AVENIQ

Cyber Resilience in Healthcare

Facing the Future

Cen Magjuni, Consultant BCM & Krisenmanagement

Cham, 31.05.2022

Agenda

- Aktuelle Cyber-Bedrohungslage
- Warum das Gesundheitswesen Cyber-Angriffen ausgesetzt ist
- Feststellungen aus der Praxis: Falsche Umsetzung von Sicherheit
- Cyber-Resilienz im Gesundheitswesen

Agenda

- Aktuelle Cyber-Bedrohungslage
- Warum das Gesundheitswesen Cyber-Angriffen ausgesetzt ist
- Feststellungen aus der Praxis: Falsche Umsetzung von Sicherheit
- Cyber-Resilienz im Gesundheitswesen

Cyber-Bedrohungslage für das Gesundheitswesen

Fallzahlen Europa 2. HJ 2021

Juli

05.07.2021
Saint-Ouen-l'Aumône (F)
Labor

14.07.2021
Wolfenbüttel (D)
Krankenhaus

14.07.2021
Périgueux (F)
Krankenhaus

Sommer 2021
Paris (F)
Gesundheitsdienstl.

16.07.2021
Paris (F)
Forschungsinstitut

August

02.08.2021
Arles (F)
Krankenhaus

12.08.2021
Olten (CH)
Krankenhäuser

Aug 2021 ?
Nijmegen (NL)
Krankenhaus

August 2021
Berlin (D)
Augenarzt

18.08.2021
Florenz (I)
Gesundheitsbehörde

August 2021
Angers (F)
Apotheke

September

Sep 2021
Syston
Scanning

Sep 2021
Antwerpen (B)
Krankenversicherung

12.09.2021
Vessy (CH)
Alten- und Pflegeheim

14.09.2021
Rom (I)
Krankenhaus

Sep 2021
Veenendaal (NL)
Pflegeeinrichtung

20.09.2021
Heidelberg (D)
Krankenhäuser

Oktober

09.10.2021
Namur / Bouge (B)
Krankenhaus

14.10.2021
Savona (I)
Gesundheitsuntern.

21.10.2021
Bordeaux (F)
Krankenhaus

30.10.2021
Rom (I)
Gesundheitseinricht.

November

Nov 2021
Eltville am Rhein (D)
Praxis-Software

Nov 2021
Eugendorf (A)
Covid-Testportal

14.11.2021
Oberottmarshausen (D)
Schutzmasken

16.11.2021
Messina (I)
Gesundheitsbehörde

29.11.2021
München (D)
Krankenhausgesellsch.

Dezember

01.12.2021
Braunschweig (D)
Krankenhaus

01.12.2021
Hazebrouck (F)
Krankenhaus

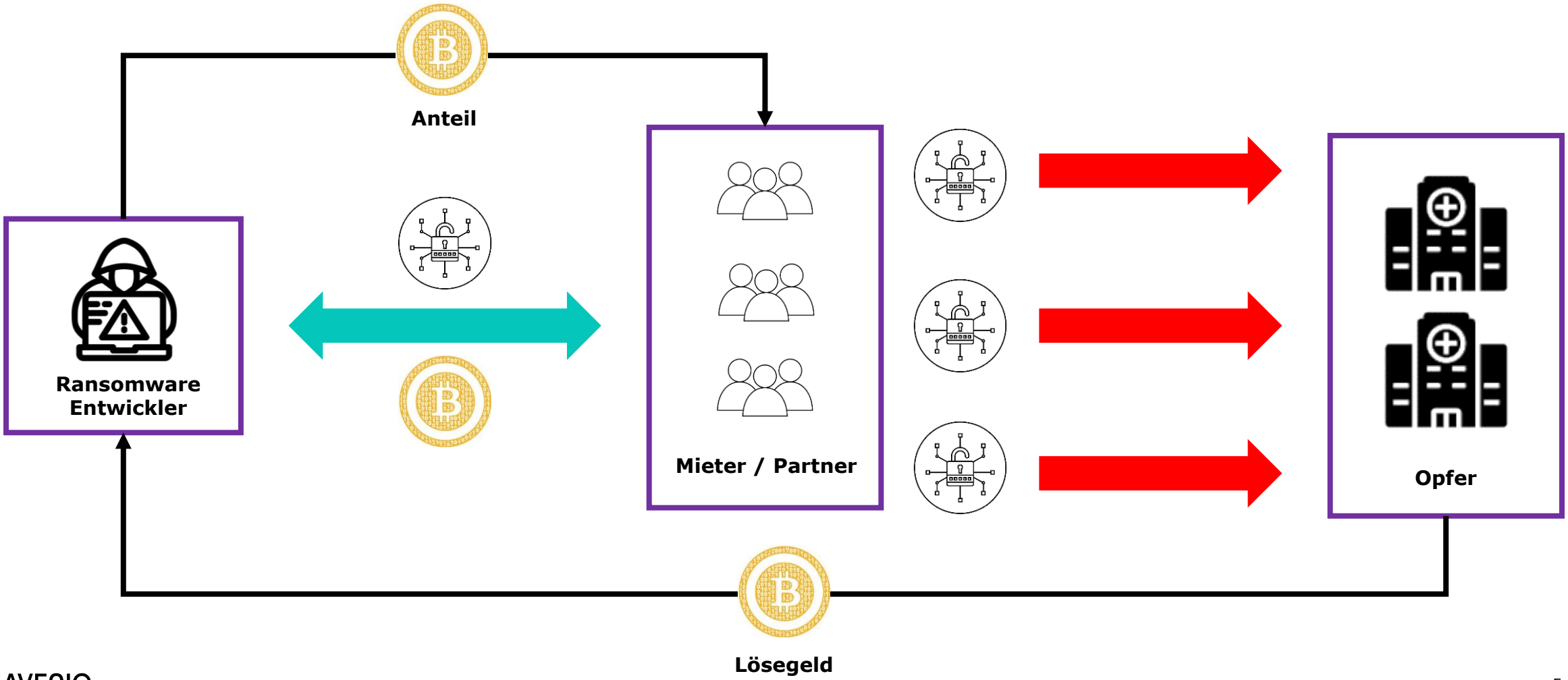
03.12.2021
Padua (Padova) (I)
Gesundheitsdienstl.

