Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Finance FDF
National Cybersecurity Centre NCSC
GovCERT.ch

TLP:WHITE

Recommendations on cybersecurity in the healthcare sector

Date:	24 May 2022
Version:	v1.0
Author:	NCSC/GovCERT

Introduction

The National Cybersecurity Centre NCSC recommends that all healthcare providers implement the minimum cybersecurity requirements set out in this paper. The NCSC considers them to be best current practice. It is important that both technical and organisational measures are defined and implemented.

Overview of measures

The following is an overview of the measures, which are discussed in more detail later in this paper.

Measure	**Implementation**	**Requirement**
Patch and lifecycle management, at technical and organisational level	Organisational	mandatory
Timely monitoring of the security perimeter log data	Organisational and technical	mandatory
Timely monitoring of endpoints	Technical	optional
Patch and lifecycle management	Organisational and technical	mandatory
Membership in the NCSC closed client base	Organisational	optional
Offline backups/disaster recovery	Technical	mandatory
Network segmentation	Technical	mandatory
Authentication protection	Technical	mandatory
Blocking dangerous email attachments	Technical	optional
Controlling file execution	Technical	optional

Patch and lifecycle management (organisational)

A concept **must** be developed and maintained for the patch and lifecycle management of software.

Software has a certain service life during which functional and security updates (patches) are provided. It is therefore essential that software is systematically provided with security updates in a timely manner. Such a concept regulates the lifespan of software (when does it need to be replaced?) as well as when security updates need to be applied. It also helps to regularly identify software that has reached the end of its service life and is therefore no longer supported with security updates (patches) (end of life – EOL) and should therefore be replaced.

Patch and lifecycle management (technical)

A system for managing software and security updates (patches) **can** be used for patch and lifecycle management of software.

Software has a certain service life during which functional and security updates (patches) are provided. It is essential that software is systematically provided with security updates in a timely manner. Automatic software distribution, such as Microsoft SCCM[1], enables organisations to keep track of the software landscape (which software version is running on which devices?), to distribute software automatically and to simplify patch management. It also helps to identify software that has reached the end of its service life and is therefore no longer supported with security updates (patches) (end of life – EOL) and should therefore be replaced.

Systems and software that no longer receive security updates but still have to be operated for organisational or operational reasons should be given additional protection. For example, they should be moved to a separate, isolated network zone. A particular challenge here is medical equipment, which often has to run on a precisely defined software stack for certification reasons.

Monitoring the security perimeter log data (organisational and technical)

Software and devices of the security perimeter (such as antivirus, firewall, web proxy and intrusion prevention systems like IDS/IPS) **must** record all activities. The recorded activities **must** be promptly reviewed for suspicious activities, intrusion attempts and detected attacks. It must be ensured that data leaks and traffic flow anomalies are detected quickly. Similarly, visibility and response capabilities on endpoints and servers must be improved. Alarm notifications generated by software and devices of the security perimeter must also be reviewed in a timely manner. These tasks **must** be carried out by appropriately trained personnel.

One possibility, for example, is a Security Operations Centre (SOC). This can identify attempted attacks and, if necessary, initiate appropriate countermeasures. In addition, it can

[1] https://en.wikipedia.org/wiki/Microsoft_Endpoint_Configuration_Manager

support an organisation in dealing with cybersecurity incidents in the event of an emergency (incident response process).

There are different options for operating a SOC:

- **Internal SOC**: The SOC is operated within the organisation with its own resources and corresponding expertise.
- **External SOC**: An external SOC-as-a-Service of a managed security service provider (MSSP) or a town/city/canton assumes operation of the SOC.
- **Association**: Several listed hospitals join forces and operate a SOC together (e.g. a hospital group).

Monitoring the security perimeter log data (technical)

The endpoints in a network (server, clients) should be monitored as closely as possible. It also makes sense to have a high level of visibility and response capabilities. This **can** be achieved by using an EDR/XDR (endpoint detection and response) tool.

Membership in the NCSC closed client base (MELANI-Net)

Membership in the NCSC closed client base (MELANI-Net) is **recommended**. This offers a multitude of advantages, and the members' sole obligation is to maintain confidentiality:

- Access to the secure exchange platform MELANI-Net. This platform informs and alerts members about important events and information concerning the cyberthreat situation.
- Access to NCSC services. These provide members with additional technical protection against cyberthreats and, in the event of a cyberincident, additional technical and human resources to analyse and defend against attacks.

Authentication protection, in particular multi-factor authentication (MFA) for remote access

Internal resources of an organisation that can be accessed via the internet (e.g. Sharepoint, webmail, but also remote access systems such as VPN, Citrix and RPD) **must** be secured with a second factor (multi-factor authentication – MFA). If the use of MFA is not possible for technical or organisational reasons, access **must** be secured via other technical measures such as restricting access to certain IP address ranges. Similarly, multi-factor authentication **must** be used to manage the IT infrastructure.

Central elements of the authentication infrastructure such as a user administration (e.g. Windows Active Directory) must be specially protected and monitored.

Blocking dangerous email attachments

There are numerous file types that are used in dangerous email attachments to spread malware. However, these file types are often used little, if at all, in business contexts. Using technical means, such dangerous file types[2] **can** already be filtered out on the email platform/using the spam filter.

Since many malware families are now spread via malicious Office documents such as Word or Excel files, it is **recommended** to filter all Office documents that contain macro program code or to mark such emails so that they are visible to the user.

Controlling file execution

A very effective security measure is to control which users are allowed to execute files from which directories. This can be achieved with tools to regulate file execution (e.g. Windows AppLocker). Likewise, the execution of macro program code in Office documents can be restricted to trusted (and digitally signed) macros. These two measures provide a high level of protection against cyberattacks involving malicious Office documents.

Network segmentation

Segmenting hospital networks is still a very important security measure. In most cases, business IT is the initial attack vector. Therefore, transitions into network zones with medical devices should be as few and as clearly defined and monitored as possible.

Another interesting approach is virtualisation on the end device, where – invisible to the user – sensitive areas, such as access to patient data, are separated from insecure activities, such as internet searches or reading emails, by means of a virtualisation layer.

Offline backups and disaster recovery

Backup copies of data **must** be available securely, i.e. isolated from the network (**offline**). This ensures, for example, that in the event of a ransomware attack and the subsequent encryption of the data, a functioning backup copy is available which can be restored once the infection has been removed.

Recovery time objectives (RTO) and recovery point objectives (RPO) are the biggest challenge in a widespread ransomware outbreak: it must be clear how long it will take to rebuild the infrastructure in the event of a large-scale cyberattack. Since this usually takes longer, the hospital must have interim solutions in place that can maintain at least minimal operations. These solutions should be technically ready for use, but completely separated from daily operations, and should be maintained and regularly tested.

[2] https://www.govcert.ch/downloads/blocked-filetypes.txt