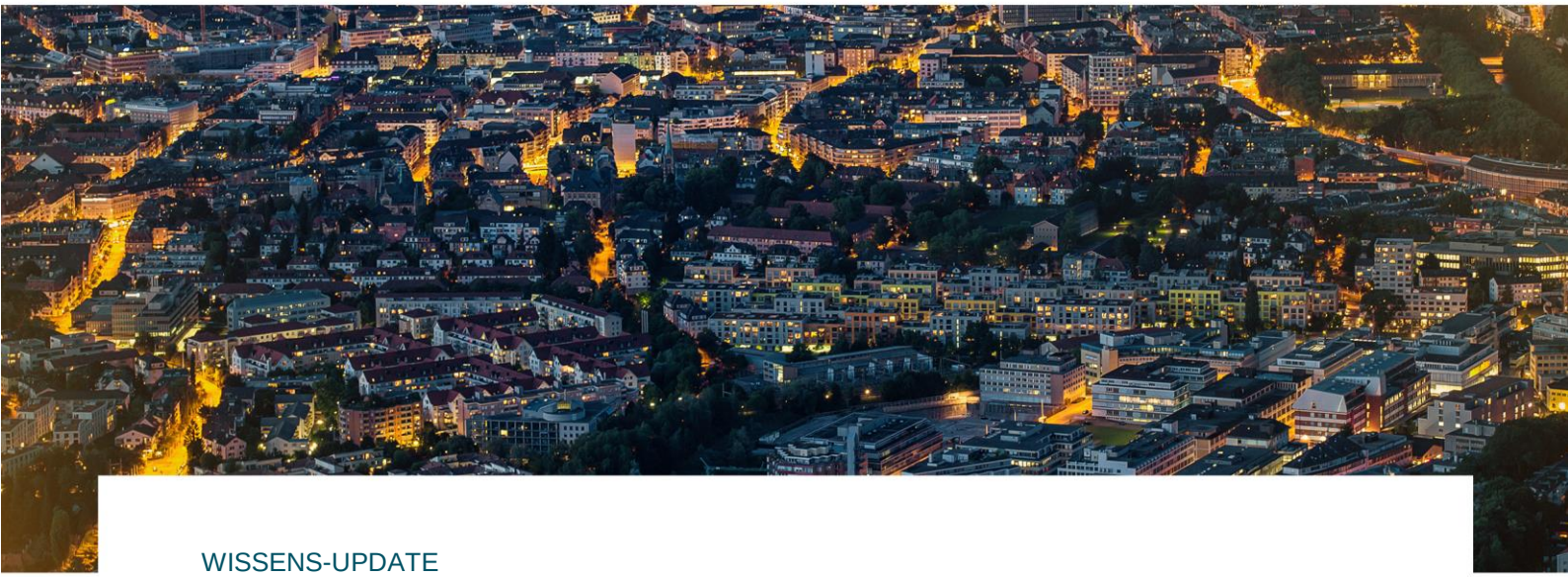
CyOne Security AG
Hinterbergstrasse 18
6312 Steinhausen

Telefon +41 41 748 85 00
info@cyone.ch
cyone.ch



WISSENS-UPDATE

Mehr Vernetzung, mehr Verletzlichkeit – die Medizinaltechnik als Sicherheitsrisiko

Stefan Frank | Security of Things Solutions | Steinhausen, 24. August 2021

Transparenter, effizienter, günstiger: Das Internet der Dinge hat im Bereich der Medizinaltechnik grosse Vorteile – und neue vielfältige Einsatzmöglichkeiten. Wie andere vernetzte Systeme macht sich aber auch das «Spital der Zukunft» zur Zielscheibe von Cyber-Angriffen – wenn essenzielle Sicherheitsüberlegungen vernachlässigt werden.

