Cyber Security in general and in particular in the Med Tech Sector

Digitalization and Cyber Threats 2022

Ludwig Sadredin Sahesch-Pur,

CEO and Founder of AIRPUR DRONES GmbH, Switzerland

MBA and Shenzhen University China,

Professor Lecturalship for Technology and Innovation & International Business Management

28. July 2022

Waldeggweg 2, Switzerland / CH-5415 Nussbaumen / +41(0)79 44 76 69 2 / info@airpurheaven.com / www.pur-consulting.org

Speaker Introduction

Ludwig Sadredin Sahesch-Pur

- CEO and Founder
- Dipl.-Ing.
- MAS Communication
- Swiss Asia MBA 2021, FHNW Basel, Switzerland

Airpur Drones GmbH

- Mobility Solutions to manage last mile in Infrastructure, Senior Care, Transportation Management
- Interconnection of People to transform communication, performance and engagement to the next level

- Founded in **2019**
- Headquarters in Nussbaumen, Aargau, Switzerland

Content

Basic Concepts

Regularotry Requirements

Situation in EU and Switzerland

Disclaimer

The view and opinion expressed in the follwoing slides are those ofthe individual author.

Copyright

Introduction

Basic Concepts

Source:

https://www.google.de/search?q=cyber+attack+in+health+inc

Cyber Security – Cyber Crime

As usual: someone has something of value (assets) that someone else wants:

- **Processing** -> crypto mining
- **Storage device data)** -> file dump (e.g. child porn, sensible information, medical
- **Information** -> steal (espionage), Hold hostage (ransomeware), Damage (vandalism, sabotage)
- **Bandwith** -> attack other targets
- **Services** -> use for free, prevent use (denial of service)

Multiplication possible – automatically attack many targets – improved return on investment: with multiple attacks (e.g. ransomeware) some are bound to succeed.

Note: Cybercrime is a billion doller induatry attracting a lot of porfessionals and state – sponsored actors.

Cyber Security – Cyberwar

Political motivation, same basic principle: someone has, someone else wants:

- **Active warfare** (e.g. Israel, - Iran, China – Rest of the world)
- **Preparation** (e.g. USA – „I hunt sysadmins“, attain strike capabilities)
- **Clandestine operations** (pretty much everyone)
- **Economic warfare** (e.g. USA – China)

Mostly state actors (APT - Advanced Persistent Threat, usually „deniable assets“).

Note: High level of skill, budget, infrastructure, persistence, Virtually impossible to defend against an active, targeted attack from an APT. Still, we can make their life harder and try to limit the impact.

Cyber Security – Medical Devices

Attacks on medical devices and health providers used to be accidental / opportunistic: i.e. a medical device / system was just another networked computer.

Targeted attacks, specially ransomware, are becoming the norm; the health sector is an easy target: security has been neglected for a long- time (manufactuers, regulators, and operators) IT system in use are complex and long-lived, higher willingness and ability to pay ransom.


INTERNATIONAL

Französisches Gesundheitswesen im Visier von Hackern

Radio SRF 4 News | 11.03.2021

Angriffe aufs Gesundheitswesen

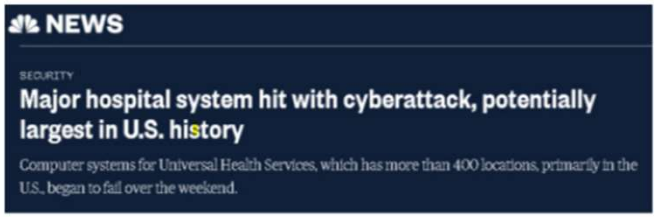
Frankreich ringt mit Pannen und Cyberangriffen auf Systeme von Gesundheitseinrichtungen. Nun will die Regierung handeln.

RADIO SRF 4 NEWS

Inhaltsart
Bericht

Sendung
HeuteMorgen

Region
International


NEWS

SECURITY

Major hospital system hit with cyberattack, potentially largest in U.S. history

Computer systems for Universal Health Services, which has more than 400 locations, primarily in the U.S., began to fail over the weekend.


BBC NEWS

Tech

Hackers threaten to leak plastic surgery pictures

By Joe Tidy
Cyber reporter

24 December 2020

Note: cyber security is not a new thing, other industries have been targeted for decades. Healthcare is lagging behind while the (cyber-world) has become increasingly more danagerous.

