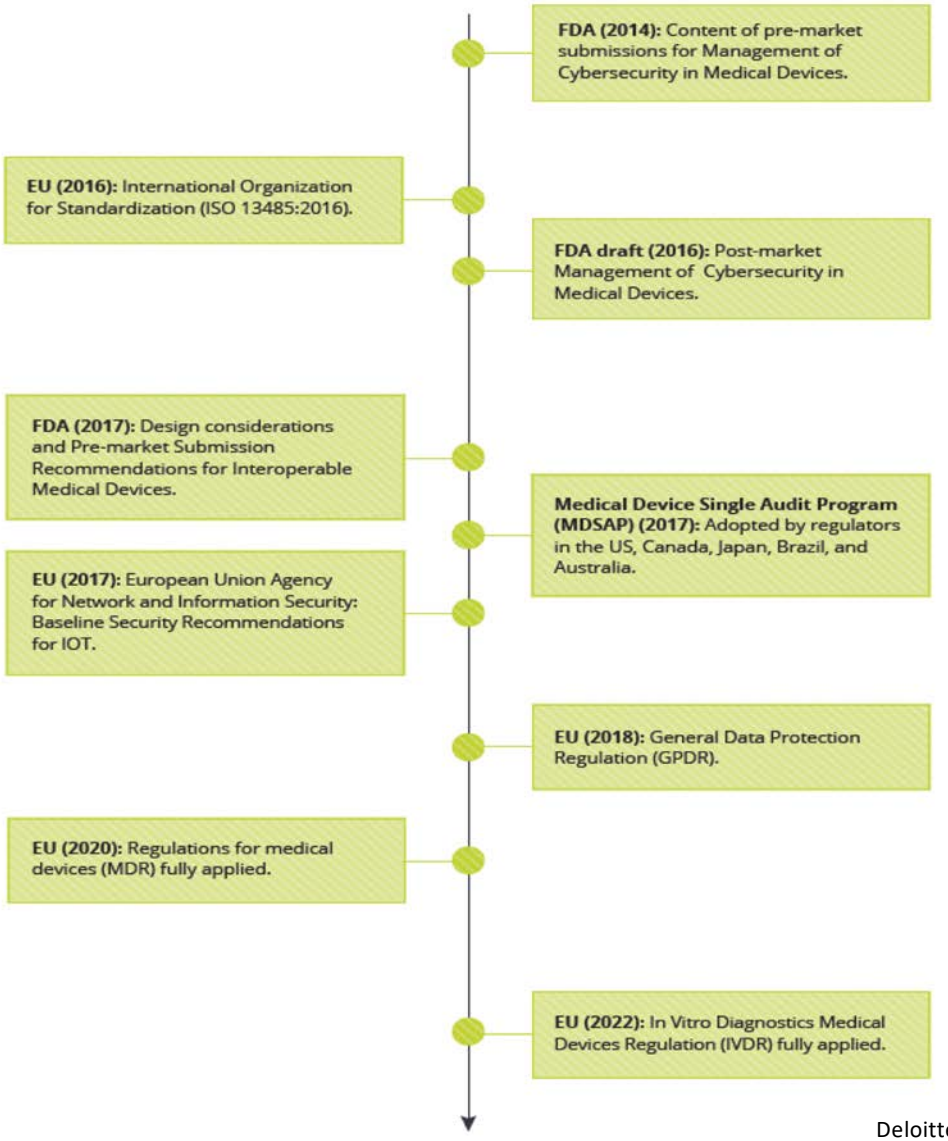
China's Center for Medical Device Evaluation (CMDE) has new "guiding principles" for medical software used in 18 product categories.

The United Kingdom is also working on a new bill called the Product Security and Telecommunications Infrastructure Bill, which aims to ascertain the cybersecurity of various web-enabled devices including those used in healthcare.

https://www.hackread.com/medical-device-regulation-technology/

Szabályozás

Figure 12: Timeline of key regulatory changes impacting medical devices



NIS2
CRA
AI Act
FDA

Deloitte-Medtech and the Internet of Medical Things (2018)

IoMT – risk categories (FDA)

A) **I. osztályú vagy non-invazív eszközök:** Az ebbe a kockázati kategóriába tartozó termékek alacsony és közepes kockázatúak. Ilyenek például a laboratóriumi berendezések és a nem gyógyszeres steril kötszerek.
B) **II. osztályú vagy invazív eszközök.** Az ebbe a kockázati kategóriába tartozó termékek közepes és magas kockázatúak. Ilyenek például a lélegeztetőgépek és az infúziós pumpák.
C) **III. osztályú vagy aktív eszközök**. Az ebbe a kategóriába tartozó termékek általában életfenntartó funkciókat biztosítanak. Példa: beültetett eszközök; pacemakerek, agystimulátorok.

