Das Problem mit der IT-Sicherheit im Gesundheitswesen

Die Probleme, die im Zusammenhang mit IT-Sicherheit im Gesundheitswesen auftreten, geben dem Personal und den Aufsichtsbehörden zunehmend Anlass zur Besorgnis. In den letzten sechs Monaten haben das Bundesamt für Sicherheit in der Informationstechnik (BSI), das Innenministerium und andere Sicherheitsorganisationen regelmäßig Warnmeldungen über erhöhte Bedrohungsstufen für Gesundheitssysteme herausgegeben. Eine Vielzahl von Gesundheitseinrichtungen ist Ransomware-Angriffen zum Opfer gefallen, die die Patientensicherheit gefährden und enorme finanzielle Schäden anrichten.

Doch warum kommt es in diesem Bereich zu einer Zunahme der Angriffe? Gibt es etwas im Gesundheitswesen, das IT-Sicherheit besonders schwierig macht? Ja. Das gibt es!

Safety vs. Security

Die Begriffe Ausfallsicherheit und Security (Safety und Security) sind eng miteinander verbunden, beschreiben jedoch unterschiedliche Konzepte. Während es bei Ausfallsicherheit (Safety) um den Schutz vor zufälligen Ausfällen und Fehlern geht, beschreibt der Begriff Security den Schutz vor bösartigen Angriffen. Diese beiden Konzepte sind in wenigen Bereiche so eng miteinander verknüpft wie im Gesundheitswesen. Rechnet man noch dazu, dass die im Gesundheitssektor verarbeiteten Daten sehr hohen Datenschutzanforderungen unterliegen, wird klar, welche Fülle an Herausforderungen es zu meistern gilt. Dabei sind perfekte Lösungen selten, oft muss man sich auf unvollkommene Kompromisse einlassen.

Ein konkretes Beispiel: Laut Datenschutzbestimmungen des Health Insurance Portability and Accountability Act (HIPAA) und der Datenschutz-Grundverordnung (DSGVO) sind medizinische Daten hochsensible Informationen, die sorgfältig geschützt werden müssen. Folglich sehen die Security-Anforderungen vor, dass nur autorisierte und sicher authentifizierte Personen auf

Datenbanken, in denen Krankenakten abgespeichert sind, zugreifen dürfen. Aus der Safety-Perspektive allerdings kann der schnelle Zugriff auf medizinische Daten eine Frage von Leben oder Tod sein.
In einem medizinischen Notfall bleibt keine Zeit für das Entsperren von Bildschirmen oder das Herausssuchen von Passwörtern.

In der Praxis reichen die Kompromisse zur Lösung dieses Security-Safety-Konflikts von aufwändigen „Break-Glass-Systemen", die im Notfall das Umgehen der normalen Zugangskontrolle ermöglichen, bis hin zu pragmatischen Lösungen wie, die Computermaus in eine „Blutbeutelwippe" zu legen, in der sie hin- und herbewegt wird, um so die Aktivierung der Bildschirmsperre zu verhindern.

Die drei Aspekte des Systems

Erschwerend kommt die einzigartige dreigeteilte Struktur der IT-Systeme im Gesundheitswesen hinzu. Natürlich verfügen alle Gesundheitsdienstleister über Büroverwaltungssysteme für Aufgaben wie E-Mails und Tabellenkalkulation. Diese Art der der IT ist in allen großen Organisationen anzutreffen. Zwar gibt es auch hier offene Fragen, was den Schutz dieser Systeme angeht, aber es existieren zumindest umfangreiche gemeinsame Kenntnisse und klare Praxisanweisungen.