05.12.2021
Ponferrada (E)
IT-Dienstl, Krankenh.

Dez 2021
Düsseldorf (D)
Zahnarztpraxis

Cyber-Bedrohungslage für das Gesundheitswesen

Leichtes Spiel für Angreifer: Ransomware as a Service (RaaS)



Cyber-Bedrohungslage für das Gesundheitswesen

Herausforderungen

Komplexe Aufgaben …

- Hochentwickelte und häufigere Cyber-Angriffe
- Ständig wechselnde Cyberä-Bedrohungslandschaft
- Digitalisierung bringt neue Sicherheitsherausforderungen mit sich
- Immer komplexere IT-Landschaften zu managen
- Gesetzliche Anforderungen

… grosse Auswirkungen

- Management (Verantwortlichkeiten, strategische Entscheide, Ressourcen etc.)
- Prozesse (Incident Management, Business Continuity, Risk Management, Vulnerability Management etc.)
- Leute (Sicherheitsbewusstsein, Schulungen, Kommunikation etc.)
- Systeme (IT-Hygiene, Konfiguration, Asset Management)
- Daten (Vertraulichkeit, Backup etc.)

Um Cyber-Angriffen stand zu halten braucht es mehr als nur Technologie.

Agenda

- Aktuelle Cyber-Bedrohungslage
- Warum das Gesundheitswesen Cyber-Angriffen ausgesetzt ist
- Feststellungen aus der Praxis: Falsche Umsetzung von Sicherheit
- Cyber-Resilienz im Gesundheitswesen

Warum das Gesundheitswesen Cyber-Angriffen ausgesetzt ist

Anfälligkeitsfaktoren

- **IT-Fachkräftemangel**
- **Die COVID-19-Pandemie**
- **Alte IT-Infrastruktur allgemein**
- **Grosse Mengen personenbezogener Daten**
- **Die Einführung von Clouds**
- **Komplexität der IT-Systeme**
- **Vernetzte Geräte**, zu denen auch viele ältere medizinische Geräte in Krankenhäusern gehören, wie MRT-Scanner und Röntgengeräte. Mit der Verbindungsfähigkeit dieser Geräte geht ein Risiko von Angriffen aus der Ferne einher. Viele dieser Geräte sind zu essenziell, um sie für Patches offline zu nehmen oder haben ihre Supportfrist bereits überschritten.
- **IoT-Geräte,** die sich zunehmender Beliebtheit erfreuen, beispielsweise für die Ausgabe von Medikamenten und die Überwachung der Vitalwerte von Patienten. Viele dieser Geräte sind nicht gepatcht und nur mit den werkseitig voreingestellten Passwörtern geschützt, was sie anfällig für Angriffe macht.
- **Professionelle Cyber-Kriminelle**, die Gesundheitsorganisationen zunehmend als leichtes Ziel sehen, weil sie mit hohen Patientenzahlen von COVID-19 zu kämpfen haben. Patientendaten, die hochsensible Informationen und finanzielle Details enthalten, sind eine lukrative Ware für Cyber-Kriminelle. Ausserdem ist es wahrscheinlicher, dass Ransomware eine Zahlung erzwingt, weil es sich Krankenhäuser nicht leisten können, lange offline zu sein. In Forschungskrankenhäusern können auch hochsensible Informationen über bevorstehende Behandlungen gespeichert sein.

