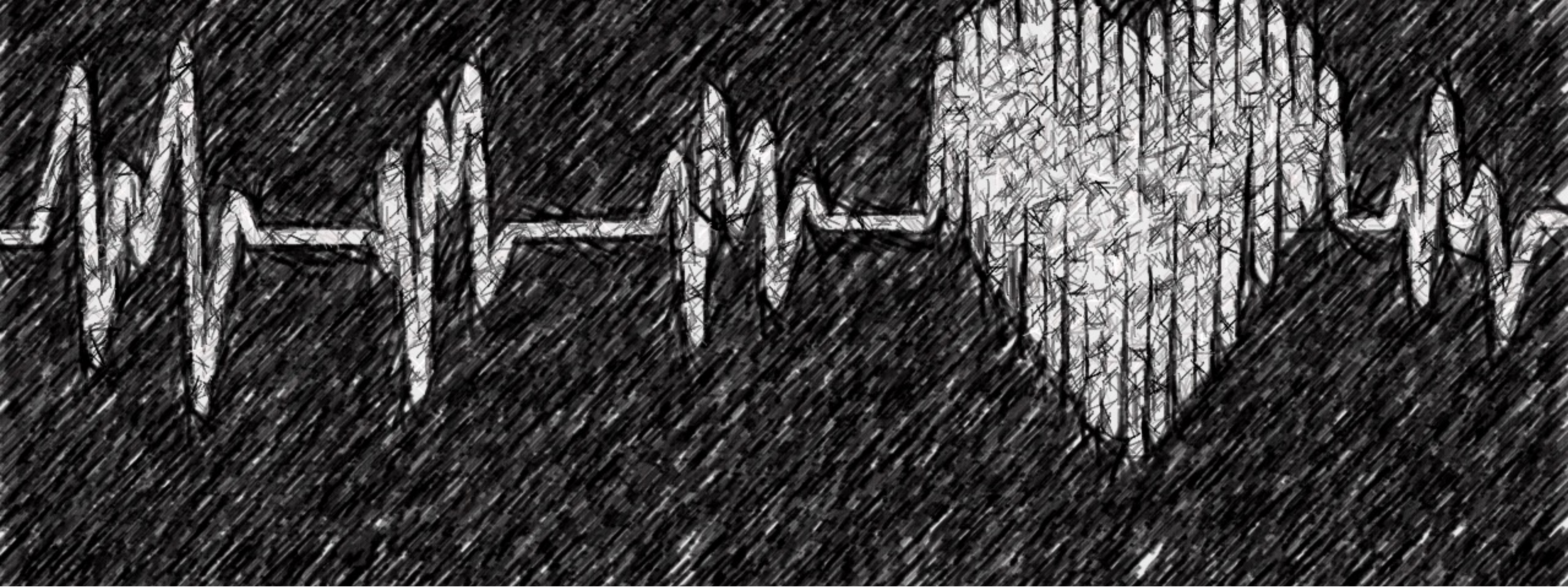


Medical Device Security

Learnings From Countless Security Assessments

ERNW RESEARCH
pursuing knowledge.

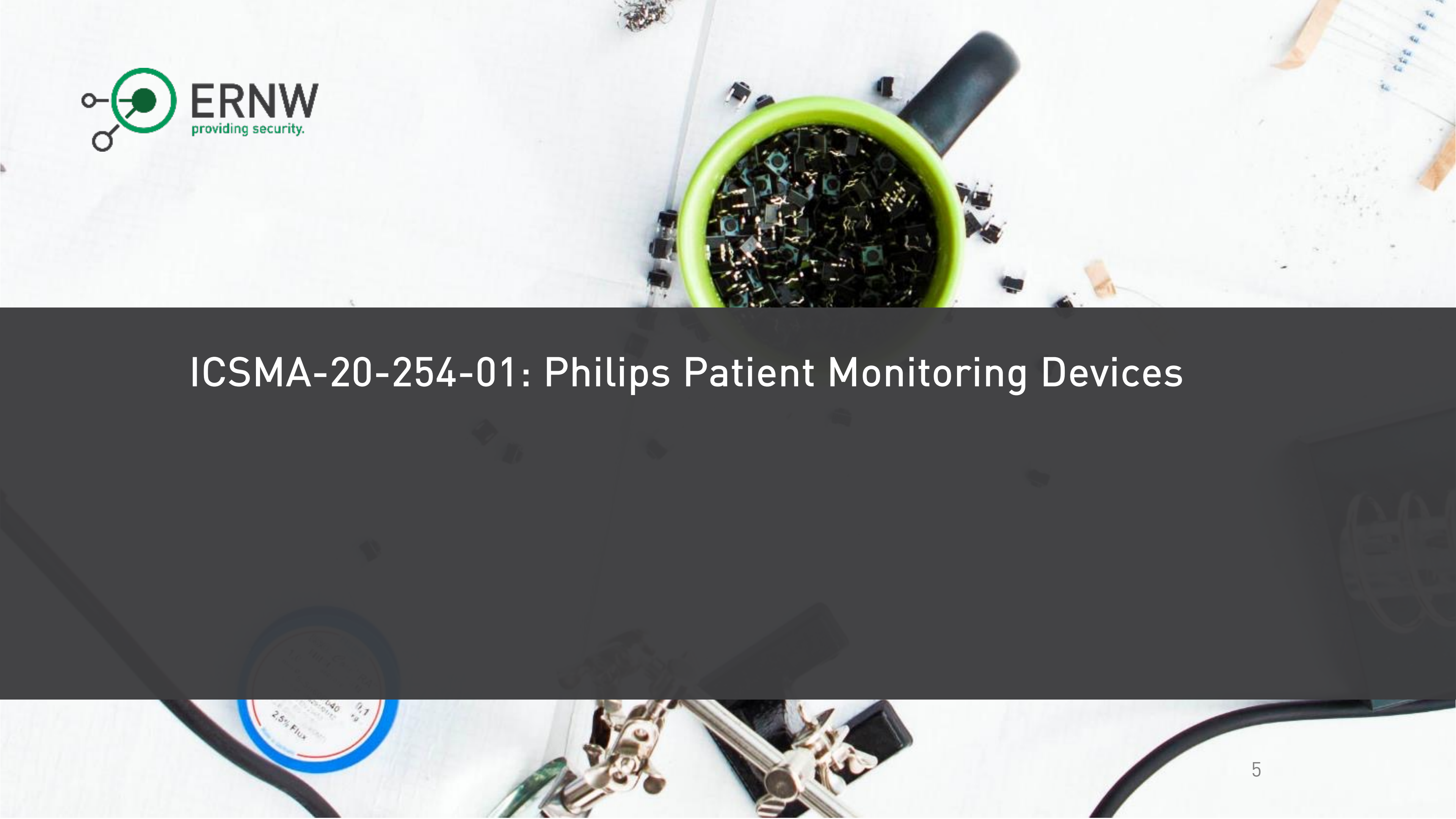
Who Am I

- Julian Suleder
- Senior Security Analyst & Researcher @ ERNW
- Medical computer science background
- Performed >25 medical device security assessments
- 🐦 @jsuleder

