Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Nationales Zentrum für Cybersicherheit NCSC
GovCERT.ch

TLP:WHITE

Empfehlungen zur Cybersicherheit im Gesundheitssektor

Datum:	24. Mai 2022
Version:	v1.0
Autor:	NCSC / GovCERT

Einleitung

Das Nationale Zentrum für Cybersicherheit NCSC empfiehlt allen Dienstleistern im Gesundheitswesen die in diesem Papier aufgeführten Mindestanforderungen an die Cybersicherheit umzusetzen. Das NCSC erachtet diese Mindestanforderung als «Best Current Practice». Es ist wichtig, dass sowohl technische wie auch organisatorische Massnahmen definiert und umgesetzt werden.

Übersicht Massnahmen

Nachfolgend eine Übersicht der Massnahmen, welche weiter in diesem Dokument vertieft beleuchtet werden.

Massnahme	Umsetzung	Vorgabe
Patch- und Lifecycle Management, auf technischer und organisatorischer Ebene	Organisatorisch	Muss
Zeitnahe Überwachung der Logdaten des Sicherheitsperimeters	Organisatorisch und Technisch	Muss
Zeitnahe Überwachung der Endpunkte	Technisch	Kann
Patch- und Lifecycle Management	Organisatorisch und Technisch	Muss
Mitgliedschaft im geschlossenen Kundenkreis des NCSC	Organisatorisch	Kann
Offline-Backups / Disaster Recovery	Technisch	Muss
Netzwerk-Segmentierung	Technisch	Muss
Schutz der Authentisierung	Technisch	Muss
Blockierung von gefährlichen E-Mail Anhängen	Technisch	Kann
Kontrolle der Ausführung von Dateien	Technisch	Kann

Patch- und Lifecycle-Management (organisatorisch)

Für das Patch- und Lifecycle-Management von Software **muss** ein Konzept erarbeitet und unterhalten werden.

Software hat eine bestimmte Lebensdauer, während welcher diese mit Funktions- und Sicherheit-Updates (Patches) versorgt werden. Es ist daher essenziel, dass solche konsequent und zeitnah mit Sicherheitsupdates versorgt werden. Ein entsprechendes Konzept regelt die Lebensdauer von Software (wann muss diese ersetzt werden?) sowie wann ein Sicherheitsupdate eingespielt werden muss. Es hilft zudem, regelmässig Software zu identifizieren, welche das Ende ihrer Lebensdauer erreicht hat und daher nicht mehr mit Sicherheitsupdates (Patches) versorgt wird («End Of Life» - EOL) und somit ersetzt werden sollte.

Patch- und Lifecycle-Management (technisch)

Für das Patch- und Lifecycle-Management von Software **kann** ein System für die Verwaltung von Software und Sicherheitsupdates (Patches) eingesetzt werden.

Software hat eine bestimmte Lebensdauer, während welcher diese mit Funktions- und Sicherheit-Updates (Patches) versorgt werden. Es ist essenziel, dass solche konsequent und zeitnah mit Sicherheitsupdates versorgt werden. Eine automatische Softwareverteilung wie z.B. Microsoft SCCM[1] ermöglicht es der Organisation, einen Überblick über die Softwarelandschaft zu erhalten (welche Software-Version läuft auf welchen Geräten?), Software automatisch zu verteilen sowie das Patch-Management zu vereinfachen. Es hilft zudem Software zu identifizieren, welche das Ende ihrer Lebensdauer erreicht hat und daher nicht mehr mit Sicherheitsupdates (Patches) versorgt wird («End Of Life» - EOL) und somit ersetzt werden sollte.

Systeme oder Software, welche keine Sicherheitsupdates mehr erhalten jedoch aus organisatorischen oder betrieblichen Gründen weiter betrieben werden müssen, sollen zusätzlich abgesichert werden. Beispielsweise sollten diese in eine separate, isolierte Netzwerkzone verschoben werden. Eine besondere Herausforderung sind dabei Medizinalgeräte, welche aufgrund der Zertifizierung oft auf einem genau definierten Software Stack laufen müssen.

