VDGH
Verband der Diagnostica-Industrie

IT-Product Security Whitepaper Template

V1.4

VDGH

24.01.2020

VDGH
Verband der Diagnostica-Industrie

Content

1. Introduction

IT Security of Medical Devices, also called “Product Security” is an important aspect of their function. It is absolutely necessary to ensure their safe operation, and to ensure:

- Confidentiality of patient data
- Integrity of the Medical Device, in other words that the device functions as intended
- Availability of the Medical Device

To ensure Product Security, a Medical Device, has to be designed, implemented and tested properly – but it also needs to be installed, configured, maintained and operated as intended.

If any of these aspects is not observed, the Medical Device’s Product Security can be easily compromised, with potential grave consequences for its safety.

The intention of the Product Security Whitepaper is to ensure that people and institutions responsible for installation, maintenance and operation of Medical Devices have all required information to do their work properly:

- Provide information regarding all relevant Product Security aspects to customer and service personnel.
- Ensure that all data and guidance are available which are required to install, configure, maintain and operate the system securely.

In addition, the Security Whitepaper is intended to provide all information that may be required during the procurement and selection process for the Medical Device, thus avoiding the need for customer specific questionnaires.

This document is intended to provide a standard Security Whitepaper content template to be used across the healthcare industry.

Product Security Whitepaper - Content

The following content should be considered when writing the Security Whitepaper for any Medical Device – system, software only or solution. The actual content has to be adapted to the specific nature of the Medical Device in question.

Purpose of this Document

This Product Security Whitepaper describes the technical aspects of <product name> that are relevant for IT Security and it is mainly intended for the service and customer personnel that are responsible for installation, configuration, maintenance, and operation and for Marketing and Sales to support the procurement process. But it also should be made available to customers on demand for transparency.

This Product Security Whitepaper contains all required information to:

- Support the procurement and selection process for the Medical Devices.
- Avoid the need for generic security questionnaires.
- Provide this information to customer and service personnel.
- Securely install, configure, maintain, and operate the Medical Devices.

2. Security Program

Generic (marketing) information on the security program and incident and vulnerability management, and additionally information on:

- Security by design
- Security testing
- Secure configuration
- Security training
- Contact address (email, website) to submit vulnerability and incident notifications
- Other security program elements implemented by the supplier

3. System Information

3.1. System Overview

Brief overview of the solution:

- Description of the device, it's intended use and market segment, taken from marketing information
- Device list (analyzers, PCs, network equipment, etc.)
- Intended use statement
- Intended operational environment
- Operation in virtualization environments

3.2. Hardware Specifications

Description of details of the hardware that is being shipped (even if not used) or that is required (at the minimum) to operate the solution, including:

- Full specs of PCs or servers
- Input devices such as keyboard, mouse, and touch
- Output devices such as monitors and printers
- External LAN, USB or Firewire ports
- Handheld barcode reader
- Uninterruptible power supply
- Wireless communication components (Wi-Fi, Bluetooth, infrared, RFID)
- Camera, Microphone, Fingerprint reader
- Compliance (CE, RoHS, FCC)

3.3. Product Software

Description of the security-related features and aspects of the solution

- User Authentication
- Audit Logging
- Connectivity
- Software Updates and Patches
- Reports
- Database

3.4. Operating System

Configuration of the OS that is shipped with the solution or configuration that the customer is required to provide to run the solution:

3.4.1. **OS Version information**

- Name and version of the operating system

3.4.2. **Patch level and patch policy**

- Patch Level of the operating system at delivery
- Vendor patch policy and interval

3.4.3. **Firewall**

- Type, name and version of firewall
- State
- Exceptions
- Logging
- Default deny for in / out connections

3.4.4. **Network Configuration**

- Internet/Web Access restricted
- IPv6

3.4.5. DHCP requirements

- DNS requirements
- Wi-Fi (including encryption algorithm)

3.4.6. Hardening

- Standard or custom?
- Unneeded accounts disabled
- Unneeded file shares disabled
- Unneeded ports disabled
- Unneeded services disabled
- Unneeded applications disabled
- Restriction of external (USB) devices
- Authentication of external devices (e.g. USB Type-C Authentication specification)

3.4.7. Customer Supplied Software

- Printer drivers
- Customer antimalware
- Other tools

3.5. Third Party Software

Software supplied by other suppliers (3rd party suppliers) with the system / solution or required to operate it. May be Off-The-Shelf Software (OTS) or Open Source Software (OSS)