Agenda

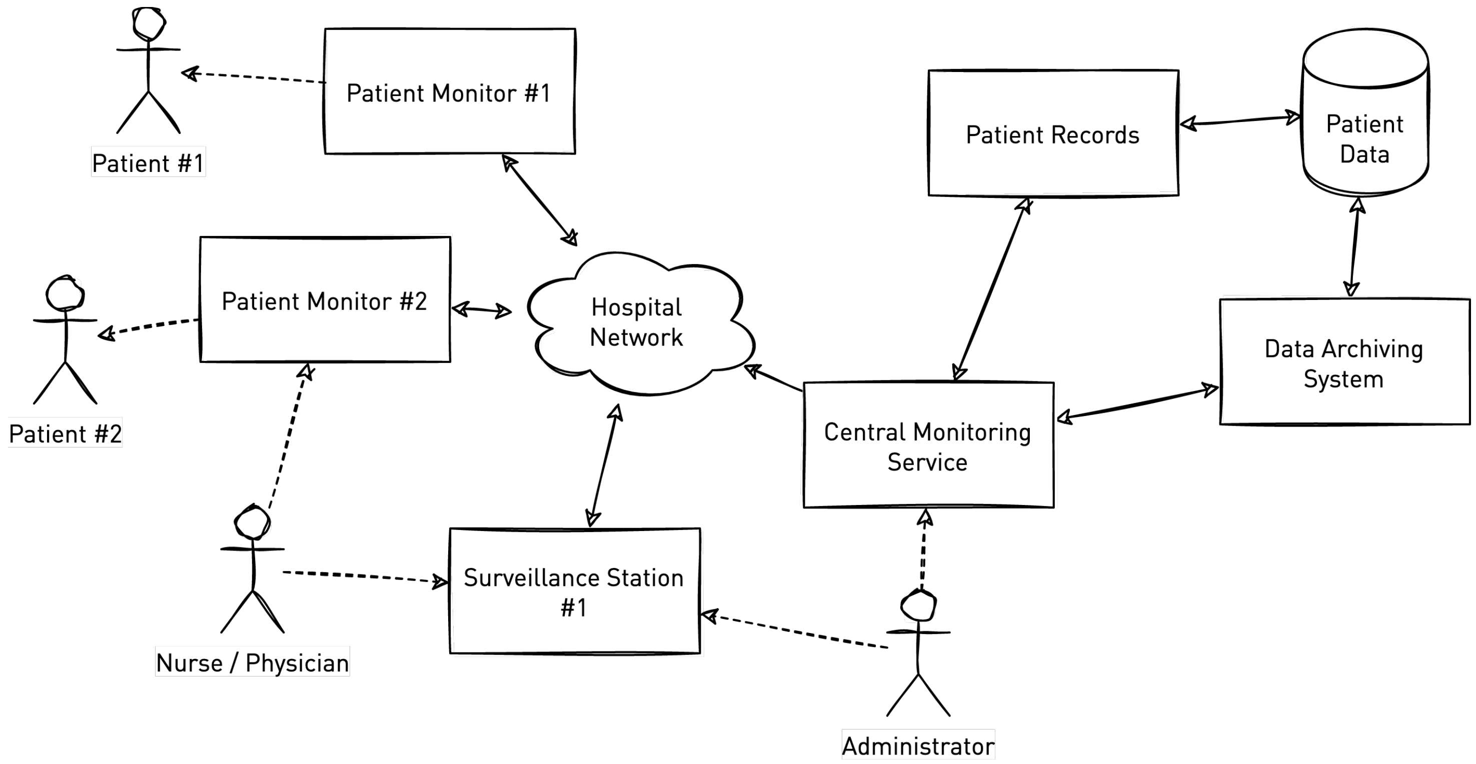
- Case Studies
- Lessons Learned
- Regulatory Requirements
- Disclosure Processes
- Closing

Case Studies



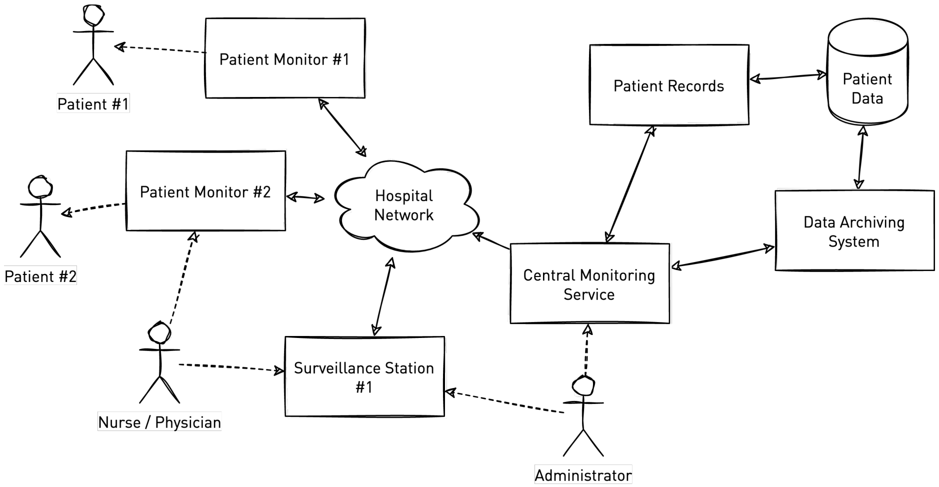
ICSMA-20-254-01: Philips Patient Monitoring Devices

Patient Monitoring System



Patient Monitoring System

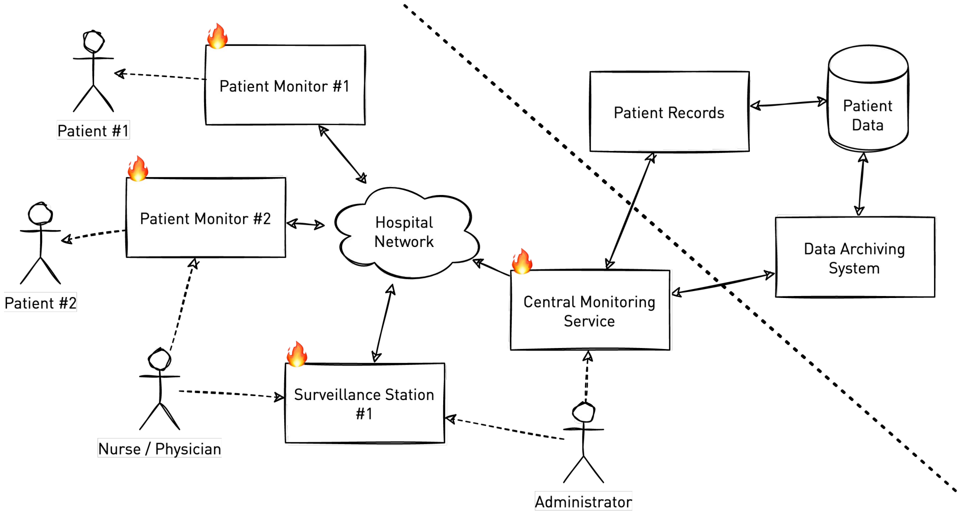
- Common trust anchor:
    - Environment CA with entity enrolment functionality
    - Certificates for every service and medical device
    - Mutual authentication via DTLS
- Communication protocol
    - Proprietary
    - Monitors need to connect to other monitors → trust?



ERNW RESEARCH pursuing knowledge.