Überwachung der Logdaten des Sicherheitsperimeters (organisatorisch und technisch)

Software und Geräte des Sicherheitsperimeters (wie Beispielsweise Antivirus, Firewall, Web-Proxy oder Intrusion Prevention Systeme wie IDS/IPS) **müssen** sämtliche Aktivitäten aufzeichnen. Die aufgezeichneten Aktivitäten **müssen** zeitnah auf verdächtige Aktivitäten, Einbruchsversuche oder detektierte Angriffe geprüft werden. Es muss sichergestellt werden, dass Datenabflüsse und Verkehrsflussanomalien rasch erkannt werden. Ebenso müssen die Sichtbarkeit und Reaktionsmöglichkeit auf Endgeräten und Servern verbessert werden. Alarm-Meldungen, welche von Software oder Geräten des Sicherheitsperimeters generiert werden, müssen ebenfalls zeitnah geprüft werden. Mit der Erfüllung dieser Aufgaben **muss** entsprechend geschultes Personal betraut werden.

Eine Möglichkeit bietet Beispielsweise ein «Security Operation Center» (SOC).

[1] https://de.wikipedia.org/wiki/System_Center_Configuration_Manager

Ein solches kann Angriffsversuche identifizieren und, falls nötig, entsprechende Gegenmassnahmen einleiten. Zudem unterstützt es die Organisation im Ernstfall bei der Bewältigung von Cybersicherheitsvorfällen («Incident Response»-Prozess).

Es gibt unterschiedliche Möglichkeiten für den Betrieb eines SOC:

- **Internes SOC**: Das SOC wird innerhalb der Organisation mit eigenen Ressourcen und entsprechendem Fachwissen betrieben.
- **Externes SOC**: Ein externes «SOC-as-a-Service» eines «Managed Security Service Providers» (MSSP) oder einer Stadt / eines Kantons übernimmt den Betrieb des SOC.
- **Zusammenschluss**: Mehrere Listenspitäler schliessen sich zusammen und Betreiben zusammen ein SOC (z.B. Spitalverbund).

Überwachung der Logdaten des Sicherheitsperimeters (technisch)

Die Endpunkte in einem Netzwerk (Server, Clients) sollen so gut wie möglich überwacht werden. Es ist auch sinnvoll, eine hohe Sichtbarkeit und Reaktionsmöglichkeit zu besitzen. Dies **kann** durch den Einsatz eines EDR/XDR (Endpoint Detection and Response) Werkzeugs erreicht werden.

Mitgliedschaft im geschlossenen Kundenkreis des NCSC (MELANI-Net)

Eine Mitgliedschaft im geschlossenen Kundenkreis des NCSC («MELANI-Net») wird **empfohlen**. Diese bietet eine Vielzahl von Vorteilen, wobei sie die Mitglieder lediglich zur Geheimhaltung verpflichtet:

- Zugang zu sicherer Austauschplattform «MELANI-Net». Über diese werden die Mitglieder auch über wichtige Ereignisse oder Informationen betreffend der Cyber-Bedrohungslage informiert und alarmiert.
- Zugang zu den Dienstleistungen des NCSC. Diese bieten den Mitgliedern einen zusätzlichen technischen Schutz vor Cyberbedrohungen sowie im Falle eines Cybervorfalles, zusätzliche technische und personelle Ressourcen zur Analyse und Abwehr des Angriffs.

Schutz der Authentisierung, insbes. Multi-Faktor-Authentisierung (MFA) für Fernzugänge

Interne Ressourcen einer Organisation, welche über das Internet erreichbar sind (Beispielsweise Sharepoint, Webmail aber auch Remote-Zugänge wie VPN, Citrix oder RPD) **müssen** zwingend mit einem zweiten Faktor abgesichert werden (Multi-Faktor-Authentisierung – MFA). Sollte der Einsatz von MFA aus technischen oder organisatorischen Gründen nicht möglich sein, **muss** der Zugang über andere technische Vorkehrungen wie Beispielsweise

die Einschränkung des Zugriffs für bestimmte IP-Adress-Bereiche abgesichert werden. Ebenso **muss** eine Multi-Faktor-Authentisierung für das Management der IT-Infrastruktur verwendet werden.