- Type of Software
- Supplier
- Version information
- Licensing information
- Vulnerability Monitoring & Patching
- Configuration information
- Which configuration settings are required for regular use

3.6. Connectivity

Description of how the solution connects to its environment and how it interacts with it:

- How does the system connect to the environment
- IP configuration

  - LIS / LAS / Remote Service Connectivity
    - Protocol & (Default/Serial) Ports
    - Modes and default mode (Server/Client)
    - Data format (file format or application layer protocol)
    - Services running on the System
    - Idling Time

  - **For each type of connectivity**:
    (For example: Secure Download, Web Service, SOAP, VNC, Remote Desktop, File Share)

- Protocol & (Default) Ports (e.g. SMB/124)
- Services running on the System
- Service Discovery
- Data format (file format or application layer protocol)
- Multicast
- Idling Time

3.7. Security Patching

- Description of Patch Process (vendor or customer supplied patches)
- Availability pf patches
    - Components which are being patched
    - Timeframe of patching
    - Delivery channels for patches

3.8. Sensitive Data

- Types of sensitive data that is processed by the solution (e.g. demographic, diagnostic, therapeutic, financial, employee or other PII).
- Statement on how the customer's data is processed (e.g. stored on or transmitted to the vendor's infrastructure or local storage only).
- Methods and scenarios used to de-identify sensitive data (e.g. replacement of data by asterisks when service is logged in, in log files or in printed reports) – anonymization and / or pseudonymization
- Handling of sensitive data in transit or at rest (e.g. encrypted when transmitted via network, when exported, when at rest in database)
- Handling of sensitive data when system is decommissioned

4. Network Diagram

4.1. Network diagram of the solution

<network diagram>

4.2. Network diagram of the solution within the customer environment

<example network diagram>

5. Security Controls

5.1. Security Controls Overview

Short summary of all security controls described in this document.

5.2. Malware and Vulnerability Protection

5.2.1. Whitelisting Software and Antivirus

- Is software pre-installed?
- Exceptions for specific folders configured?
- Customer supplied anti-virus allowed?
- Are (Pattern-) updates provided for pre-installed software?

5.2.2. Additional Security Applications

- EMET
- AppLocker
- Backup Solutions
- (User Account Control)
- (Windows Defender)

5.3. Network Controls

Description of controls implemented to protect the solution and the environment from attacks:

- Usage of security appliances
- Firewall configuration
- Intrusion detection systems
- Network segmentation

5.4. Incident and Vulnerability Handling - Software Updates and Security Patches

Description of

- Patch / vulnerability remediation process (vendor or customer supplied patches),
- Availability of patches (components, time frame, delivery channels) and the
- Vulnerability handling process

5.5. Remote Connectivity

How is remote connectivity secured? Description of the process (including training) and the security controls.

5.6. Authentication and Authorization

5.6.1. Accounts

- Purpose of each account
- Hidden accounts
- Shared accounts

5.6.2. Default accounts Role based access control

- Description of the roles

5.6.3. Authentication Mechanisms

- LDAP/AD Directory integration
- PKI or Dual Factor Authentication
- Session timeout
- Username / Password
    - Passwords are changeable by the customer
    - Unique passwords per system or product
    - Admin access for the customer
    - Requirement to change the initial password before use
- Credentials cached in the system (excluding OS)
- Verbose error messages (user name or password…)

5.6.4. Break the Glass concept

- How does the mechanism work?
- Where is the use logged?

5.6.5. Password rules

- Min Length
- Complexity
- Expiration
- Reuse

5.6.6. Data Segregation

Description of the data segregation mechanism, if the system has one.

Explanation: Data segregation means that data from different users or from different use cases is strictly separated. For example, an application could store private (and personal) data from the user, and also company proprietary data. These data should not be stored in the same location.