Findings

- Central Monitoring Service:
  - Crashed and rebooted via unauthenticated TCP packet
  - Crash via certificate enrolment service
  - Short SCEP Pins: Obtain trusted certificates via brute-force
- Monitor:
  - Incorrectly validates received input via the DTLS-secured channel



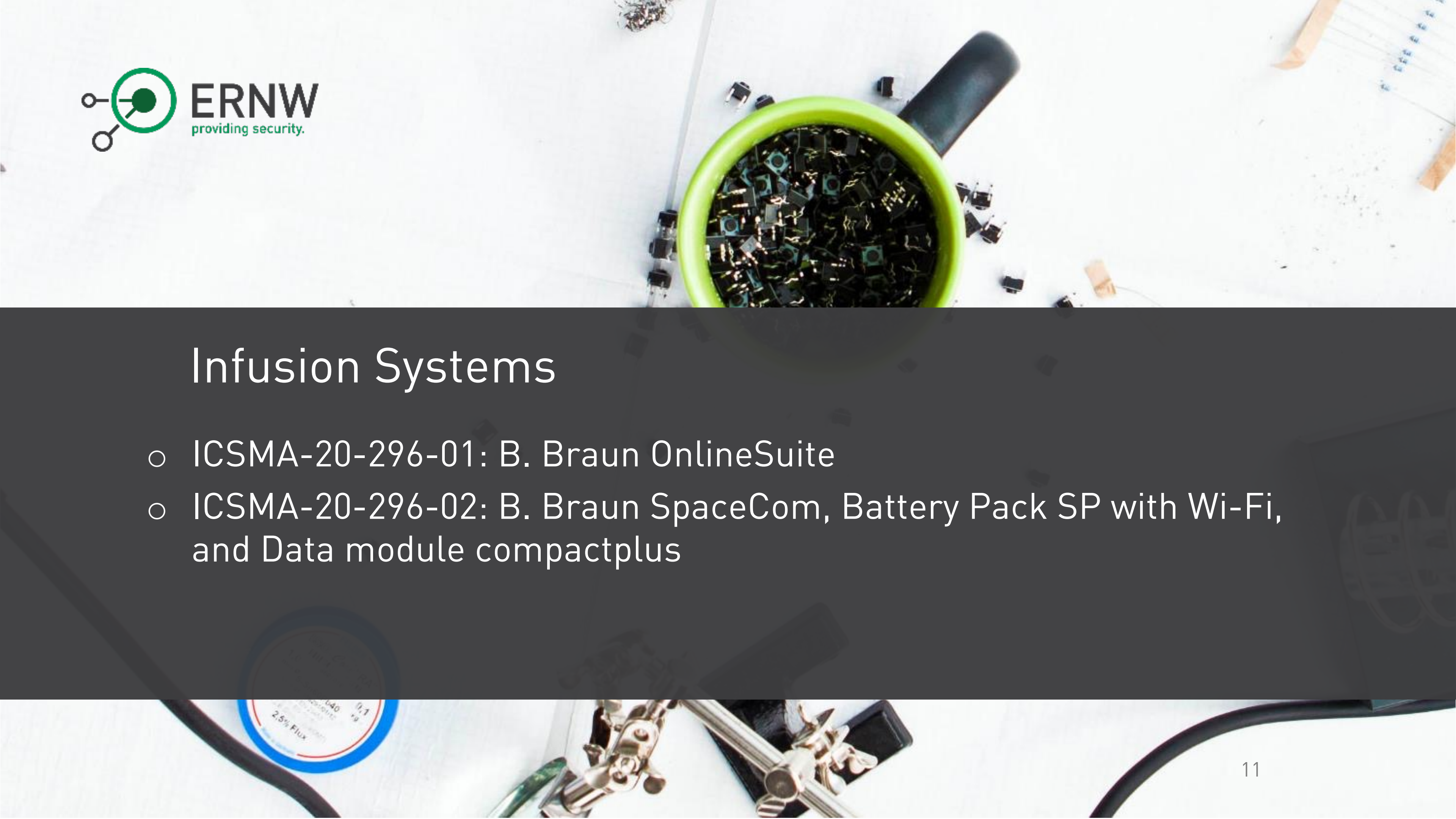
Impact: Interrupted monitoring, access to patient health information.

Implications & Mitigations

- Disaster recovery:
  - Assume there is a compromised entity in your environment
  - How to handle compromised devices?
  - What is the impact on the device ecosystem?
- Trust relationships must be maintained between components.

Implications & Mitigations

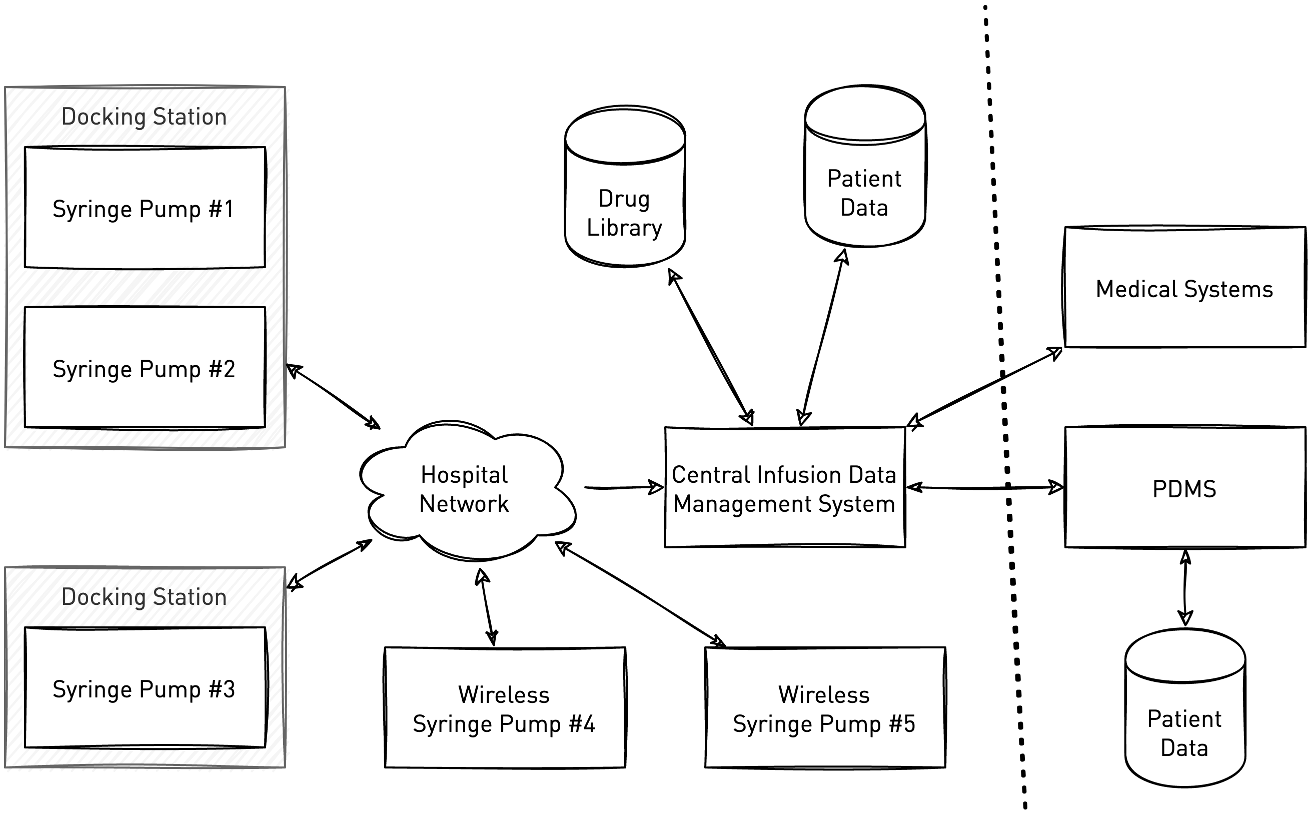
- Describe the processes that need to be established by operators:
  - Which configurations need to be checked on a regular basis?
  - Where is key material that needs rotation or certificates that expire?
  - How can operators terminate trust relationships of single devices?
- → Render secure operation feasible