Die Digitalisierung verändert nicht nur Industrie, Mobilität und Kommunikation – sondern auch die Medizin. Dem Internet der Dinge (IoT) kommt dabei eine zentrale Bedeutung zu. Das IoT vernetzt Sensoren und Geräte untereinander, verbindet sie mit Datenbanken und ermöglicht dank Informations- und Kommunikationstechnologien eine automatisierte, barrierefreie Zusammenarbeit. Die Einsatzmöglichkeiten im Gesundheitswesen sind vielfältig und noch längst nicht ausgeschöpft.
Im Consumer-Bereich bereits heute weit verbreitet sind Fitnesstracker, die Daten aus unserem Alltag aufzeichnen und uns zu gesundheitsfördernden Tätigkeiten animieren sollen. Aus dem Bereich Prävention sind tragbare Messgeräte bekannt, die zum Beispiel Puls, Blutdruck oder Blutzuckerwerte überwachen. Sie erkennen Unregelmässigkeiten, alarmieren und regeln im Fall der Blutzuckerüberwachung die Insulinzufuhr. Sie können mithelfen, schwerwiegende gesundheitliche Folgen zu vermeiden. Um die Messdaten auszuwerten, ist oftmals nur ein Smartphone nötig – für Patientinnen und Patienten bedeutet das mehr Kontrolle, Sicherheit und schlussendlich mehr Lebensqualität.

IoT in Heimen und Spitälern

Auch im klinischen Umfeld – in Gesundheitseinrichtungen wie Heimen und Spitälern – ist die IoT-Technologie bereits im Einsatz. Patienten können mit elektronischen Armbändern eindeutig identifiziert werden; das minimiert die Verwechslungsgefahr und stellt sicher, dass die richtige Person ein bestimmtes Medikament oder die auf sie abgestimmte Behandlung erhält. Das Kantonsspital Baden führt derzeit einen Pilotversuch mit solchen Armbändern durch. Auch medizinische Geräte sind dank Barcode oder Chip mit einer unverwechselbaren ID ausgerüstet. So kann etwa analysiert werden, wie häufig ein bestimmtes Gerät eingesetzt oder wann ein Skalpell desinfiziert wurde. Dank der Vernetzung werden Daten zu Medikation und Behandlung, Bilder von Röntgenaufnahmen oder MRIs sowie allfällige Befunde übertragen und direkt im richtigen elektronischen Patientendossier gespeichert. Im Störungsfall oder bei geplanten Wartungen von Medizinal-Devices ist es nicht mehr zwingend nötig, dass ein Fachspezialist des Geräteherstellers vor Ort ist – die Problembehebung kann über eine entsprechende Wartungsschnittstelle aus der Distanz oder anders gesagt «remote» erfolgen.

Effizienz steigern, Kosten sparen

Die Vorteile der Technologie sind offensichtlich: Die Identifikation von Patienten, Maschinen und Medikamenten sorgt für mehr Sicherheit, weil das Risiko von Fehlern und menschlichem Versagen minimiert wird. Automatisierte Prozesse steigern die Effizienz im Gesundheitswesen und sparen Kosten – Kosten, die künftig aufgrund der Überalterung der Gesellschaft ohnehin steigen dürften. Auch eine Integration von Smarthome-Anwendungen ist denkbar und könnte sich zusätzlich positiv auswirken: mit Sensoren und Kameras, die zum Beispiel den Genesungsprozess aufzeichnen, Stürze älterer Menschen automatisch detektieren oder die Einnahme von Medikamenten über-wachen. Das könnte teure stationäre Spital- oder Heimaufenthalte in vielen Fällen überflüssig machen und somit weitere Kosten einsparen.

Zielscheibe für Cyber-Angriffe

Neben all diesen Vorteilen weist das Internet der Dinge für Gesundheitsinstitutionen und -anwendungen auch Nachteile auf, primär in Sachen Sicherheit. Denn alle vernetzten Systeme können aufgrund ihrer zahlreichen Knotenpunkte zu Zielscheiben für Cyber-Angriffe werden. Gerade die erwähnten Wartungsschnittstellen für den Remote-Zugang sind oftmals kaum gesichert, funktionieren über veraltete Protokolle und sind so ein ideales Einfallstor für Hacker. Der Bund hat die Gefahr erkannt und die Gesundheitsversorgung in seine Strategie zum Schutz kritischer Infrastrukturen aufgenommen. Zwar sei das Gesundheitswesen mit seiner dezentralen Struktur selten in seiner Gesamtheit bedroht, schreibt das Bundesamt für Bevölkerungsschutz in einem Factsheet. Werde ein Spital angegriffen, könnten in der Regel andere Institutionen aushelfen. Allerdings könne auch ein Angriff auf eine einzelne Organisation bereits gravierende Auswirkungen für Patientinnen und Patienten haben.

