Sustainable Cyber Resilience im Gesundheitssektor:

Gesundheitsversorgung, Krankenhäuser und Notfalldienste

Whitepaper

Greenbone Networks GmbH
Neumarkt 12
49074 Osnabrück

www.greenbone.net

Greenbone
Sustainable Resilience

09/2018

Management Summary

Medizinische Einrichtungen zählen zu den kritischen Infrastrukturen und sind ein attraktives Ziel für Hacker. Um für angemessenen Schutz zu sorgen, reicht es nicht mehr aus, reaktive Maßnahmen zu ergreifen. Stattdessen müssen Unternehmen einen Zustand der Sustainable Cyber Resilience anstreben: der nachhaltigen Widerstandsfähigkeit. Dabei handelt es sich um ein umfassendes Konzept, das eher strategisch als technologisch ausgerichtet ist und einen Schritt weiter geht als IT Security. Sustainable Cyber Resilience sorgt zum einen dafür, Angriffsflächen zu verringern. Zum anderen stellt sie sicher, dass Unternehmen ihren Betrieb auch im Falle eines Angriffs aufrechterhalten und ihre angestrebten Geschäftsziele erreichen können – unter Berücksichtigung der Wirtschaftlichkeit. Dieses Whitepaper zeigt, warum Sustainable Cyber Resilience für den Gesundheitssektor so wichtig ist, was sie bedeutet und wie sie sich mithilfe von Vulnerability Management umsetzen lässt.

Inhalte

Einleitung

Sustainable Cyber Resilience ist für Unternehmen aller Branchen wichtig. Unverzichtbar ist sie aber im Bereich der kritischen Infrastrukturen (KRITIS). Darunter fallen laut Definition der Bundesregierung „Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden." KRITIS-Organisationen müssen sich daher besonders gut gegen Cyberangriffe schützen – das schreibt der Gesetzgeber vor. Die EU begann bereits 2006 mit dem European Programme for Critical Infrastructure Protection (EPCIP) und erweiterte und ergänzte dieses in den folgenden Jahren. Mitgliedsstaaten setzen die EU-NIS-Direktive in nationales Recht um, Deutschland beispielsweise mit dem IT-Sicherheitsgesetz (IT-SIG). Große Wirtschaftsnationen haben bereits Regulierungsinstanzen entwickelt. In den USA ist dies zum Beispiel das US National Institute of Standards and Technology und in Deutschland das Bundesamt für Sicherheit in der Informationstechnik (BSI).

In Deutschland sind die kritischen Infrastrukturen in 9 Sektoren eingeteilt. Einer davon ist Gesundheit. Unternehmen und Organisationen im Gesundheitssektor zählen laut einer Studie des Ponemom Instituts zu den am häufigsten von Cyber-Angriffen betroffenen Branchen. Für Hacker sind sie besonders attraktiv, denn sie finden hier eine Fülle an sensiblen Patientendaten, die sie teuer verkaufen können. So verzeichnete der Gesundheitssektor 2017 im Branchenvergleich die höchsten Kosten pro gestohlenem Datensatz. Datenschutzverletzungen können teuer werden, gerade auch im Hinblick auf die neue europäische Datenschutz-Grundverordnung (DSGVO), die seit 25. Mai 2018 für alle EU-Mitgliedsstaaten verbindlich gilt. Doch bei Cyber-Angriffen auf Krankenhäuser, Notfalldienste & Co. steht noch viel mehr auf dem Spiel. Denn hier geht es um die Gesundheit von Patienten und um Menschenleben. Durch die zunehmende Digitalisierung und Vernetzung steigt die Gefahr, dass auch medizinische Systeme von Hackern kompromittiert werden. Cyber-Kriminelle könnten zum Beispiel Steuerungsinformationen oder erzeugte Daten blockieren, beziehungsweise verändern und dadurch die Funktion von Geräten beeinträchtigen.