Agenda

- Aktuelle Cyber-Bedrohungslage
- Warum das Gesundheitswesen Cyber-Angriffen ausgesetzt ist
- Feststellungen aus der Praxis: Falsche Umsetzung von Sicherheit
- Cyber-Resilienz im Gesundheitswesen

Falsche Umsetzung von Sicherheit

Feststellungen aus der Praxis

Neue Vorgehensweisen mit grosser Auswirkung

- Attacke über IT Supply Chain
- Gestohlene Credentials
- Schnelle Verbreitung
- Destruktives Vorgehen

Gefordert ist eine Kombination aus präventiven / reaktiven Massnahmen

Erkennung des Angriffs & Backup-Verfügbarkeit

- Angriff wurde zu spät erkannt
- Online Backups oder Backup-Infrastruktur waren nicht verfügbar

Detektion und Response sind Schlüsselfaktoren
Nutzung von Off-site Backups / Dokumenten

Kommunikationswege

- SaaS-Software oftmals nicht betroffen; aber Active Directory & Federation nicht verfügbar falls On-Premise

Nutzung von Mobiltelefon, Text Messaging, WhatsApp, Twitter, etc.

Cyber wird als «IT-Problem» gesehen; Auswirkungen betreffen aber alle Geschäftsbereiche

Agenda

- Aktuelle Cyber-Bedrohungslage
- Warum das Gesundheitswesen Cyber-Angriffen ausgesetzt ist
- Feststellungen aus der Praxis: Falsche Umsetzung von Sicherheit
- Cyber-Resilienz im Gesundheitswesen

Cyber-Resilienz im Gesundheitswesen

Das NIST-Modell

Massnahmen über alle Cyber-Resilienzbereiche hinweg:

- **Identify:** Umfeld, Assets, Risiken, Governance
- **Protect:** Schutz der Daten, Benutzer-Accounts, Sicherheits-Tools und –Architektur
- **Detect:** Unregelmässigkeiten/ Gefahren erkennen, Monitoring, Verwundbarkeit der eigenen Umgebung
- **Respond:** auf Gefahren reagieren, Kommunikation
- **Recover:** Disaster Recovery Planung, Verbesserungen

Cyber-Resilienz im Gesundheitswesen

Kernelemente

Präventive IT-Security-Massnahmen

- Kritische Security Updates
- Isolation von nicht-unterstützten OS-Versionen
- IT Supply Chain Security
- Systemhärtung

Schutz der Identität

- Local-Admin-Passwort-Lösungen (LAR-Lösungen)
- Trennung von privilegierten Accounts
- Multi Factor Authentication

Erkennung und Reaktion

- Einführung von effizienten/effektiven Detektionsmassnahmen
- Security-Incident-Response-Prozesse
- Echtzeitschutz von Clients (z.B. automatisierte Response, XDR)

Business Continuity

- Krisenmanagement
- Regelmässiges Testen des End-to-End-Prozesses
- Business-Impact-Analysen durchführen
- Cloud-Lösungen für Recovery-Lösungen

Cyber-Resilienz im Gesundheitswesen

Goldene Regeln

- Verschaffen Sie sich einen **Überblick über die Angriffsfläche**, einschliesslich aller IT-Ressourcen, deren Patch-Status und Konfiguration. Eine regelmässig aktualisierte CMDB (Configuration Management Database) ist hier nützlich, um das Inventar zu katalogisieren.
- Stellen Sie ausserdem sicher, dass diese **Anlagen korrekt konfiguriert** und über kontinuierliche, risikobasierte Patch-Management-Programme **gepatcht** sind.
- Setzen Sie sich mit **Risiken in der Lieferkette** durch regelmässige Audits und Überwachung auseinander.
- Bauen Sie eine **starke Verteidigungslinie** gegen Phishing auf, indem Sie die Benutzer in Ihrem Netzwerk besser schulen.
- Implementieren Sie **Identitäts- und Zugriffsmanagement** mit Multi-Faktor-Authentifizierung (MFA) überall und richten ein Least-Privilege-Prinzip für den Zugriff ein.
- Erwägen Sie den Schutz Ihrer Netzwerke nach dem **Zero-Trust-Ansatz**
- Sammeln und Analysieren Sie **Telemetriedaten der Sicherheitstools** in der gesamten Umgebung zur schnellen Erkennung von und Reaktion auf Vorfälle.

Danke für Ihre Aufmerksamkeit

Cen Magjuni
Consultant BCM & Krisenmanagement

M +41 76 576 59 57
cen.magjuni@aveniq.ch | aveniq.ch