CyberTalk – Buyer's Guide to IoMT Security Solutions (2021)

IoMT – MDR

Az európai jogszabályok bejelentési kötelezettséget vezetnek be a kórházak számára. Egyes esetekben az értesítésnek követnie kell az ellátási láncot. Ezt előre kell látni a beszerzési eljárás során.

Az MDR-ben (Medical Devices/SW) meghatározott általános biztonsági és teljesítménykövetelmények a következők:

ismételhetőség, megbízhatóság és teljesítmény a tervezett felhasználásnak megfelelően
a **fejlesztési életciklus, kockázatkezelés, verifikáció és validáció** elvei
szoftverek használata mobil számítástechnikai platformokkal kombinálva
IT biztonsági intézkedések, beleértve a jogosulatlan hozzáférés elleni védelmet

Az **Orvostechnikai Eszközök Koordinációs Csoportja (MDCG) 2019** decemberében közzétette az Útmutató az orvostechnikai eszközök kiberbiztonságához című dokumentumot, hogy útmutatást adjon a gyártóknak az MDR összes vonatkozó alapvető követelményének teljesítéséhez. Ezek az orvostechnikai eszközökről szóló rendelet I. mellékletében felsorolt kiberbiztonsági követelmények a forgalomba hozatal előtti és a forgalomba hozatalt követő szempontokkal egyaránt foglalkoznak. Az MDCG valamennyi tagállam képviselőiből áll, elnöke pedig az Európai Bizottság képviselője. Az orvostechnikai eszközökkel foglalkozó csoport tanácsokkal látja el a Bizottságot, és segíti a Bizottságot és a tagállamokat az orvostechnikai eszközökre vonatkozó rendeletek harmonizált végrehajtásának biztosításában.

ENISA - PROCUREMENT GUIDELINES FOR CYBERSECURITY IN HOSPITALS (2020)

Medical device – standard

Standard	Description
ISO 13485	ISO 13485 defines the requirements that a quality management system must meet for the design and manufacture of medical devices. This regulation is based to some extent on ISO 9001. ISO 13485 requires only that the certified organization demonstrate the quality system is effectively implemented and maintained and is often seen as the first step in achieving compliance with European regulatory requirements.
ISO 14971	ISO 14971 establishes the standard recommended for medical device risk management to determine the safety of a medical device during the product life cycle. Such activity is required by higher level regulation (EU directives 93/42/EEC, 90/385/EEC and 98/79/EEC) and other quality management system standards such as ISO 13485. Technical report **ISO/TR 24971,** also from ISO, provides guidance on the application of this standard.
MDS2	The standard, ANSI/NEMA HN 1-2019, Manufacturer Disclosure Statement for Medical Device Security, consists of the MDS2 form and instructions for completing it. The updated MDS2 calls for medical device manufacturers to use a new spreadsheet, which is included in the document, to describe their products' security features in order to ease healthcare organisations' efforts to perform risk assessments and protect the data created, received, transmitted, or maintained by their medical devices. Healthcare organisations can use data in the new MDS2 form to compare equipment from different manufacturers and make informed purchasing decisions that comply with their security and privacy policies.
ISO 15225:2016 (withdrawn)	ISO 15225:2016 specified rules and guidelines for a medical device nomenclature data structure, in order to facilitate cooperation and exchange of data used by regulatory bodies on an international level between interested parties. Included guidelines for a minimum data set and its structure. These guidelines are provided for system designers setting up databases that utilize the nomenclature system described herein. The requirements contained in this International Standard were to be applicable to the development and maintenance of an international nomenclature for medical device identification.

ENISA - PROCUREMENT GUIDELINES FOR CYBERSECURITY IN HOSPITALS (2020)

IoT - guideline

IoMT – clinical guideline

Guideline

Clinical guidelines on the application of Internet of Things (IOT) medical technology in the rehabilitation of chronic obstructive pulmonary disease

Xiang et al (2021)

IoMT – Paolo Alto 6 lépés a biztonságért

1. **Teljes áttekintést** szükséges az összes IoMT-eszközről az egészségügyi szolgáltatást nyújtó szervezetében
2. **Proaktívan kell csökkenteni a kockázatot** az IoMT eszközök folyamatos kockázatfigyelésével és értékelésével
3. Használj **automatizált eljárásokat** a kockázatalapú biztonsági politika végrehajtása érdekében
4. **Gyorsan** lépj az ismert fenyegetések megelőzése érdekében
5. Ismeretlen fenyegetések **észlelése után gyorsan reagálj**
6. Szerezzen **működési ismereteket** a klinikai és orvosbiológiai csapatok számára