„According to a press release issued by healthcare IoT cyber firm Cynerio, 53% of connected medical devices in hospitals have a known critical vulnerability. Potentially more concerning when it comes to patient safety, “

Source: https://incompliancemag.com/medical-devices-increasingly-vulnerable-to-cyberattacks/

Cyber Security – Medical Devices

Note: cyber security is not a new thing, other industries have been targeted for decades. Healthcare is lagging behind while the (cyber-world) has become increasingly more danagerous.

Here's how to protect against cyberattacks on medical devices in the age of healthcare IoT.

- The healthcare industry is vulnerable to cyberattacks, including ransomware, malware, data breaches, DDoS and cryptojacking.
- Patient care and safety, data loss, and damage to a healthcare provider's reputation are among the consequences of networks being breached.
- To stop cyberattacks on medical devices, you need to monitor and segment devices, keep software updated, and implement a response plan to an attack.
- **This article is for medical practices, hospitals, and other healthcare organizations interested in better protecting patient data and their networks by securing connected medical devices.**

Source: https://www.businessnewsdaily.com/15031-connected-medical-devices-healthcare-cybersecurity.html

Cyber Security – Medical Devices

Note: cyber security is not a new thing, other industries have been targeted for decades. Healthcare is lagging behind while the (cyber-world) has become increasingly more danagerous.

5 reasons the healthcare industry is a target for cyberattacks in 2021

1. Patient data is valuable.
2. Medical devices are easy to hack.
3. Healthcare staff are not adequately educated on data security risks.
4. Patient data is shared remotely with numerous healthcare providers.
5. Smaller healthcare organizations are easier targets.

Source: https://www.businessnewsdaily.com/15031-connected-medical-devices-healthcare-cybersecurity.html

Cyber Security – Basic Principles applied to Medical Devices

Integrity

…is protected : e.g.the software, configuration data, patient data are protected against accidental or malicious modification and corruption -> the device works correctly

Availability

The device is available when needed.

Confidentiality

The medical device or system protects information from unauthorized access; e.g. patient information and health records

Take Away Message

- **Medical devices** are targets (even if it is just a means to an end)
- **Medical device manufacturers** are targets (supply chain attacks, industrial espionage)
- **Your customers** are targets
- Attackers are **many**

Regulatory Requirements

- **An overview:**
- Two different perspectives to consider:
- The manufacturers and the customers view.

Regulatory Requirements

- Note: these directives and regulations **do** have an impact on MD.

Legislation – Strategic Level

Legislation	Title	Applies to	Core Topics
NCS	National Cybersecurity Strategy	Switzerland	Critical Infrastructure
NIS Directive	Network Information Security Directive	European Member States	Critical Infrastructure
KRITIS / BSI-Gesetz	Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz	Germany	Critical Infr
2008/114/EG	Ermittlung und Ausweisung europäischer kritischer Infrastrukturen	European Member States	Critical Infr

Name	EU
MDR – Medical Device Regulation **IVDR** – Invitro Diagnostic Device Regulation	Regulations
MDCG 2019-16 – Medical Device Coordination Group – Guidance on Cybersecurity for medical devices	Need to be followed
ISO 14971:2012 - Application of risk management to medical devices	Harmonized Standard
ISO 14971:2019 - Application of risk management to medical devices	State of the art

Regulatory Requirements - The manufacturers view.

Legislation – Industry Level

Legislation	Title	Applies to	Core Topics
MDR	Medical Device Regulation	Europe, Medical Devices	Risk Management, Information Basic Safety / Sa
MedDO	Medical Devices Ordinance	Switzerland, Medical Devices	Risk Managemer Basic Safety / Sa
BSI Gesetz / B3S	Branchenspezifischer Sicherheitsstandard (B3S) für Krankenhäuser	Germany, Hospitals (HDO, Operators)	Risk Managemer Cybersecurity
21CFR820.30	Quality System Regulation	USA, Medical Devices	Risk Managemer Safety Lifecycle
GDPR	General Data Protection Regulation	Europe++, Personal information	Privacy