Diebstahl, Blockierung und Manipulation von Daten

Cyber-Angreifer könnten zum Beispiel vertrauliche Patientendaten stehlen und persönliche Informationen an Versicherungen, Arbeitgeber oder kriminelle Organisationen weitergeben. Sie könnten die hohen Anforderungen bezüglich Daten- und Serviceverfügbarkeit ausnutzen und zum Beispiel mittels Denial-of-Service-Angriff und Cyber-Erpressung hohe Geldforderungen stellen. Weitaus schwerwiegendere und potenziell tödliche Folgen hätte die Manipulation von Daten oder Funktionen:

- wenn in Patientendossiers plötzlich wichtige Angaben fehlen, die einem Arzt Informationen über bestehende Allergien, Unverträglichkeiten oder kontraindizierte Medikamente vorenthalten

- wenn Messresultate von ungeschützten Diagnoseinstrumenten manipuliert werden und so eine falsche Behandlung des Patienten nach sich ziehen
- wenn logistische Prozesse wie die Medikamentenbestellung durch Angriffe lahmgelegt würden
- wenn Reinigungs- und Sterilisationssysteme nicht mehr sauber arbeiteten
- wenn patientennahe Systeme wie Infusionen oder sogar Herzschrittmacher gehackt würden
- oder wenn operationsunterstützende Systeme wie Herz-Lungen-Maschine oder Operationsroboter manipuliert würden

Cyber-Angriffe in den USA und Deutschland

Aus dem Ausland sind bereits Fälle von Cyber-Angriffen oder Meldungen über ungesicherte Anlagen bekannt. In verschiedenen Spitälern in den USA waren beispielsweise Infusionspumpen im Einsatz, die via Krankenhausnetzwerk von Dritten hätten angesteuert und manipuliert werden können. Im schlimmsten Fall hätte Patienten eine Überdosis verabreicht werden können. Die Pumpen werden mittlerweile nicht mehr verwendet. Aus Deutschland ist der Fall eines Desinfektionsgeräts bekannt, das nicht ausreichend gesichert war. 2016 wurden deutsche Spitäler Opfer von Cyber-Attacken, die mit Schadsoftware IT-Systeme lahmgelegt hatten. Die Systeme mussten heruntergefahren, die Kommunikation auf Papier geführt und nicht-dringende Operationen sogar verschoben werden.

Hersteller in der Pflicht

Ein Problem liegt in der Produktsicherheit an sich: Hersteller von Medizinaltechnik stehen unter hohem wirtschaftlichem Druck seitens ihrer Kunden, ihre Devices vernetzbar zu machen. Sie müssen bereits bei der Entwicklung von vernetzten Geräten die Sicherheit in der späteren Anwendungsumgebung berücksichtigen – und das in einem besonders schnelllebigen Marktumfeld. Fachleute sind sich einig: Viele Hersteller haben die neuen technologischen Entwicklungen zu rasch umgesetzt und Sicherheitsüberlegungen in Bezug auf ein vernetztes Einsatzumfeld noch zu wenig Aufmerksamkeit geschenkt. Das kann zu Schwachstellen führen, welche die Handhabung von sensiblen medizinischen Daten oder lebenswichtige medizinische Mess-, Prüf- und Regelungsprozesse gefährden können.

Operationelle und Systemsicherheit

Auch die Sicherheit des IT-Systems, in das ein Medizinal-Device eingebettet ist, spielt eine wichtige Rolle. Spitäler und andere Gesundheitseinrichtungen sind mit der Anforderung konfrontiert, ihre IT-Infrastruktur auf dem neusten Stand zu halten. Dabei werden oft «Best practice»-Ansätze aus der Industrie verfolgt. Es ist aber eine grosse Herausforderung für den Spital-IT-Betreiber, die vorhandene Medizinaltechnik sicher zu integrieren. So muss ein Spital – infolge des Kostendrucks – zusammen mit dem Hersteller einen Weg finden, um bestehende Geräte so zu konfigurieren, dass sie den Ansprüchen der vernetzten Medizin genügen und weiterhin eingesetzt werden können.