PaloAlto - The Healthcare CISO's Guide to IoT Security (2021)

IoMT – 6 lépés – 6. (példa)

6. Szerezzen működési ismereteket a klinikai és orvosbiológiai csoportok számára

A legtöbb orvostechnikai eszköz a nem éri el a teljes kihasználtságot, és gyakran olyan tőke- és működési kiadásokat jelentkenek, amelyek szükségtelen kiadásokat eredményeznek. Ezen túlmenően, mivel az orvosi eszközöket a Hatóság szabályozza, minden rajtuk lévő szoftverfrissítést az eredeti berendezés gyártójának (OEM) felül kell vizsgálnia annak ellenőrzése érdekében, hogy a szoftvermódosítások továbbra is fennállnak annak érdekében, hogy az eszköz biztonságos legyen a betegek számára. Azoknak az egységeknek, amelyek az orvostechnikai eszközök használatának vagy kezelésének ezekkel a szempontjaival foglalkoznak, gyakorlatias üzleti és működési ismeretekre van szükségük, amelyek révén optimalizálhatják a költségeket, miközben tájékozottak maradnak arról, hogy az eszköz mikor állhat készen a javításra és a szoftverfrissítésekre. A megoldásból származó működési betekintések segítenek a csapatoknak azonosítani az eszközöket, szükség szerint beépíteni azokat, a használati adatok alapján optimalizálni a teljesítményüket, és biztonságosan kivonni őket az iparági előírásoknak megfelelően **(business and machine data)**

Az ideális IoMT biztonsági megoldásnak a következőket kell tennie:

- Nyomon követi és jelentéseket készít az egyes orvosi eszközök eszközhasználati statisztikáit és a döntések előkészítésben részt kell venni.
- Csúcshasználati időket előtt a megelőző karbantartások és a szoftverfrissítések megtervezése szükséges
- Analitikai adatokat (machine data) biztosít a képalkotó eszközök használatáról, beleértve azt is, hogy mely munkatársak használják az eszközöket, és hogyan használják őket
- Gyorsan kell kezelni a gyártói értesítéseket, az FDA visszahívásait és a problémákat – ehetőleg egy helyen
- A leltári- nyilvántartási rendszerek frissítése szükséges, és folyamatosan naplót kell vezetni az eszközökről
- Monitorozni kell a betegrekordokat, ami révén feltárható, hogy hogyan használják és tárolják az egyes eszközök az adatokat,

PaloAlto - The Healthcare CISO's Guide to IoT Security (2021)