Name	EU	US
IEC TR 60601-4-5:2021 Safety related technical security specifications for medical devices	Likely to become a harmonized standard	
IEC 62443-3-2:2020 Security for industrial automation and control systems – Security risk assessment for system design		
AAMI TIR57:2016 - Principles for medical device security - Risk management.	Not mandatory	Consensus Standard for the FDA
ISO/TR 24971:2020 - Guidance on the application of ISO 14971	Not mandatory	
IEC 81001-5-1:2020 - Health software and health IT systems safety, effectiveness and security - Security - Activities in the product life cycle	Likely to become a harmonized standard	N/A
UL 2900-2-1:2018 - Software Cybersecurity for Network-Connectable Products – Requirements for Healthcare Systems	N/A	Recommended by FDA
FDA cybersecurity guidance	N/A	Recommended
DIN 80001-1:2010 – Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software - Application of risk management	N/A	N/A

Regulatory Requirements

Medial Device Regulation (MDR)

In contrast to the MDD (Medical Device Directive), The MDR directly addresses cybersecurity issues

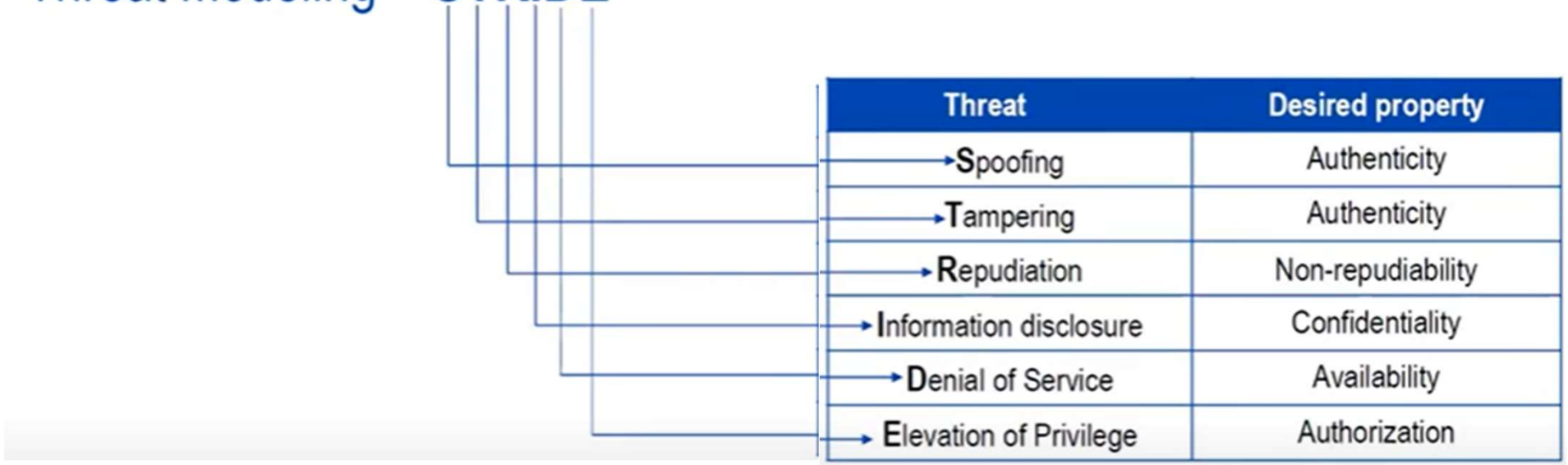
General Safety and Performance Requirements:

17.2. … software shall be developed and manufactured in accordance with the **state of the art** taking into account the principles of development life cycle, risk manafgement, including information security. …

17.4. Manufactures shall **set out minimum requirements** concerning hardware, **IT networks characterictis** and **IT security measures**, incvluding protection against unauthorized access, necessary to run the software as intented.