Infusion Systems

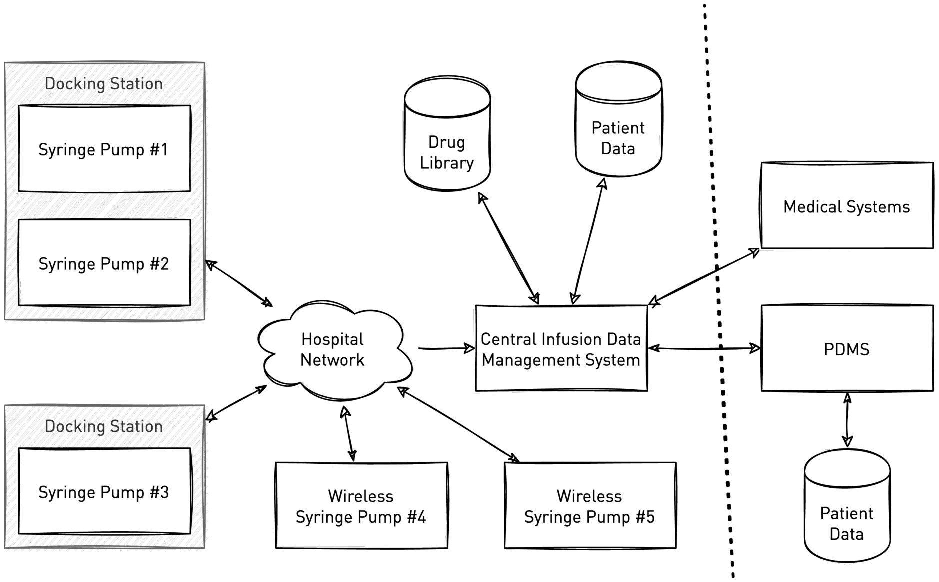
- ICSMA-20-296-01: B. Braun OnlineSuite
- ICSMA-20-296-02: B. Braun SpaceCom, Battery Pack SP with Wi-Fi, and Data module compactplus

Infusion Systems



Infusion Systems

- Docking stations act as communication gateway
- No remote-control functionality
- Manual interaction on device needed for medical use
- → Communication solely is for documentation / monitoring purposes



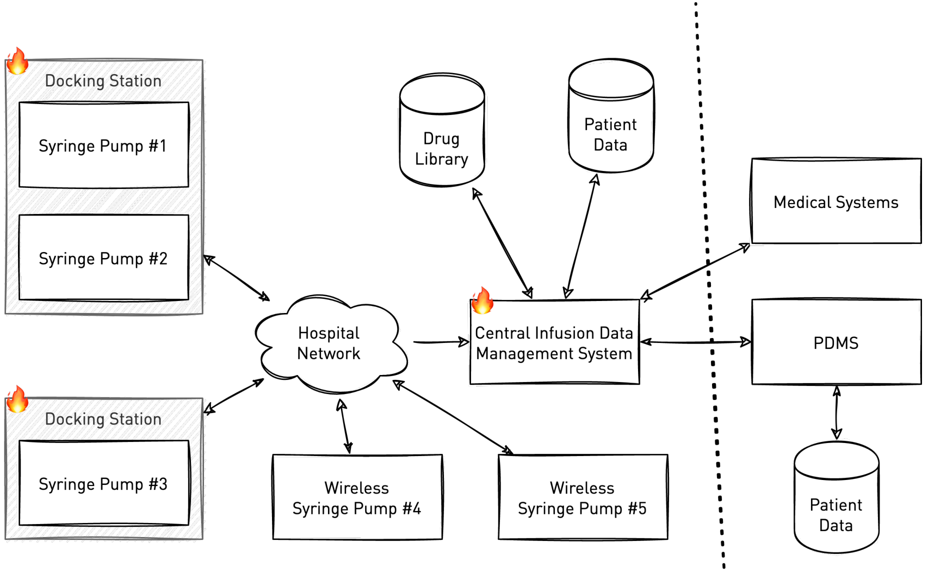
Findings

- Docks are running an administrative web application
  - XPath injections in login
  - Passwords stored hashed with MD5
  - Path traversal via authenticated file upload
  - Authenticated command injection
  - Privilege escalation to root via magic binary
- Central Management Service based on web services
  - Path traversal in unauthenticated file upload and download
  - DLL hijacking via bundled third-party library

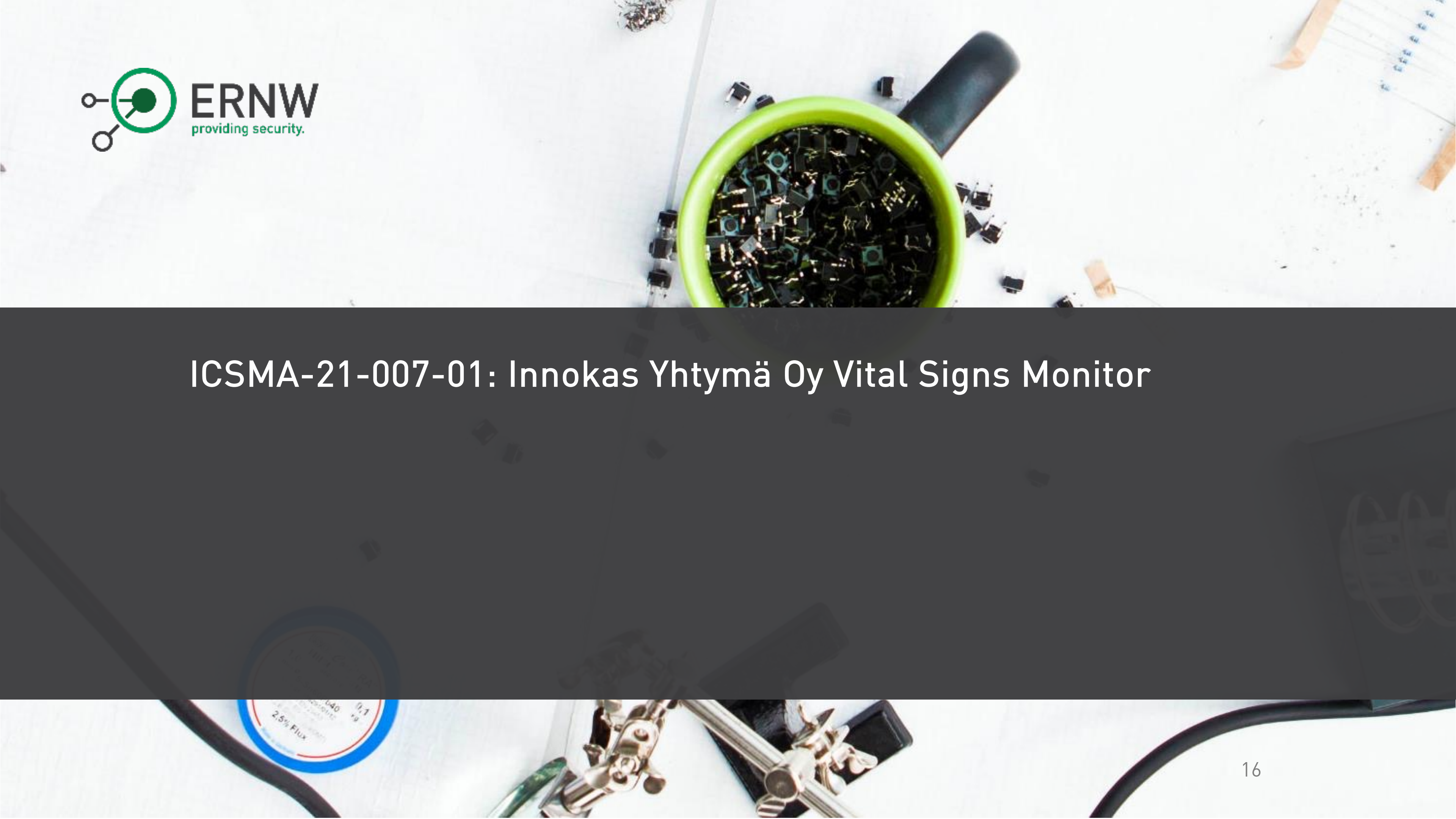
ERNW RESEARCH pursuing knowledge.

What is the impact?