Beispiele für Cyber-Attacken auf medizinische Einrichtungen

In den vergangenen Jahren gab es weltweit bereits zahlreiche Angriffe auf Gesundheitseinrichtungen. Sie geben einen Vorgeschmack darauf, was noch kommen wird. Denn Cyber-Kriminelle sind heute gut organisiert und stimmen ihre Attacken gezielt auf ihre Opfer ab. Es hat sich geradezu eine kommerzielle, kriminelle Branche entwickelt, die versucht, mit Hacker-Angriffen möglichst großen Profit zu erzielen. Prominentestes Beispiel war die WannaCry-Welle im Mai 2017, die besonders den National Health Service (NHS) in Großbritannien traf. Die Ransomware verschlüsselte Daten auf zahlreichen Computern der britischen Gesundheitsbehörde und machte sie so funktionsunfähig. Dabei nutzte sie eine Sicherheitslücke in Windows-Systemen aus. Insgesamt waren 81 der 236 NHS Trusts betroffen. 6.912 Termine mussten verschoben werden, darunter auch zahlreiche Operationen.

In den USA drang der Krypto-Trojaner Samsam im Januar 2018 in das Netzwerk des Hancock Health Krankenhauses im Bundesstaat Indiana ein und infizierte einen Teil der IT-Systeme der Klinik. Er nutzte einen Exploit im Remote Desktop Protocol (RDP) aus. Das Krankenhaus zahlte den Erpressern 60.000 US-Dollar, um seine Systeme schnell wieder funktionsfähig zu machen. Auch in Deutschland gab es schon Cyber-Angriffe auf Krankenhäuser. 2016 wurden das Klinikum Arnsberg und das Lukas Krankenhaus in Neuss Opfer von Ransomware-Attacken. Beide konnten ihre Systeme zwar ohne Lösegeldzahlung wieder betriebsfähig machen. Das Lukas Krankenhaus hat der Kampf gegen den Erpressungs-Trojaner Locky jedoch rund eine Million Euro gekostet.

Ein bedeutender Fall von Datendiebstahl im Gesundheitssektor ereignete sich 2015 bei Anthem Inc, dem größten Krankenversicherungsunternehmen in den USA. Über eine Phishing-Attacke konnten sich Hacker Zugang zum Netzwerk verschaffen und personenbezogene Daten von rund 79 Millionen Versicherten erschleichen, darunter Name, Adresse, Einkommensinformationen, Sozialversicherungsnummer und Krankenversicherungsnummer. 2017 erklärte sich Anthem in einem Gerichtsverfahren bereit, Schadensersatz in Höhe von 115 Millionen US-Dollar an die Betroffenen zu zahlen.

Ein Fall von Datenklau im südostasiatischen Stadtstaat Singapur zeigt zudem deutlich, welche übergreifenden Folgen beim Verlust sensibler Patienteninformationen drohen. So beschafften sich Kriminelle die Datensätze von Patienten, die zwischen Mai 2015 und Juli 2018 eine Klinik besucht hatten. Besonders brisant: Die Hacker hatten es laut den Ermittlern explizit auf Medikationsinformationen des Ministerpräsidenten Lee Hsien Loong abgesehen. Dringen diese sensiblen Informationen eines wichtigen politischen Amtsträgers an die Öffentlichkeit, sind die Folgen für das staatliche Gemeinwesen nicht absehbar.