Legislation in Switzerland – Outlook on MDR Update

Threat Modeling – STRIDE



Threat	Desired property
Spoofing	Authenticity
Tampering	Authenticity
Repudiation	Non-repudiability
Information disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

Threat Modelling STRIDE

Asset	Attack vector	STRIDE	Threat	Ability to exploit	Severity	Risk	Risk control solution	Ability to exploit	Severity	Risk
Therap eutic settings	BLE	Tampering	Stopping therapy by changing bits in RAM	I - Easy to exploit	Death	Un-acceptable	1,2,3,4	V - Difficult	Death	Acceptable

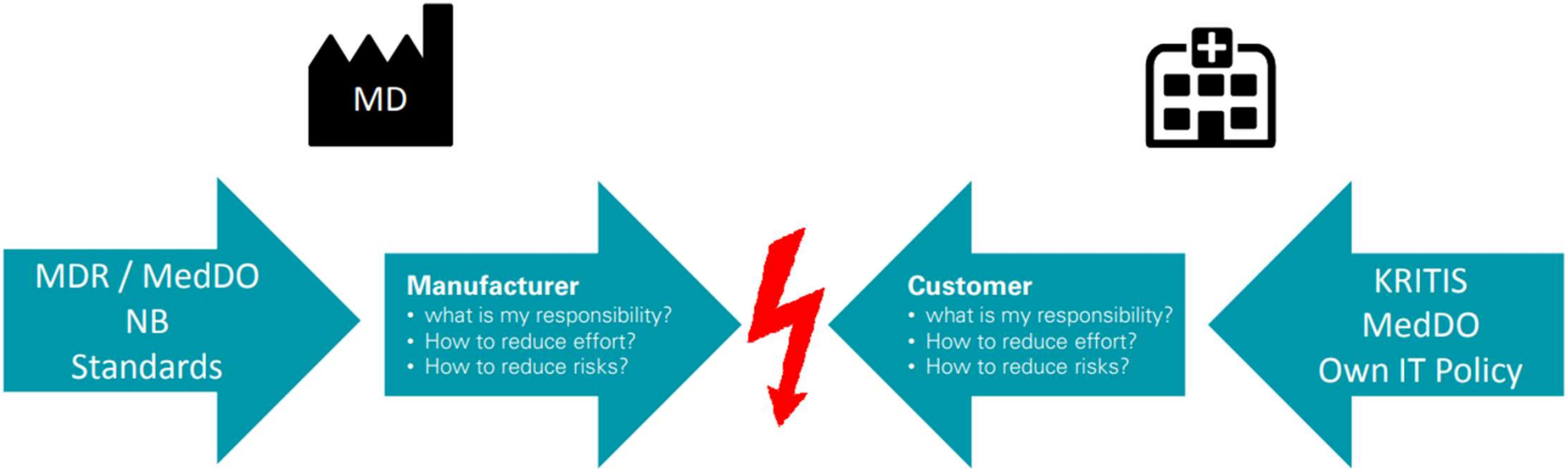
Legislation in Switzerland – Outlook on MDR Update

Art. 74 Cybersicherheit

«Gesundheitseinrichtungen treffen alle technischen und organisatorischen Massnahmen, die nach dem Stand der Technik notwendig sind, um bei netzwerkfähigen Produkten den Schutz vor elektronischen Angriffen und Zugriffen sicherzustellen.»