- Device is not affected in its medical operation or purpose
- Devices lose their ability to communicate
- An attacker is in the position of directly communicating with the infusion devices
- → **Prerequisite for more attacks**



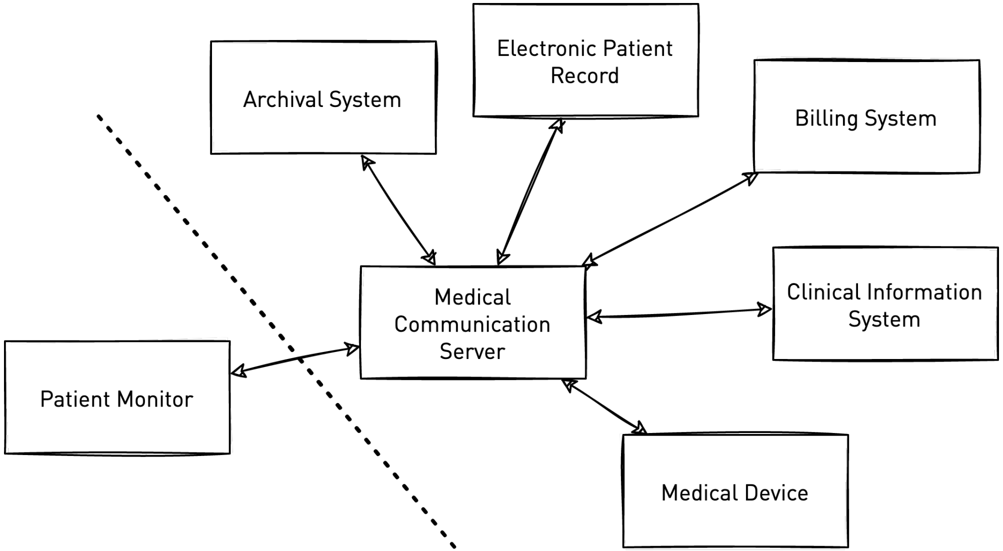
Impact: Full compromise of the medical device's accessory.



ICSMA-21-007-01: Innokas Yhtymä Oy Vital Signs Monitor

The HL7 v2.x Standard

- Goal: Interoperability of heterogeneous medical systems
- → Agreements on message structure and content representations
- Common, text-based standard for transactions between medical systems


Archival System
Electronic Patient Record
Billing System
Medical Communication Server
Clinical Information System
Patient Monitor
Medical Device

The Vulnerability

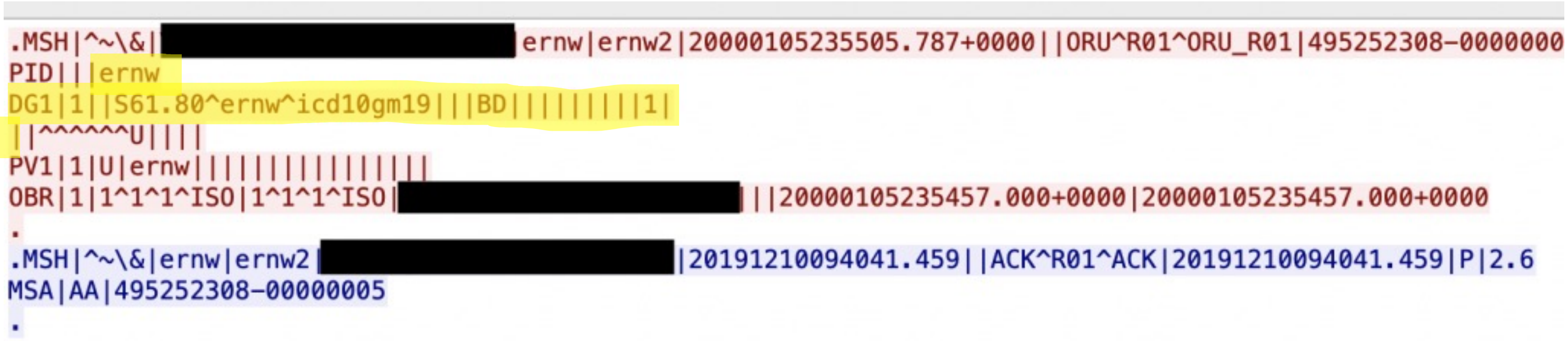
- Encoding characters in untrustworthy inputs are processed
- Requires physical access to the device
- Inject valid HL7 v2.x segments into the HL7 v2.x message with a connected barcode reader

- This barcode bypasses restrictions to special characters in input:
  `ernw\rDG1|1||S61.80^ernw^icd10gm19|||BD|||||||||1|\r`

ernwDG1|1||S61.80^ernw^icd10gm19|||BD|||||||||1|

The Payload

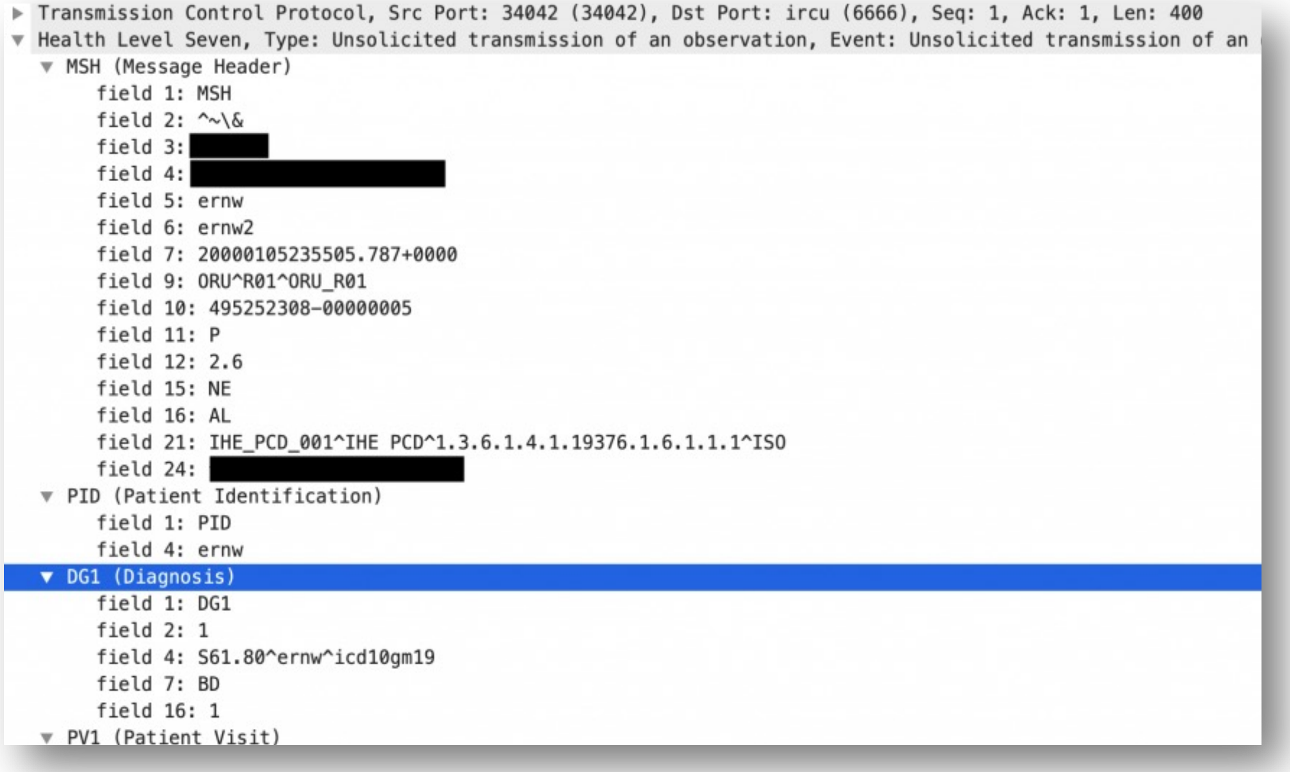
- The payload adds an HL7 v2.x diagnosis segment according to a medical diagnosis code coding system
- Injecting the prepared payload in the patient's name causes the following HL7 v2.x communication between the device (red) and an HL7 v2.x – capable system (blue)



```
.MSH|^~\&|[redacted]ernw|ernw2|20000105235505.787+0000||ORU^R01^ORU_R01|495252308-0000000
PID|||ernw
DG1|1||S61.80^ernw^icd10gm19|||BD|||||||||1|
||^^^^^^^U||||
PV1|1|U|ernw||||||||||||||||
OBR|1|1^1^1^ISO|1^1^1^ISO|[redacted]||20000105235457.000+0000|20000105235457.000+0000
.
.MSH|^~\&|ernw|ernw2|[redacted]|20191210094041.459||ACK^R01^ACK|20191210094041.459|P|2.6
MSA|AA|495252308-00000005
.
```

```
ernw\rDG1|1||S61.80^ernw^icd10gm19|||BD|||||||||1|\r
```