Zweitens verfügen die größeren Institutionen im Gesundheitswesen über eine Vielzahl von vernetzten medizinischen Geräten. Diese reichen von Infusionspumpen und Insulinmonitoren bis hin zu hochmodernen MRT-Scannern, die alle aus Gründen der Überwachung, des Datenaustauschs und des Fernzugriffs an ein Computernetzwerk angeschlossen sind.
Diese Geräte müssen strenge Safety-Anforderungen erfüllen, die häufig mit den grundlegenden IT-Security-Praktiken, wie regelmäßige Software-Updates, unvereinbar sind. Tatsächlich werden auf vielen in medizinische Geräte integrierten Computern, Betriebssysteme ausgeführt, die vom Hersteller gar nicht mehr unterstützt werden. Würde ein IT-Sicherheitsingenieur verlangen, diese unsicheren Systeme in vollständig isolierte Netzwerke zu verlegen, würde er scheitern, da die Mitarbeiter von ihren Büroarbeitsplätzen aus Zugriff auf medizinische Daten benötigen. Darüber hinaus haben viele Krankenhäuser und Kliniken Verträge mit spezialisierten Anbietern, wie z. B. Teleradiologie-Unternehmen, die in verschiedenen Zeitzonen arbeiten, um die Abdeckung auch außerhalb der eigenen Arbeitszeiten zu ermöglichen. Die MRT-Scans müssen folglich jederzeit an Spezialisten auf der anderen Seite der Welt übertragen werden können.

Und schließlich gibt es drittens außer Verwaltungssystemen und medizinischen Geräten ein weiteres, häufig vergessenes System: das Supervisory Control and Data Acquisition (SCADA)-System (Überwachung, Steuerung und Datenerfassung), das die Infrastruktur des Krankenhauses oder der Klinik überwacht und steuert.
Alle von uns als selbstverständlich hingenommenen Versorgungsleistungen, wie Heizung, Lüftung, Strom, Beleuchtung und Wasserversorgung werden von speziellen Computersystemen gesteuert. Das Krankenhaus oder die Klinik ist für den ordnungsgemäßen Betrieb dringend auf solche Systeme angewiesen, die jedoch bei der IT-Security kaum Beachtung finden. Hier müssen zahlreiche realistische und leider auch erschreckende Szenarien berücksichtigt werden.

Wenn ein Ransomware-Angreifer herausfindet, wie er die technischen Arbeitsstationen für die Heizungs- und Lüftungssysteme angreifen kann, kann er beispielsweise die Belüftung der Operationssäle und die Arbeitsstationen abschalten und damit den Abbruch aller größeren Operationen in einem Krankenhaus herbeiführen. Ein Angreifer, der sich Zugang zu den Steueranlagen der Energieversorgung verschafft, kann die Primär- und Reservestromversorgung deaktivieren und so innerhalb von wenigen Minuten lebensbedrohliche Situationen herbeiführen. Die Liste der Alptraumszenarien ließe sich leicht fortsetzen.

Eine Fülle von Vorschriften

Während IT-Systeme im Gesundheitssektor per se schon sehr komplex sind, ist das regulatorische Umfeld, in dem sie existieren, ein wahres Labyrinth. Sehen wir uns nur mal ein typisches System zur Verteilung von medizinischem Sauerstoff an, bei dem Gas in Druckleitungen durch das Krankenhaus geleitet wird. In einem normalen Krankenhaus-Setting trägt das Facility-Personal die Verantwortung für die physische Verrohrung, während das Gas selbst ein Medizinprodukt ist, das von zertifiziertem Pflege- oder ärztlichem Personal verantwortet wird. Hinzu kommen branchenweit geltende Sicherheitsvorschriften für den Umgang mit Druckgasen, die die Einrichtung einer internen Gassicherheitsorganisation vorschreiben. Es herrscht absolut keine Klarheit darüber, wer von den beteiligten Akteuren die endgültige Verantwortung für die IT-Sicherheit des Gasverteilungssystems trägt.

Angesichts dieser unklaren Verantwortungsketten steigt das Risiko dafür, dass Probleme unentdeckt bleiben, und es wird schwieriger, eine einheitliche IT-Security-Politik durchzusetzen.