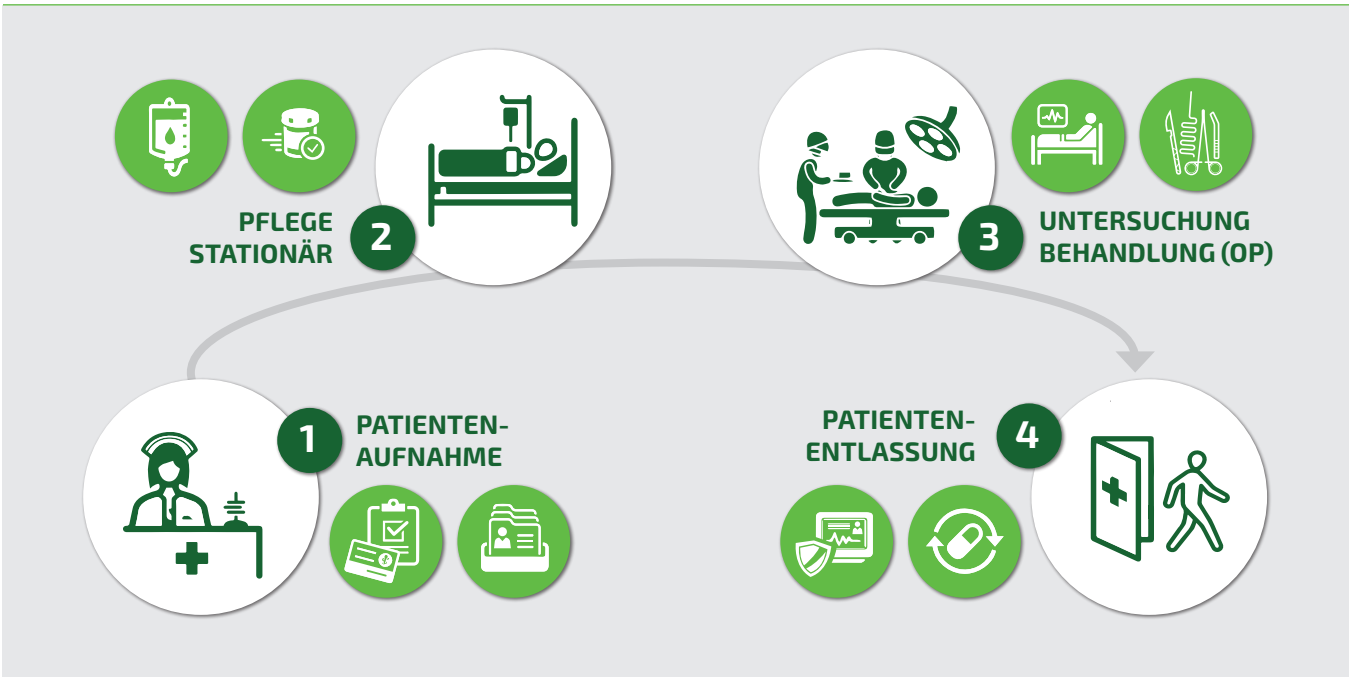
IT-Systeme und Prozesse in Krankenhäusern

Als ein Beispiel für IT-gestützte Abläufe in einem Krankenhaus nutzt die Grafik unten die Betreuung eines Patienten. Schon bei der Patientenaufnahme (1) ist die Erfassung der entsprechenden Daten (zum Beispiel zu Allergien, Unverträglichkeiten, Spenderausweis, chronischen Erkrankungen) wichtig, damit diese später im Verlauf des Aufenthalts verfügbar und korrekt sind. Denn das Pflegepersonal (2) ist unter anderem bei der Medikamentengabe darauf angewiesen (Versorgung durch die Krankenhausapotheke). Hierbei erleichtern außerdem IP-fähige Überwachungs- oder Infusionssysteme die Pflege, bieten gleichzeitig aber auch mehr Angriffsfläche. Resultate vorheriger Behandlungen (3) oder aktuelle Untersuchungsergebnisse, wie etwa digitale Röntgenbilder, müssen dem richtigen Patienten zugeordnet sein. Im Falle einer Operation sollte zudem auch die Sterilisation des OP-Bestecks dokumentiert werden. Schließlich kommt es bei der Entlassung des Patienten (4) auf die vollständige und korrekte Aktualisierung der Behandlungsinformationen und der weiteren Medikation an.

Um die IT in Krankenhäusern und anderen Gesundheitseinrichtungen gegen Cyber-Angriffe zu schützen und Schaden zu minimieren, ist es zunächst wichtig, sich einen Überblick über die eingesetzten Systeme zu verschaffen. Zu berücksichtigen ist sowohl die Unternehmens-IT als auch die medizinische IT.