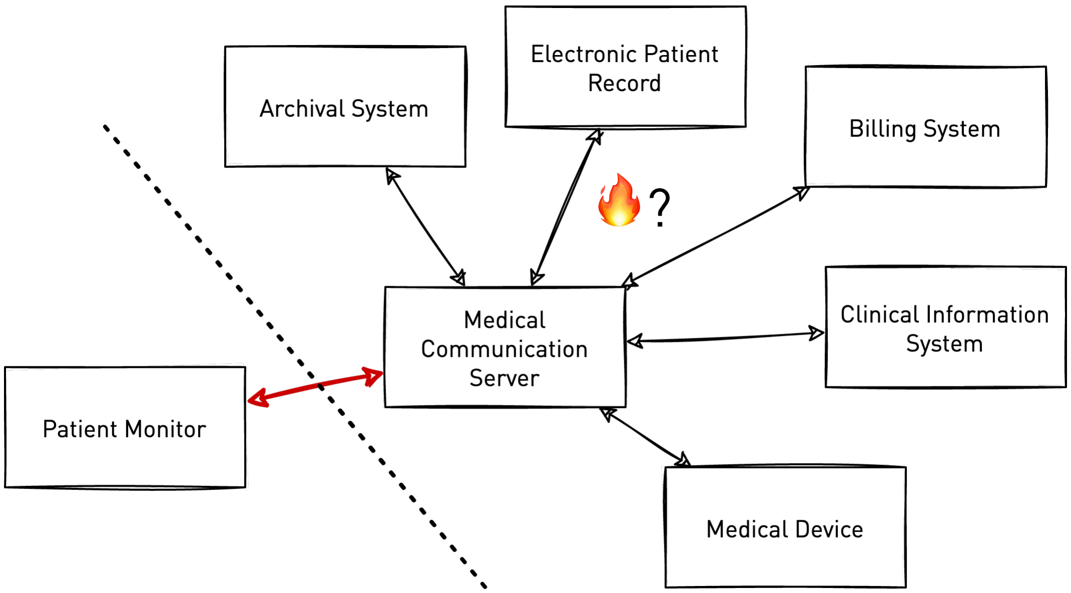
What is the impact?



```
▶ Transmission Control Protocol, Src Port: 34042 (34042), Dst Port: ircu (6666), Seq: 1, Ack: 1, Len: 400
▼ Health Level Seven, Type: Unsolicited transmission of an observation, Event: Unsolicited transmission of an
  ▼ MSH (Message Header)
      field 1: MSH
      field 2: ^~\&
      field 3: [redacted]
      field 4: [redacted]
      field 5: ernw
      field 6: ernw2
      field 7: 20000105235505.787+0000
      field 9: ORU^R01^ORU_R01
      field 10: 495252308-00000005
      field 11: P
      field 12: 2.6
      field 15: NE
      field 16: AL
      field 21: IHE_PCD_001^IHE PCD^1.3.6.1.4.1.19376.1.6.1.1.1^ISO
      field 24: [redacted]
  ▼ PID (Patient Identification)
      field 1: PID
      field 4: ernw
  ▼ DG1 (Diagnosis)
      field 1: DG1
      field 2: 1
      field 4: S61.80^ernw^icd10gm19
      field 7: BD
      field 16: 1
  ▼ PV1 (Patient Visit)
```

Further Information: https://insinuator.net/2020/04/hl7v2-injections-in-patient-monitors/

What is the impact?

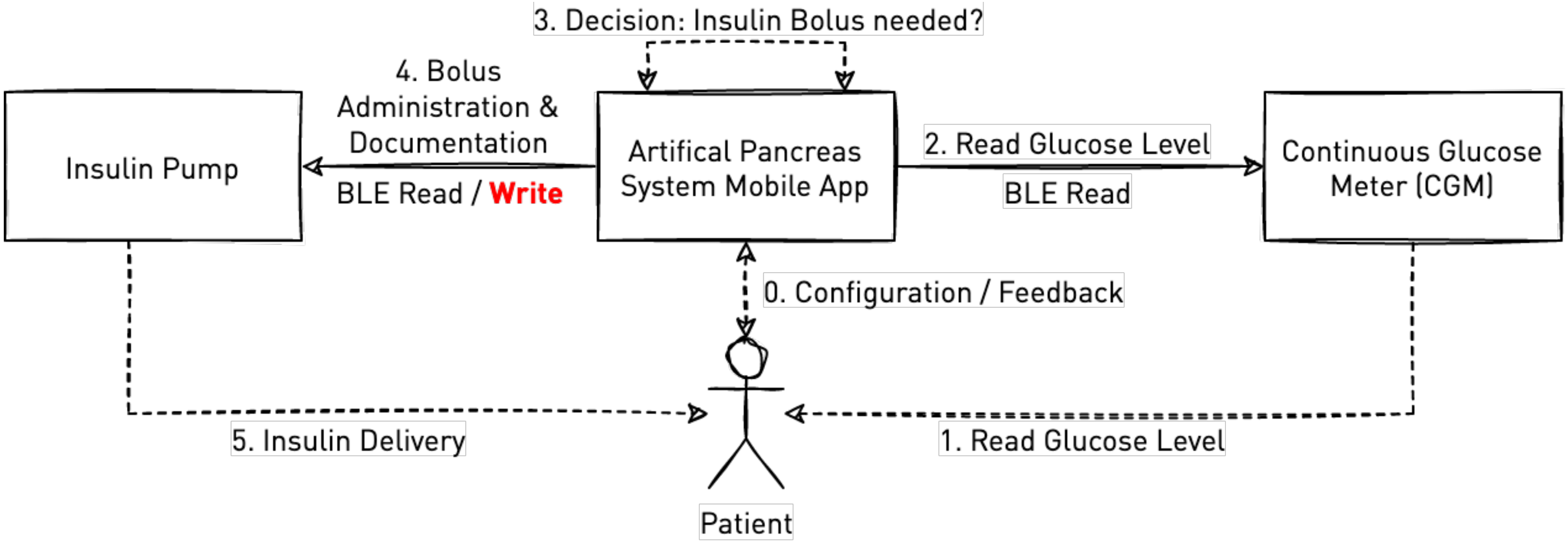

Archival System
Electronic Patient Record
Billing System
🔥?
Medical Communication Server
Clinical Information System
Patient Monitor
Medical Device

- No direct impact on the patient monitor
- Exploitation allows an attacker to modify communications to downstream devices
- → Diagnosis may be parsed by clinical systems