IoMT – CISA - Zero Trust Architecture

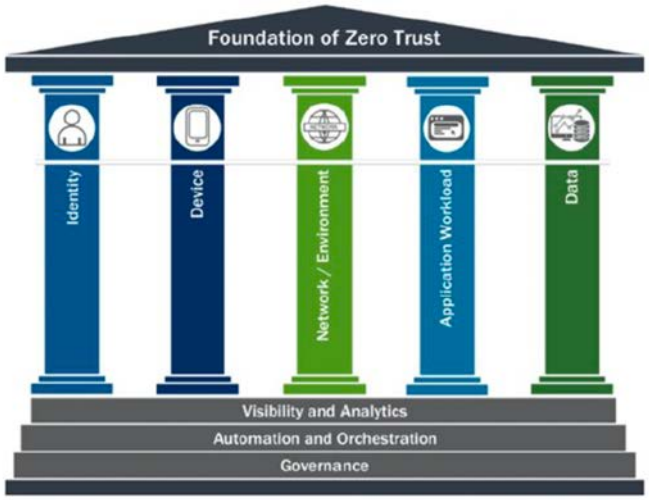


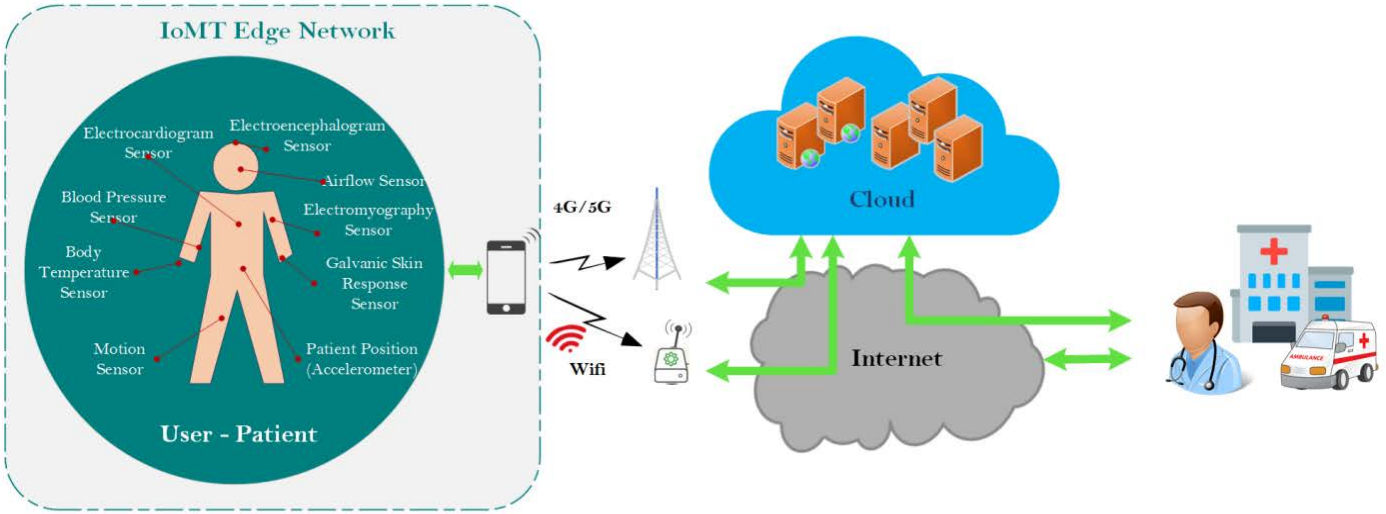
Figure 1 Foundation of Zero Trust

"The Zero Trust Maturity Model represents a gradient of implementation across five distinct pillars, where minor advancements can be made over time toward optimization. The pillars, depicted in Figure 1, include Identity, Device, Network, Application Workload, and Data. Each pillar includes general details regarding Visibility and Analytics, Automation and Orchestration, and Governance. This maturity model is one of many paths to support the transition to zero trust."

1. Az orvostechnikai eszközök kézi kezelése **munkaigényes**, mivel a legtöbb egészségügyi intézményben nagy az eszközök száma.
2. A szolgáltatóknak eszközökre van szükségük a **hálózati mikroszegmentáció, a szabályzat érvényesítésének, a sebezhetőség azonosításának, valamint a végpontészlelés és válaszadás** kezeléséhez.
3. **Orvosi eszköz kezelő programra** van szükség az összes eszköz láthatóságának és leltárának biztosításához, beleértve a helyüket is.
4. A hatékony engedélyezési döntések érdekében a programnak tartalmaznia kell az **eszköz ujjlenyomatát**.
5. Az orvostechnikai eszközök kezeléséhez **speciális termékek** állnak rendelkezésre, amelyek közül néhány képes azonosítani a sebezhetőséget és a kockázatokat.
6. A választott eszköznek **átfogó képet kell adnia** az orvostechnikai eszközök ökoszisztémájáról.

CISA – Medical Devices in Zero Trust Architecture (2023)