Zu den gängigen Systemen und Anwendungen im medizinischen Umfeld gehören zum Beispiel Patienten-Management-Systeme (PMS) für die Aufnahme und Administration. In ihnen werden sensible Patientendaten gespeichert, die unter die DSGVO fallen. Krankenhausinformationssysteme (KIS) unterstützen administrative Prozesse in der Klinik, etwa in der Abrechnung, im Controlling, dem Auftragsmanagement oder der Pflegedokumentation. In der Radiologie kommen Radiologie-Informationssysteme (RIS) zum Einsatz. Teilweise sind sie bereits im PMS integriert. Sie steuern alle Abläufe in der Abteilung, erzeugen eine Liste zur Abarbeitung von Röntgenaufträgen und sorgen für

Digitale Systeme und Abläufe im Krankenhaus



eine optimale Auslastung der Geräte. Das RIS arbeitet mit dem PACS zusammen, dem digitalen Bilddatenarchivierungs- und Kommunikationssystem. Dessen Aufgabe besteht darin, alle anfallenden Bilddaten und Befunde zu managen. Hinzu kommen Monitoring-Systeme auf Intensivstationen, Krankenhaus-Apotheken, die mit den einzelnen Stationen und dem PMS vernetzt sind sowie Systeme von Sterilisierungsdiensten, um Abläufe zu protokollieren. Nicht vergessen sollte man auch Systeme der Gebäude-Technik wie die zentralen Klimaanlagen. Auch hier könnten Hacker durch eine Manipulation den Krankenhausbetrieb erheblich beeinträchtigen.

Zunehmend wird die Krankenhaus-IT durch mobile Endgeräte ergänzt. Ärzte nutzen zum Beispiel iPads bei der Visite, um digitale Patientenakten zu öffnen und direkt am Krankenbett Bilder oder andere Daten abzurufen. Zudem kommt häufig Kollaborations-Software zum Einsatz, die die Zusammenarbeit erleichtert und Prozesse beschleunigt. So können verschiedene Behandler ortsunabhängig, schnell und unkompliziert miteinander kommunizieren.

Besondere Herausforderungen für Resilience im Gesundheitssektor

Organisationen und Unternehmen im Gesundheitssektor stehen bei der Etablierung von Sustainable Cyber Resilience vor einigen Herausforderungen. So sorgt zum Beispiel die Bandbreite an Systemen, Appliances, Betriebssystemen, Anwendungen und vernetzten medizinischen Geräten sowie der umfangreiche und äußerst komplexe Bestand an Legacy-Systemen und brandneuen Geräten für Sicherheitslücken und Unzulänglichkeiten. Verbunden mit Governance- und Regulierungsrichtlinien, die zu widersprüchlichen Handlungen auffordern, entsteht ein wahres Chaos. Wenn die IT-Verantwortlichen diese Sachlage ignorieren, wird unweigerlich jede IT-Sicherheitsarchitektur ineffizient und angreifbar und damit zu einem Bremsfaktor für die gesamte Organisation.

Ein weiterer Gefahrenherd besteht in dem routinemäßigen und automatisierten Informationsaustausch zwischen Mensch und Maschine sowie zwischen unterschiedlichen Systemen. Diese sogenannten Converged Technologies erzeugen einen Zustand, in dem die Angriffsfläche der gesamten Infrastruktur vergrößert wird. Viele medizinischen Geräte haben heute Protokolle wie TCP/IP für die Internetkommunikation integriert und verfügen über Embedded-Versionen von MS Windows oder Linux. Das macht sie genauso angreifbar wie einen Bürocomputer. Durch die zunehmende Vernetzung können sich Angriffe auf medizinische Geräte auch auf die Unternehmens-IT auswirken – und umgekehrt.

Zudem muss Resilience im Gesundheitssektor neben Security, also der technischen Absicherung der Systeme gegen Angreifer, auch Safety umfassen. Letztere bezeichnet die Sicherheit der Geräte, sodass Mitarbeiter oder Patienten sich bei ihrem Betrieb nicht verletzen.