See: https://www.cisa.gov/uscert/ics/advisories/icsma-21-007-01

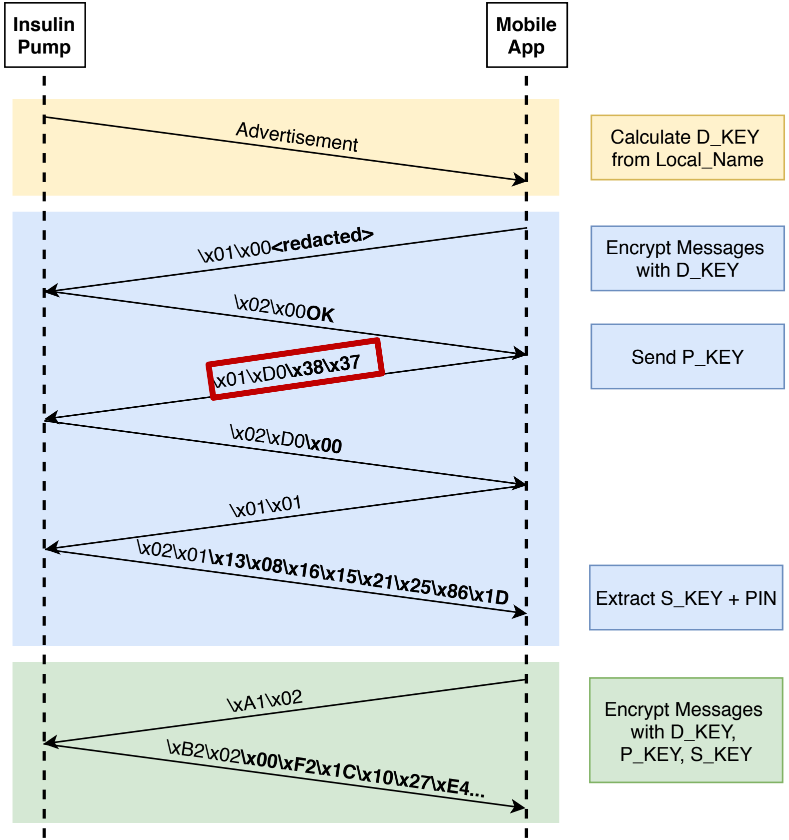
Insulin Therapy Systems & Point-of-Care-Testing Devices (POCT)

Insulin Therapy Systems

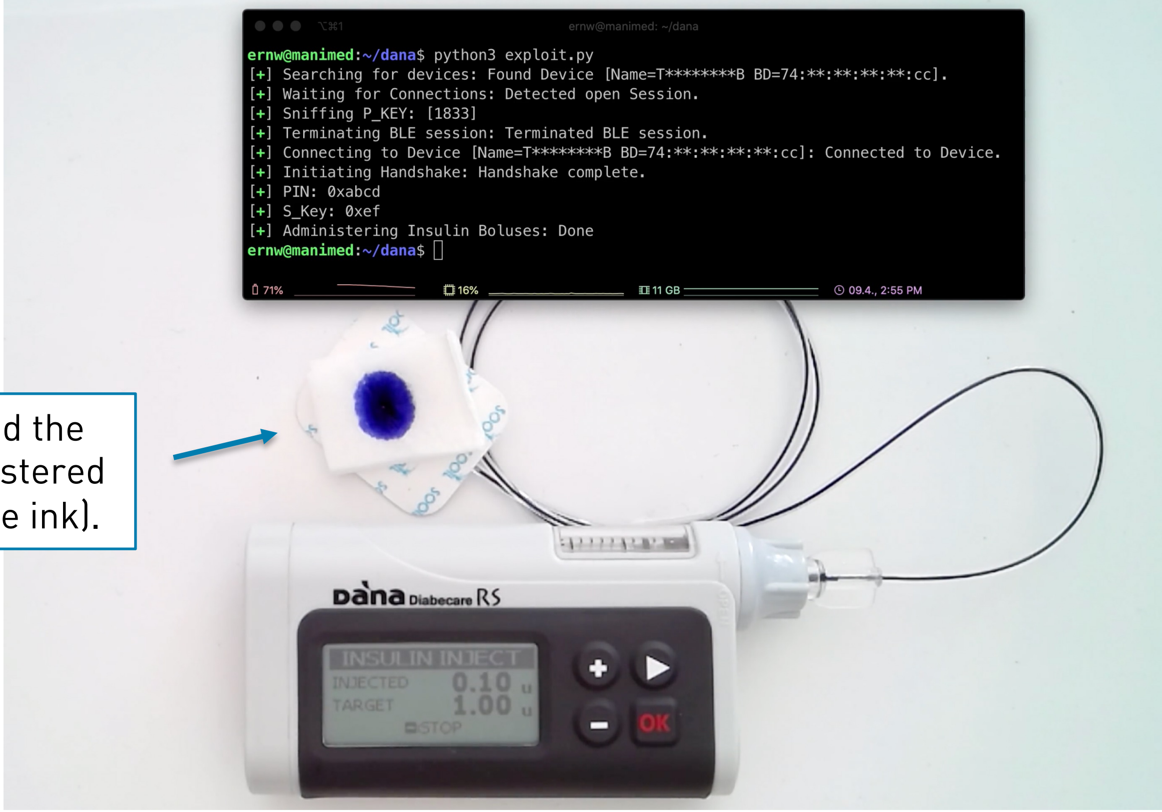

3. Decision: Insulin Bolus needed?
4. Bolus Administration & Documentation
Insulin Pump
Artifical Pancreas System Mobile App
2. Read Glucose Level
Continuous Glucose Meter (CGM)
BLE Read / Write
BLE Read
0. Configuration / Feedback
5. Insulin Delivery
1. Read Glucose Level
Patient

Broken Communication Protocol

- Application-layer protocol on top of unauthenticated BLE GATT read/write
- Authentication relies on the app-layer pairing key.
- An attacker needs to be in proximity to the pump and sniff a single handshake between a pump and a paired mobile application.


Insulin Pump
Mobile App
Advertisement
Calculate D_KEY from Local_Name
\x01\x00<redacted>
Encrypt Messages with D_KEY
\x02\x00OK
\x01\xD0\x38\x37
Send P_KEY
\x02\xD0\x00
\x01\x01
\x02\x01\x13\x08\x16\x15\x21\x25\x86\x1D
Extract S_KEY + PIN
\xA1\x02
\xB2\x02\x00\xF2\x1C\x10\x27\xE4...
Encrypt Messages with D_KEY, P_KEY, S_KEY

What is the impact?



```
ernw@manimed:~/dana$ python3 exploit.py
[+] Searching for devices: Found Device [Name=T********B BD=74:**:**:**:**:cc].
[+] Waiting for Connections: Detected open Session.
[+] Sniffing P_KEY: [1833]
[+] Terminating BLE session: Terminated BLE session.
[+] Connecting to Device [Name=T********B BD=74:**:**:**:**:cc]: Connected to Device.
[+] Initiating Handshake: Handshake complete.
[+] PIN: 0xabcd
[+] S_Key: 0xef
[+] Administering Insulin Boluses: Done
ernw@manimed:~/dana$
```

Attacker hijacked the pump and administered Insulin (here: blue ink).

Full video: https://www.youtube.com/watch?v=0GMe2poiYtE

Implications & Mitigations

- Don't roll your own cryptography!
- Use security functionality provided by communication protocols
- Implement application-layer protocols only on top when needed
- Design your device with residual resources not to limit the possibilities in using stronger cryptography!

ERNW RESEARCH
pursuing knowledge.

Point-of-Care-Testing Devices

- Medical purpose:
  - Bed-side lab diagnostics
  - May also be used by patients
- Portable, small, usually no wired connection

ERNW RESEARCH
pursuing knowledge.