5.7. Physical Protection

Description of physical protections measures that were implemented or need to be implemented by the customer, e.g.:

- Protection of external ports
- Access control systems
- Environment Requirements

5.8. Event/Audit Logging

List of logging capabilities of the solution, for example:

- Windows audit logging
- Software audit trail
- Software trace logs
- Firewall logging
- (Audit) log file protection against manipulation
- External log server support (e.g. syslog)
- Specify what events are logged and how long it is stored
- Information in logs: e.g. user ID, date, time, and resources accessed
- Display of logging events: displayed to the user and/or pushed to another system (e.g. log server) without delay

5.9. Data Protection

List of actions taken to protect sensitive data, e.g.:

5.9.1. Protection of data in transit

- Encrypted network traffic
- Does the solution/device send PHI or PII?
- Specify method, algorithm, key length, shared secret or certificate, …

5.9.2. Protection of data at rest

- Encrypted hard disk
- Encrypted database / data files
- Does the solution/device store PHI or PII?
- Specify method, algorithm, key length, …

5.9.3. Protection of exported data

- Encrypted backups
- Encrypted exports
- Specify method, algorithm, key length, shared secret or certificate, …

5.9.4. Additional data protection

- Memory protection
- Data integrity protection
- Encrypted external media support

5.9.5. Cloud / hosted solutions

- Is data stored on company servers?
- Where are these servers located?

5.9.6. Data handling at end of life of device

- Mechanisms for secure deletion of sensitive data

5.10. Disaster Prevention and Recovery

Description of all disaster prevention and recovery features and measures, including:

- Backup and restore mechanism
- Support for customer supplied backup solutions
- External storage support
- Data compressions algorithms
- Support for multiple archive destinations
- Automatic purging of data

5.11. Compliance and Certifications

Description of any standards that the solution complies with and any certification that the solution has got, e.g.:

- Standards (IEC 27001, 80001, 62443, …)
- Certifications (RMF (formerly DIACAP), …)
- Regulations (HIPAA, …)

6. Secure Configuration

6.1. Installation and Initial Configuration

Description of any security-related aspects during installation and initial configuration (can be duplicates of the information above), including:

- Physical Protection
- Firewalls and network configuration
- Initial passwords that need to be changed
- Software updates that need to be installed
- Integration into the customer's IT infrastructure
- Trainings that need to be completed prior to installing or operating the solution

6.2. Modifications to the System

Description of what the customers are allowed to do and how they should do it, e.g.

- Password change
- Customer specific protection software
- Customer provided printer drivers
- Customer provided logging solutions
- Customer provided anti-malware solutions

Responsibility of the customer in case of modifications, including requirements for revalidation.

6.3. Security best-practices

Collection of rules for operation of the solution, e.g.:

- Do not access the internet from the device
- Do not directly expose the device to the internet
- Never install unapproved software
- Use the system only for its intended purpose
- Do not connect radio links
- Only change system settings if it is explicitly allowed (documented in manuals)
- Report strange behavior of the system to the customer service

7. Regulatory Compliance

7.1. EU General Data Protection Regulation 2016/679 (GDPR)

The General Data Protection Regulation (GDPR) has been released on 04 May 2016 and is in applicable since 25 May 2018. The regulation enforces strict data protection rules, which are also applicable for personal health data handled by medical device software.

GDPR requests two specific principles to be implemented:

Privacy by Design: Data privacy through technology design - The design and implementation of the system shall ensure that privacy requirements are met.

Privacy by Default: The configuration of the system ensures privacy out of the box – the system shall be configured in such a way that privacy is ensured directly after installation, without having to do/enable additional security settings.

The chapter states how these principles are met. It also lists specific organizational and technical elements that have been implemented in order to achieve GDPR compliance:

- Has a Privacy Impact Assessment been done
- Does the system store personal data
  If yes: list data types (e.g. data concerning health [sensitive], genetic data [sensitive], biometric data, personal data)
  and state the purpose of data storage.
- Is only the minimum required personal data stored?
- Are personal data stored in anonymized or pseudonymized form?
- Can the user customize the data collection? If yes: how?
- Can personal data be permanently erased?
- Are personal data encrypted in rest on the system / in transit outside of the system?
- Are personal data transferred to other systems?
  - via network connections
  - via logfiles
  - via remote connectivity
- Are any personal data transferred to the supplier of the system? If yes, state how GDPR compliant handling of these data is ensured.
  - Are any such personal data transferred to third parties, e.g. subcontractors?
  - If yes: are contracts governing the compliant handling of these data in place?
- Are personal data protected from loss
  - backup mechanisms
- Are personal data protected from unlawful processing
  - User access control mechanisms in place
  - For all users, including administrators, standard users, service personnel
- Can personal data be exported to ensure data portability

8. Attachment: MDS² Form

https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/Expertenkreis_CyberMed_MDS2.pdf?__blob=publicationFile&v=3

9. Legal Statement / Disclaimer

<disclaimer>