Vulnerability Management als wichtiger Baustein für Sustainable Cyber Resilience

Resilienz ist ein kontinuierlicher Prozess. Er verstärkt die Fähigkeiten eines Unternehmens, einer Attacke zu widerstehen, und versetzt es in die Lage, auch während eines Angriffs zu funktionieren. Um dies zu erreichen, ist es wichtig, die Angriffsfläche zu reduzieren und so die Basis zu stabilisieren. Das bedeutet, Schwachstellen zu identifizieren, die von einem Angreifer ausgenutzt werden könnten. Letztlich heißt es, dem Angreifer einen Schritt voraus zu sein.

Das Schwachstellenmanagement von Greenbone funktioniert mit dem Greenbone Security Manager (GSM) und ist dafür gedacht, Resilience durch einen kontinuierlichen Prozess nachhaltig zu etablieren. Dieser besteht aus den folgenden, größtenteils automatisierten Schritten:

Prepare

Im ersten Schritt geht es darum, den Kontext zu IT-Sicherheits-Policies, Risikobewertungen, Unternehmensprozessen und unternehmenskritischen Systemen herzustellen. Was will ich wie und wie intensiv schützen? Wie viel Risiko bin ich bereit zuzulassen? In Konfigurationsrichtlinien legen die IT-Verantwortlichen fest, was im Rahmen der Sicherheitsvorgaben erlaubt ist. Diese Richtlinien können dann mit einer technischen Kontrolle im GSM verknüpft werden. Hinzu kommen Informationen rund um den Security Workflow und die Verantwortlichkeiten. Wer muss informiert sein? Wer entscheidet, ob eine Schwachstelle behoben werden soll oder darf? Wer behebt sie?

Identify

Jetzt folgt die Analyse der Ist-Situation. Ein Vulnerability Scan stellt fest, welche Schwachstellen die Infrastruktur aktuell aufweist und wo sie von Konfigurationsvorgaben abweicht. Dabei muss sichergestellt werden, dass die Datenbank mit den Schwachstelleninformationen auf dem neuesten Stand ist. Außerdem wird identifiziert, wo genau sich die Schwachstelle oder Abweichung von der Norm befindet, und hinterfragt, wie belastbar die gefundenen Ergebnisse sind. Das dient dazu, False Positives und False Negatives zu vermeiden.

Greenbone hat dafür das Feature QoD „Quality of Detection“ eingebaut. Es nennt einen Prozentwert, mit welcher Wahrscheinlichkeit die Schwachstelle tatsächlich existiert.

Classify

Die gesammelten Informationen werden jetzt nach unterschiedlichen Kriterien eingeteilt, die das Unternehmen individuell festlegen kann – zum Beispiel wo ein System physikalisch steht, zu welcher Abteilung es gehört, in welchem Netzsegment es sich befindet und welche Funktion es im Unternehmen erfüllt. Diese Einteilung ist unabhängig von der Kritikalität der Schwachstelle. Classify macht nichts anderes, als die Funde anhand der vorhandenen Merkmale zu gruppieren. Wichtig hierbei ist, dass eine solche Gruppierung im Sinne der Automatisierung in Regeln abgebildet werden kann.

Prioritize

Jetzt wird priorisiert, was auf Basis der Ziele aus dem ersten Schritt „Prepare“ mit den gefundenen Schwachstellen aus dem Schritt „Identify“ anhand der Einteilungen von „Classify“ am wichtigsten und damit als Erstes zu tun ist. Welcher Fund hat die größte Auswirkung und muss zuerst bearbeitet werden?

Widerstandsfähigkeit durch den Schwachstellen-Management-Prozess

Assign, Mitigate & Remediate

Die technischen Erkenntnisse müssen in einem Arbeitsprozess münden, der zur Schließung der Schwachstelle führt. Ein Vulnerability-Management-Prozess sollte regeln, wer wann welche Informationen zu entdeckten Schwachstellen bekommt, wer für welche Schritte verantwortlich ist und welche Mittel und Wege zur Verfügung stehen. Das Vulnerability-Management-System sollte hier so viele Informationen wie nur möglich mitliefern. Die Handlung kann auch über den Austausch mit anderen Workflow Tools initiiert werden, zum Beispiel einem ISMS, einem Ticket-System für Helpdesks oder einem SIEM-System zur weiteren Korrelation von Security Events beziehungsweise Incidents.

