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

Digitalization and Cyber Threats 2022

Ludwig Sadredin Sahesch-Pur,

Regensburg, Zürich

MBA and Shenzhen University China,

Lecturalship Professor 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

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

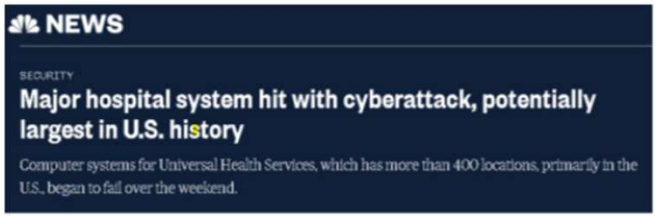
Frankreich ringt mit Pannen und Cyberangriffen auf Systeme von Gesundheitseinrichtungen. Nun will die Regierung handeln.

4 NEWS RADIO SRF

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.