Veraltete Software, unsichere Protokolle, falsch konfigurierte Netzwerkdienste, eine unverschlüsselte Datenübertragung oder Software-Updatekanäle können zu Einfallstoren für Cyber-Angreifer werden. Daher empfiehlt es sich, Medizinalgeräte an voneinander getrennten Netzen anzuschliessen, damit sich zum Beispiel Schadsoftware nicht ungebremst ausbreiten kann. Das gilt vor allem für Geräte mit Remote-Zugriff. Auch die operationelle Sicherheit spielt hier eine eminent wichtige Rolle und sollte nicht vernachlässigt werden: Schwache Passwörter, eine zu weitreichende und dadurch nicht kontrollierbare Vergabe von Zugriffsrechten oder Betriebspersonal, das nicht für IT-Sicherheitsaspekte sensibilisiert ist, erhöhen das Risiko von Angriffen zusätzlich. Gerade im Medizinalbereich sei das Bewusstsein für Cyber-Risiken besonders gering, schrieb das Branchenmagazin «Netzwoche» kürzlich.

Beizug von Cyber Security-Experten unumgänglich

Um fatale Folgen zu verhindern, müssen Hersteller und Anwender Massnahmen zur Prävention von Angriffen, zur Detektion und schliesslich auch zur Reaktion auf Cyber-Attacken treffen. Dazu gehören zum Beispiel geschützte Backups, die im Angriffsfall die Wiederherstellung des letzten gesicherten Standes erlauben. Neben der Produktsicherheit spielen starke Authentifizierungsmass-nahmen als eine Präventionsmassnahme eine zentrale Rolle. Um Angriffe schnellstmöglich zu entdecken, können Security Information und Event Management-Technologien eingesetzt werden. Sie erkennen Anomalien in den IT-Aktivitäten und zunehmend auch in den IoT-Verhaltensweisen eines Unternehmens und können dank schneller Reaktionszeiten zur Schadensbegrenzung bei-tragen. Es ist essenziell, dass die gesamte Kette von den Sensoren und der Steuerung über die Datenspeicherung bis hin zur Datenauswertung sicherheitstechnisch berücksichtigt werden. Unter-nehmen, die in der Medizinaltechnik tätig sind, müssen das Thema Cyber-Sicherheit zwingend in ihre Geschäftsstrategie integrieren. In der Umsetzung dieser Sicherheitsmassnahmen ist dabei der Einbezug von Cyber Security-Experten unumgänglich.

CyOne Security ist der kompetente Partner

Bei der Entwicklung von vernetzten Medizinal-Devices wie auch beim Einsatz von bis anhin standalone betriebenen Geräten in einem grösseren IT-Netzwerk bleibt, wie oben beschrieben, die Sicherheit oft auf der Strecke. Deshalb müssen bisherige Sicherheitsansätze grundlegend überdacht werden. Verfügbarkeit, Verhinderung von Zweckentfremdung und Wahrung der Datensicherheit sind zwingende Voraussetzungen für eine seriöse Nutzung des enormen Potenzials, das die neuen digitalen Welten für uns bereithalten.

Informations- und Datensicherheit ist ein substanzieller Bestandteil der Entwicklung von Medizinaltechnik. Um die vernetzten Produkte und Systeme vor Cyber-Attacken zu schützen, bringt die CyOne Security tiefes Expertenwissen in Cipher- und Cyber Security in die Sicherheitskonzepte und -lösungen ein, die auf der 360°-Sicherheitskompetenz von Product Security, System Security und Operational Security basieren.

Beginnen Sie heute und schützen Sie die vernetzten Dinge in der Medizinaltechnik vor Cyber-Risiken.

Machen Sie den ersten Schritt: Analysieren Sie gemeinsam mit unseren Experten Ihre aktuellen und zukünftigen Sicherheitsbedürfnisse Ihrer vernetzten Medizinalprodukte, damit wir mit Ihnen über zielgerichtete Sicherheitslösungen diskutieren können.

Kontaktieren Sie uns für ein kostenloses Expertengespräch.