Store & Repeat, Improve

Die letzten Schritte dienen der Auditierbarkeit des Systems nach ISO 27000 sowie der Verbesserung, Veränderung und Anpassung. Store & Repeat protokolliert wichtige Informationen, zum Beispiel, wann eine Schwachstelle zum ersten Mal gefunden wurde, wann sie gemeldet wurde und wie lange es gedauert hat, sie zu beheben. Dies hilft bei der Analyse von Sicherheitsvorfällen. „Improve“ ist der Übergang zu einem erneuten Durchlauf des Vulnerability-Management-Prozesses, der wieder mit „Prepare“ beginnt. Jetzt können Sicherheitsverantwortliche die Zielsetzung verfeinern, verschärften oder an veränderte Policies anpassen. Schwachstellenmanagement ist kein statisches System, sondern ein dynamischer Prozess, bleibt aber immer automatisierbar.

Grenzen von Vulnerability Management

Vulnerability Management ist ein wichtiger Baustein, um Sustainable Cyber Resilience zu erreichen. Es ist jedoch nur ein Element in einer umfassenden Gesamtarchitektur. Für nachhaltige Cyber Security und Widerstandsfähigkeit sind noch viele weitere Faktoren zu berücksichtigen, die ineinandergreifen müssen. Neben der Absicherung der Systeme gegen Hackerangriffe dürfen Unternehmen auch die physische Sicherheit nicht vernachlässigen. Zudem spielen organisatorische Maßnahmen eine wichtige Rolle. Unternehmen müssen genau festlegen und dokumentieren, wie Security-Prozesse aussehen und wer welche Aufgaben und Verantwortung übernimmt. Außerdem dürfen Unternehmen den Faktor Mensch nicht vergessen. Eine wichtige Präventionsmaßnahme sind nach wie vor Schulungen zur Sensibilisierung für IT-Risiken. Denn viele Mitarbeiter sind sich nicht bewusst, wie gefährlich Fehlverhalten oder Unachtsamkeit sein kann.

Nicht umsonst schreiben zahlreiche Richtlinien und Gesetze Schwachstellen-Scans und Risikobewertung vor. So erwartet zum Beispiel die EU-DSGVO ein implementiertes Schwachstellenmanagement. Auch für eine ISO 27001-Zertifzierung ist dies Voraussetzung. Die Fähigkeit, Schwachstellen zeitnah aufzufinden, zu priorisieren und zu beseitigen, ermöglicht es Unternehmen, ihre IT-Systeme kontinuierlich sicherer zu machen und die Angriffsfläche zu reduzieren. Das ist ein laufender Prozess, der nie abgeschlossen sein darf. Für Organisationen, die unter die KRITIS fallen, ist Vulnerability Management Pflicht.

Über Greenbone

Greenbone Networks wurde 2008 von Netzwerksicherheits- und Open-Source-Experten gegründet. Hauptsitz des international agierenden Privatunternehmens ist Osnabrück. Die Greenbone Security Manager (GSM) basieren auf Open Source Software. Sie analysieren IT-Netzwerke auf Schwachstellen und liefern Sicherheitsberichte sowie Hinweise zur Behebung, bevor Angreifer die Sicherheitslücken ausnutzen können. Bestandteil der Lösungen ist ein tägliches, automatisches Security Update. Es bündelt Prozeduren zur Erkennung von aktuellen Sicherheitsproblemen und überwacht Desktop-PCs, Server, Anwendungen und intelligente Komponenten wie etwa Router oder VoIP-Geräte. Die Greenbone-Lösung ist inzwischen eine wichtige Sicherheitskomponente in über 30.000 professionellen Installationen und Integrationen quer durch alle Branchen und Unternehmensgrößen. Die Greenbone Vulnerability Management Software wurde bereits mehr als 2,5 Millionen Mal heruntergeladen.

Weitere Informationen unter **greenbone.net**
Folgen Sie uns auf Twitter: **twitter.com/GreenboneNet**