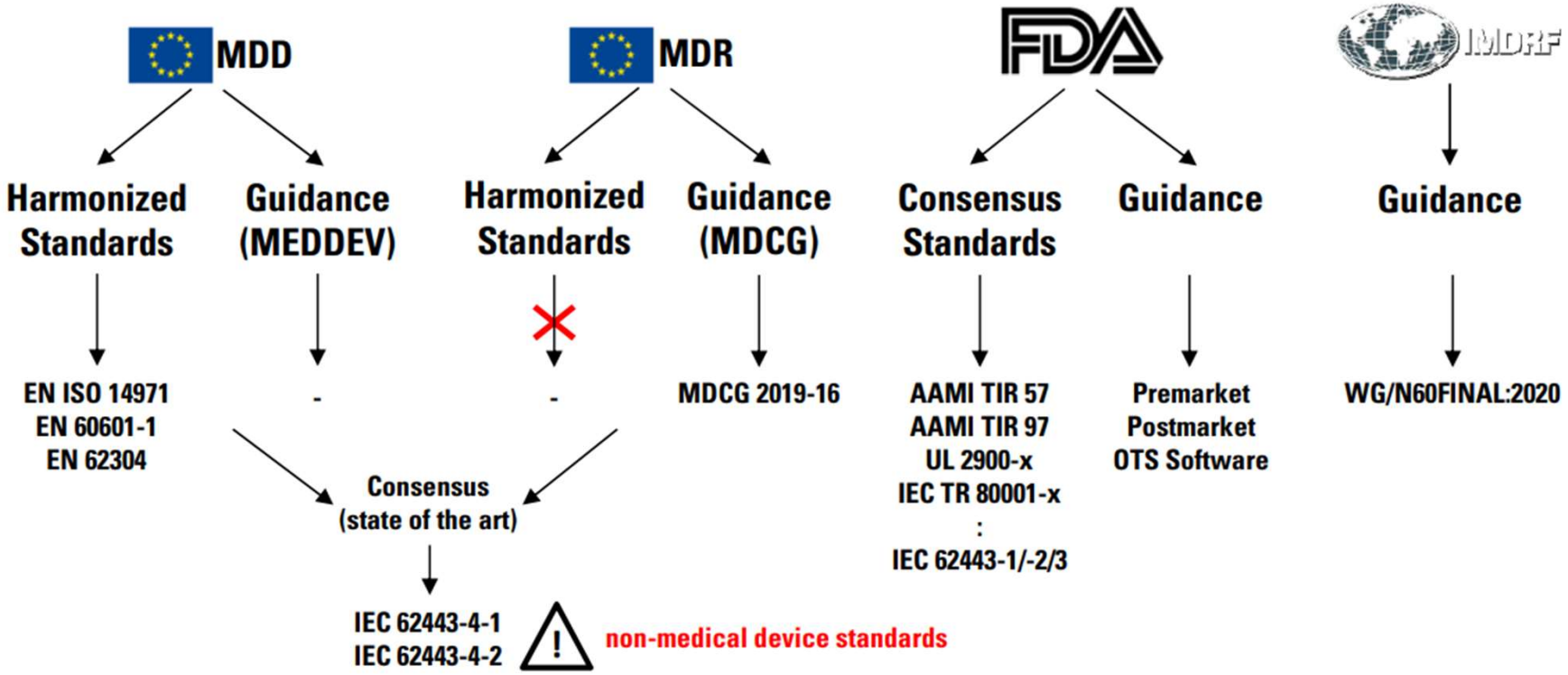
(will come into force on the 26th of May 2021)

That mean ?



Usually, the customer is in a strong position, meaning we (industry) have to move

Standards and Standardisation - An Overview – The Challenge: The Current Situation.



Standards and Standardisation

An Overview – The Challenge: The Current Situation. retrived on 24th July 2022

Useful Links and Wikipedia Explanation for cyber security nomenclauture

MDR, MDD etc. :

https://www.pqegroup.com/blog/2021/03/eu-mdr-2017-745-new-cybersecurity-requirements-for-networked-md-producers/

https://www.t-systems.com/ch/de/branchen/gesundheitswesen/medical-device-regulation-im-uebrblick?wt_ga=114625914185_574637923115&wt_kw=p_114625914185_medical%20device%20regulation&wt_mc=114625914185.574637923115.p.medical%20device%20regulation

https://www.swiss-medtech.ch/sites/default/files/2021-03/Session%203_Cybersecurity%20Regulations%20and%20Guidelines.pdf

Swiss MEDTECH:

https://www.swiss-medtech.ch/veranstaltungen/veranstaltung/mdrnoon-cybersecurity-fuer-medizinprodukte

Praktische Hinweise für App Entwickler und Hersteller der eHealth Suisse:

https://www.e-health-suisse.ch/fileadmin/user_upload/Dokumente/D/Leitfaden_e-Health_Suisse_fuer_App_Entwickler.pdf

Global Reports Cyber Threats:

https://go.crowdstrike.com/global-threat-report-2022.html?utm_campaign=globalthreatreport&utm_content=gtr22&utm_medium=sem&utm_source=goog&utm_term=cyber%20threat%20report&gclid=EAIaIQobChMI8suZqbuS-QIVFo9oCR2pRwU4EAAYASAAEgLXb_D_BwE

Cyber Reports Switzerland: https://www.pwc.ch/de/dienstleistungen/consulting/cybersecurity

Back Up Slides:

Healthcare organizations create, receive, maintain and transmit vast amounts of confidential patient data, making their networks and connected devices prime targets for cyberattacks. While the average cost of a data breach in 2020 was $3.86 million across all global industries, healthcare has the highest industry-average cost of $7.13 million, according to IBM Security's annual report.