Zentrale Elemente der Authentisierungsinfrastruktur wie eine Benutzerverwaltung (z.B. Windows Active Directory) müssen speziell geschützt und überwacht werden.

Blockierung von gefährlichen E-Mail Anhängen

Es gibt eine Vielzahl von Dateitypen von gefährlichen E-Mail Anhängen, welche für die Verbreitung von Schadsoftware (sogenannter «Malware») verwendet werden. Oftmals werden diese Dateitypen im Geschäftsumfeld jedoch wenig oder gar nicht gebraucht. Solche gefährlichen Dateitypen[2] **können** technisch bereits auf der E-Mail-Plattform bzw. dem Spam-Filter gefiltert werden.

Da sich mittlerweile viele Malware-Familien über schädliche Office Dokumente wie Word oder Excel verbreiten **empfiehlt** sich zudem, sämtliche Office Dokumente, welche Makro-Programmcode enthalten, ebenfalls zu filtern oder solche E-Mails für den Benutzer sichtbar zu markieren.

Kontrolle der Ausführung von Dateien

Eine sehr wirksame Sicherheitsmassnahme ist die Kontrolle darüber, welche Benutzer/innen aus welchen Verzeichnissen Dateien ausführen dürfen. Dies kann mit Werkzeugen zur Steuerung der Ausführung erreicht werden (z.B. Windows AppLocker). Ebenso kann das Ausführen von Makro-Programmcode in Office Dokumenten auf vertrauenswürdige (und digital signierte) Makros eingeschränkt werden. Diese beiden Massnahmen bieten eine hohe Schutzwirkung gegen Cyberangriffe mit schädlichen Office Dokumenten.

Netzwerk-Segmentierung

Eine Segmentierung der Netzwerke in einem Spital ist nach wie vor eine sehr wichtige Sicherheitsmassnahme. In den meisten Fällen ist der initiale Angriffsvektor die Geschäfts-Informatik. Deshalb sollte es möglichst wenige und klar definierte und überwachte Übergänge in Netzwerkzonen mit medizinischen Geräten geben.

Ein ebenfalls interessanter Ansatz ist die Virtualisierung auf dem Endgerät, bei der – für den Benutzer unsichtbar – heikle Bereiche wie der Zugriff auf Patientendaten von unsicheren Tätigkeiten wie dem beispielsweise Recherchen im Internet oder dem Lesen von E-Mails durch eine Virtualisierungsschicht getrennt werden.

Offline-Backups und Disaster Recovery

Sicherungskopien von Daten (sogenannte «Backups») **müssen** sicher, das heisst vom Netzwerk getrennt («**Offline**») zur Verfügung stehen. So kann beispielsweise sichergestellt wer-

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

den, dass bei einem Ransomware-Angriff und der darauffolgenden Verschlüsselung der Daten eine funktionstüchtige Sicherungskopie vorhanden ist, welche nach der Bereinigung der Infektion wiederhergestellt werden kann.

Wiederherstellungsziele (RTO – Recovery Time Objective und RPO – Recovery Point Objective) sind bei einem weit verbreiteten Ransomware-Ausbruch die grösste Herausforderung: Es muss klar sein, wie lange es dauert, bei einem grossflächigen Cyberangriff die Infrastruktur neu aufzubauen. Da dies in der Regel länger Zeit in Anspruch nimmt, muss das Spital Zwischenlösungen bereit haben, welche zumindest einen minimalen Betrieb aufrechterhalten können. Eine solche Zwischenlösung sollte technisch einsatzbereit, aber komplett abgekoppelt vom täglichen Betrieb bereitstehen, gewartet und regelmässig getestet werden.