Ransomware, der Albtraum

Angesichts der oben geschilderten Punkte dürfte es keine Überraschung sein, dass viele Gesundheitseinrichtungen ziemlich durchlässige Ziele für entschlossene Angreifer darstellen. Die meisten wollen dabei finanziellen Gewinn aus ihren Angriffen schlagen. Zwar hatten gestohlene Krankenakten schon immer einen gewissen Wert auf dem Markt, doch hat in den letzten Jahren mit dem Aufkommen groß angelegter Ransomware-Operationen die Bedrohung für die IT-Security im Gesundheitswesen rasant zugenommen.
Ein normales, von einer Ransomware-Attacke betroffenes Unternehmen, kann sich einfach weigern (aus einem gewissen Gemeinschaftssinn heraus oder aus reiner Bosheit), Lösegeld zu zahlen, was dazu führt, dass Zeit und Aufwand, die der Angreifer in den Angriff gesteckt hat, verloren sind. Eine Gesundheitseinrichtung dagegen steht unter dem enormen Druck, ihre Systeme wiederherzustellen, da die Patientensicherheit gefährdet ist. Für ausreichend gewissenlose Angreifer sind Gesundheitseinrichtungen daher ein gutes Ziel, da sie eher bereit sind, auf Forderungen einzugehen.
Dies lässt sich durch die Tatsache untermauern, dass zwar ein großer Teil der Ransomware-Angreifer öffentlich erklärt hat, während der COVID-19-Pandemie keine Gesundheitseinrichtungen anzugreifen, andere Gruppen jedoch ihre Angriffe verstärkt haben, da ein Opfer, das bereits durch die Pandemie unter Druck steht, noch viel mehr bereit ist, Lösegeld zu zahlen. Eine der berüchtigtsten Gruppen ist die russische Ryuk-Bande, die immer wieder in den Warnhinweisen der Behörden auftaucht.

Eine Lösung, ein Königreich für eine Lösung

Leider gibt es keine einfachen Lösungen für die Krise der IT-Sicherheit im Gesundheitswesen, keine magische Blackbox, die man einfach an das Netzwerk anschließen kann, keine Checkliste mit fünf Punkten, die alle Probleme löst. Da liegt der Wunsch nahe, alle IT-Kriminellen einfach hinter Schloss und Riegel zu bringen. Doch viele – oder sogar die meisten – operieren aus Staaten mit unkontrollierbaren Rechtssystemen wie dem Iran oder Russland und sind damit unantastbar.
Die Lösung ist ein langer Weg, bei dem alle Akteure an einem Strang ziehen müssen. Die Gerätehersteller müssen ihre Geräte-Security verbessern, die Strafverfolgungsbehörden die internationale Zusammenarbeit effizient gestalten, und zu guter Letzt müssen die Gesundheitseinrichtungen lernen, wie sie die Security kontinuierlich verbessern können.
Es gibt es zwar keine einfachen Lösungen, doch zumindest einige grundlegende Hinweise zur Verbesserung Ihrer Security.

Dazu gehört vor allem die Erkenntnis, dass man niemals fertig ist. Sie haben es mit hoch motivierten und intelligenten Gegnern zu tun, die sich immer wieder neue Angriffsmöglichkeiten einfallen lassen. Auch wenn die Redensart „Sicherheit ist ein Prozess, kein Produkt" ein Klischee ist, so ist sie dennoch wahr.
Auch sollten Sie nicht vergessen, dass die Verbesserung der Security ausgewogen erfolgen muss. Wenn Sie Ihr gesamtes Budget für die Verbesserung der Security Ihrer medizinischen Geräte ausgeben, laufen Sie Gefahr, dass sich die Kriminellen stattdessen einfach Ihr Büronetzwerk vornehmen werden. Sie können mit Sicherheit davon ausgehen, dass die Angreifer Sie immer an Ihrem wunden Punkt treffen werden.

Last but not least: Bitte vergessen Sie auf keinen Fall die SCADA-Systeme!

Leif Nixon - Sicherheitsexperte bei Sectra Communication

SECTRA
Knowledge and passion