Point-of-Care-Testing Devices

- Technically:
  - Embedded devices
  - Resources: Not very powerful microcontrollers, SoCs, etc.
  - Embedded software stack / RTOS
  - Few software abstraction layers
  - Communication via:
    - USB, serial interfaces, Infrared
    - Bluetooth and WiFi

Vulnerabilities & Challenges

- Product Lifecycle Issues:
  - Outdated/ end-of-life OS and dependencies
  - Broken firmware update mechanisms
  - Masses of vulnerable third-party software, dependencies, etc.
- Design & Development:
  - Hard-coded secrets and credentials
  - Custom implementations for AES, Bluetooth stack, TLS, encryption and authentication protocols, …
- Operation:
  - Unprotected service and debug interfaces
  - Compatibility assurance causes secure and insecure versions of protocols being available at the same time

Lessons Learned

Lessons Learned

- Most vulnerabilities concerning medical devices are not specifically medical → e.g., OWASP IoT Top 10
- The device should be designed and manufactured in a way that ensures that the risks associated with environmental conditions are removed or minimized.
- There should be frequent security testing during design, development and the post-market lifecycle.

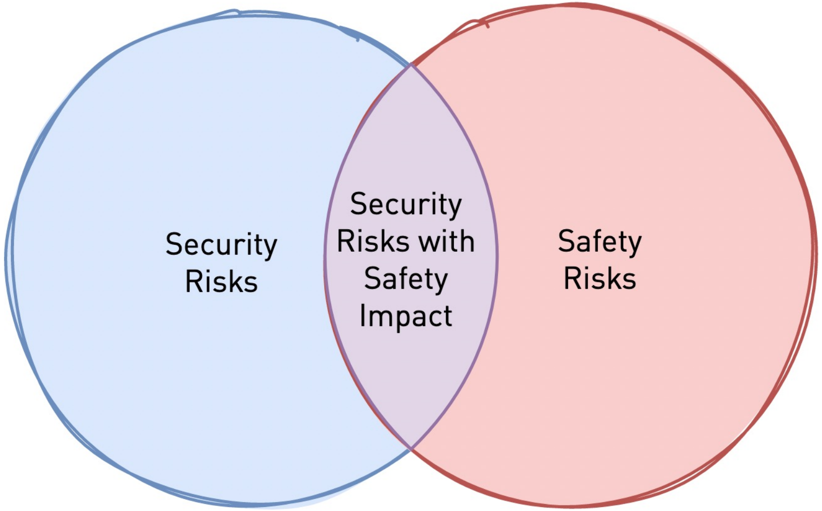
Regulatory Requirements

Medical Device Regulations

- Europe: Since 2017 there are two new regulations – MDR & IVDR
- Relevant changes for us in this context:
  - Safety approach based on the entire product life cycle:
    - Quality & Risk management
    - Intense post-market surveillance activities
- → MDCG 2019-16: Guidance on Cybersecurity for medical devices

Relationship: Safety & Security

- Any risks associated with the operation of medical devices must be acceptable.
- MDCG 2019-16:
  - Establishment of a **balance between benefit and risk** during all possible operation modes.
  - **Relationship between safety and security** as they relate to risk.



Requirements

- The manufacturer must implement state-of-the-art security capabilities depending on the risk management which is based on known vulnerabilities and attack vectors.
- **Security verification and validation testing:**
  - Processes are used to document the security testing to ensure that
    - all the security requirements have been met for the product
    - security of the product is maintained when used as intended
  - Security testing should be aligned to other product test activities

ERNW RESEARCH pursuing knowledge.

Lifecycle Aspects

The security situation for software may change rapidly due to newly emerging security vulnerabilities, or new attack vectors.

A medical device is considered secure with respect to known vulnerabilities at a specific point in time.

Without any security maintenance the device may become unsecure and possibly unsafe.

Post-market Surveillance System

- The MDR requires a post market surveillance system (PMS) which must include security considerations:
  - Actively and regularly collect user experience from the market,
  - Collect information about 3rd-party software and hardware
  - Timely implement necessary corrective actions considering the risks

Post-market Surveillance System

- An effective and successful PMS should include:
  - Sharing and dissemination of cybersecurity information and knowledge of cybersecurity vulnerabilities and threats
  - Vulnerability remediation
    - Possible mitigations in the operating environment
    - Quick fixes
    - Medical device software updates
    - 3rd party software updates or patches
  - Information to operators of medical devices on the identified risk

Software Updates & Recertification

- Changes that should be considered a **significant change in design or intended purpose** require reporting to a notified body.
- → The MDCG guideline 2020-03 tries to clarify:
- Minor changes without impact to diagnosis or treatment:
  - Correction of an error which does not pose a safety risk (bugfixes),
  - Security update (e.g., cyber-security enhancements)
  - And some more software changes
- Reducing risks via software changes is considered major changes!

Supply Chain?

- Software Bill of Materials (SBOM)
  - Digital information sheet for software components and its dependencies
- Relevance: For which audience is the information?
  - MDCG 2019-16 mentions the SBOM as to be shared with operators
    - Hard to assess whether a component really is vulnerable
    - → Useless for medical device operators

Supply Chain?

OASIS Draft

- Common Security Advisory Framework (CSAF) 2.0
  - Standard for automated and interoperable exchange of advisories
  - Can be mapped to SBOM data of a specific product
- Profile: Vulnerability Exploitability eXchange (VEX)
  - Provide information on whether a product is impacted by a vulnerability
  - Are there remediations / workarounds recommended?
- Relevant information for vendors, systems integrators, and operators: **Is there a risk? What do we need to do to reduce it?**

Vulnerability Disclosure Processes

MDR - Vulnerability Disclosures?

- The MDR poses requirements for a PMS that includes security
- The MDR does not actively require a vulnerability disclosure statement, but the notified body / auditor may require a mature vulnerability disclosure process as part of an effective and successful PMS.
    - → “Sharing and dissemination of cybersecurity information and knowledge of cybersecurity vulnerabilities and threats”

ERNW RESEARCH pursuing knowledge.

Experiences from Disclosures

- Few manufacturers publish a vulnerability disclosure statement or contact information
- Manufacturers wanted a proof of impact on patient safety to act
- Complexity of creating fixes and rollouts to the field:
  - Development process complexity & release cycles
  - Fixes and remediations: simple fix vs. the device is "totally broken"
  - Update process complexity requires a service technician
- Communication:
  - Stagnant progress and ambiguous statements about future actions
  - Strict information policies that strictly prohibit sharing information

Experiences from Disclosures

- Limit misunderstandings and ease the process by providing:
  - Information about the vulnerabilities
    - A detailed explanation of every vulnerability
    - Recommendations for fixes
    - Descriptions with observed (safety) impacts (videos of the device crashing, unintended behavior, etc.)
  - Information about the process
    - Expectations to communication and responsiveness
    - Expectations to process timelines (start the clock!)
    - Intended results such as CVEs, blog posts, white papers, etc.
  - Escalation paths:
    - Involvement of authorities such as BfArM / BSI or a CERT

Closing

Summary

- Many vulnerabilities concerning medical devices are not specifically medical, but the operation environment is.
- MDR and its processes and requirements will help to:
  - Focus on the relationship between safety and security
  - Apply mature IT security process in the medical sector
  - Security verification and validation testing will increase the security level of new products in the product's lifecycle

Challenges

- Short-term impairment on security as of certification
- Rendering legacy devices compliant to MDR requirements
- How to secure an existing environment with existing equipment?
  - Customers are not replacing the entire environment at once
  - Compatibility between old and new equipment and devices?
- Securing and operating on-premise and cloud environments
  - Safety impact of cloud or connection outage?
  - Medical devices with permanent cloud connections?

ERNW
RESEARCH
pursuing knowledge.

Thank you for your Attention!

✉

@jsuleder

www.ernw.de

www.insinuator.net