Healthcare providers can greatly mitigate their risks of breaches, ransomware, and costly noncompliance fines from HIPAA and the European Union's General Data Protection Regulation by investing in security orchestration, automation, and response (SOAR) – a system designed to increase detection rates and reduce the response and containment time.

The vast number of connected medical devices of varying specifications and from different manufacturers makes security upkeep especially challenging for healthcare IT professionals. While medical devices don't always store significant amounts of patient data, they can be vulnerable entry points for attackers to access data-rich servers. Keeping these entry points updated and secure must remain a priority for the healthcare industry to reduce the costs and damage of unauthorized access.

Cyberattacks on medical devices can be dangerous, even life-threatening. A hospital in Germany suffered a ransomware attack in September 2020, stopping the intake of new patients and forcing reroutes for emergency patients. One patient died while the hospital struggled to restore services. With access to connected devices and networks storing sensitive patient data, everyone working in your healthcare organization is a member of your security team. That's why it's critical for you and your staff to embrace a zero-trust security model to prevent unauthorized access to confidential data.

The emergence of telemedicine and collaboration between medical providers greatly increases the patient's chance to receive the best care possible. Protecting patient data in a remote environment is increasingly challenging, however. Many organizations are implementing multifactor and risk-based authentication methods to identify and grant access to authorized individuals across devices and locations. IT administrators can establish increasing stringency on the authentication process based on unusual activity.

Back Up Slides: Praktische Hinweise – useful hints from the regulators

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

C GDK S

eHealth Suisse

Leitfaden für App-Entwickler, Hersteller und Inverkehrbringer

Praktische Hinweise

Bern, 7. April 2022

ehealthsuisse
Kompetenz- und Koordinationsstelle von Bund und Kantonen
Centre de compétences et de coordination

2.7 Risikoklassen von Medizinprodukten

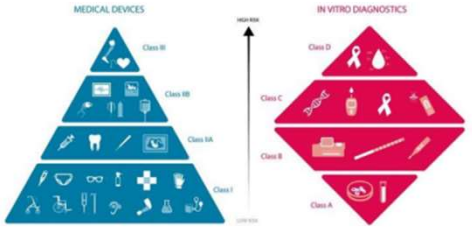


Abbildung 1 Risikoklassen MD und IVD EU (Quelle: MedTech Europe)

Risikoklassen MD

In der Schweiz und Europa werden Medizinprodukte in vier Risikoklassen eingeteilt: Bei klassischen Medizinprodukten erfolgt die Einteilung in die Klassen I, IIa, IIb und III nach Anhang VIII der MDR, wobei die Produktinformation immer zu berücksichtigen ist. Abhängig von Verwendungszweck, Anwendungsdauer und der anatomischen Lage des Produkts können ähnliche Produkte zu unterschiedlichen Klassen gehören.

Risikoklasse	*Klasse I (geringes Risiko)*	*Klasse IIa (geringes bis mittleres Risiko)*	*Klasse IIb (mittleres bis hohes Risiko)*	*Klasse III (hohes Risiko)*
Beispiele	*Heftpflaster, Korrektionsbrillen*	*Kontaktlinsen, Zahnfüllstoffe, Trachealtuben*	*Röntgengeräte, Harnröhrenstents*	*Kardiovaskuläre Katheter, Hüft-, Schulter- und Kniegelenksprothesen, Herzschrittmacher*

Abbildung 2 Verordnung (EU) 2017/745 über Medizinprodukte Artikel 51

Back Up Slides: Praktische Hinweise – Inputs which have not been adressed and added here

- Cybersecurity is **necessary**, is **required** and **mandatory** for market access
- Guidance and standards are available or being developed
- Major content should be **cybersecurity risk management process** and **secure life cycle process** to ensure **defense in depth**
- The effectiveness of security implementation should be tested

Not discussed:

- Security issues in software incorporating artificial intelligence
- Adversarial attacks
- Adversarial Policy attacks
- Further requirements defined in MDCG
- Linkage to IMDRF Principles and Practices for Medical Device Cybersecurity

Waldeggweg 2, Switzerland / CH-5415 Nussbaumen / +41(0)79 44 76 69 2 / info@airpurheaven.com /
www.pur-consulting.org