IoMT ökoszisztéma vizsgálata –
GOKI-SE-NBSZ/NKI-Alverad

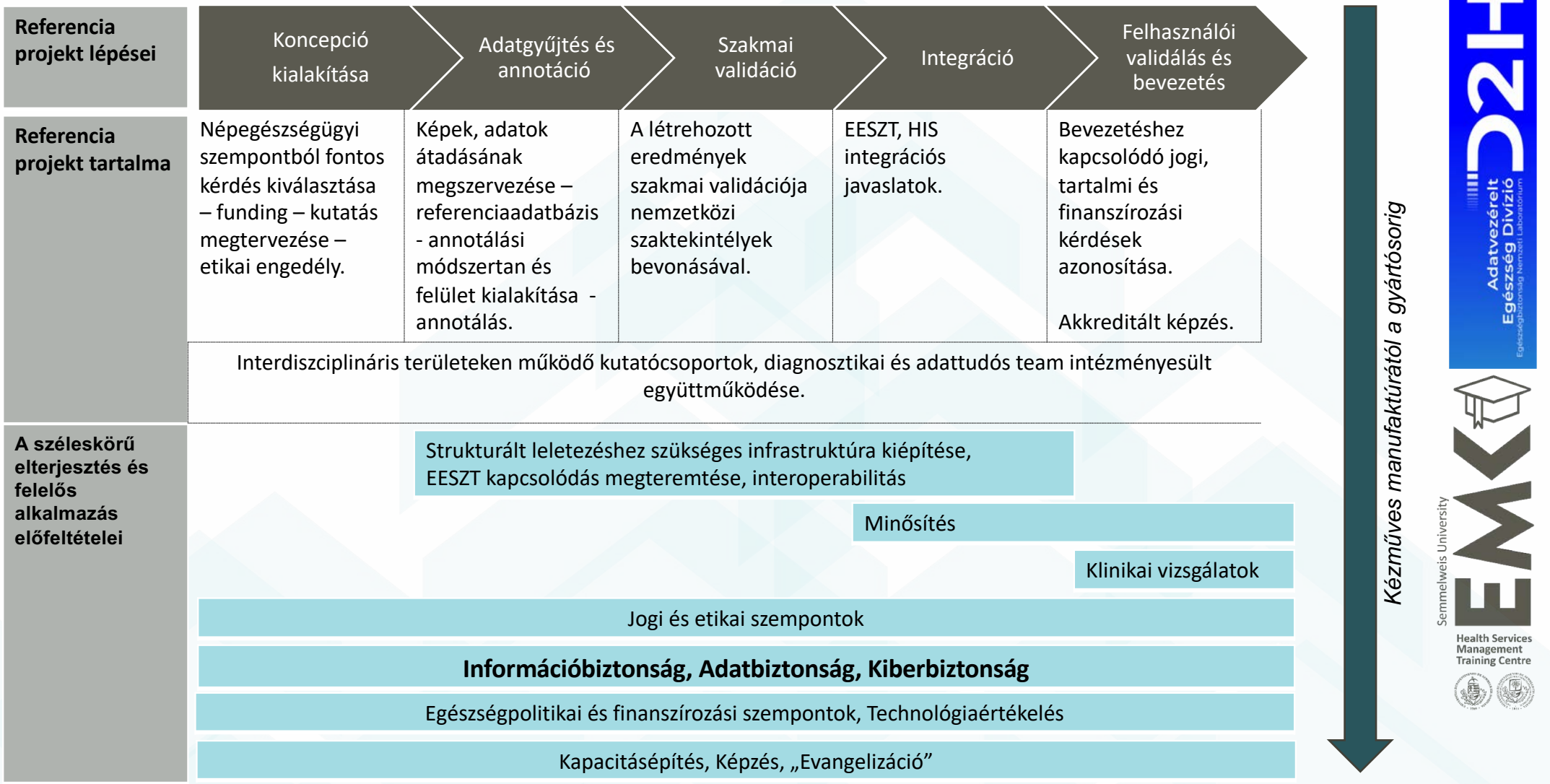


- IoT eszközök és rendszerek értelmezése az egészségügyben
- IoT biztonság aktualitásai, biztonsági hiányosságok, tipikus sérülékenységi vektorok, eszközök képességeivel kapcsolatos biztonsági fejlődési trendek
- A biztonsági követelményekre vonatkozó elvárások, ajánlások, szabványok,
- **Egészségügyi IoT ökoszisztéma értékelése, kockázatok felmérése, biztonsági elemzése, tesztelése**
- **IoT ökoszisztéma biztonsági ajánlás kidolgozása**

Egészségbiztonsági Nemzeti Labor-Adatvezérelt Divízió

- Adatbányászati képességek;
- **Mesterséges Intelligencia gyártósor** (mintázatfelismerő és adatbányászati);
- VIR, BI (egészségügyi szakmai és vezetői adatok);
- **Telemedicina megoldások, IoMT, Digitális ellátási modellek**
- Egészségügyi adat- és információbiztonság
- Egészségpolitikai értékelés
- Képzés területén úttörő szerep

Mesterséges Intelligencia – gyártósor



Adatvezérelt Egészség Divízió

Semmelweis University EMK Health Services Management Training Centre

Egészségügyi kiberbiztonsági disszemináció

- **Egészségügyi Kiberbiztonsági Szemle**

Megjelenik 2022. április 19-től, 2 hetente

- **XXII. IME - Adatvezérelt egészség és kiberbiztonság Konferencia-**

2024. április 25.

Adatvezérelt Egészség Divízió
Egészségbiztonság Nemzeti Laboratórium

Semmelweis University
EMK
Health Services Management Training Centre

Quantum expert: 'Hack now, decrypt later' is here today

By **Dan O'Shea** • Oct 15, 2021 12:00am

Harvest now, decrypt later!

Semmelweis University
EMK
Health Services Management Training Centre

Köszönöm a figyelmet!

palicz.tamas@emk.semmelweis.hu

Adatvezérelt Egészség Divízió
Egészségbiztonsági Nemzeti Laboratórium

Semmelweis University
EMK
Health Services Management Training Centre