CYBERSICHERHEIT IM KRANKENHAUS

So hilft Dräger, Ihr Krankenhaus zu schützen

Vernetzte Informationstechnik in Krankenhäusern sorgt für einen schnellen Austausch von Informationen und automatisierte Prozesse. Sie erhöht aber auch das Risiko von Angriffen durch Cyberkriminelle. Bei Dräger arbeiten wir kontinuierlich an der Umsetzung von Best Practices im Bereich Cybersicherheit. Darüber hinaus berücksichtigen wir die Cybersicherheit umfassend in jeder Phase des Produktentwicklungszyklus.

Cyberangriffe: ein Risiko für Gesundheitseinrichtungen

Krankenhäuser sind mehrfach Opfer von Cyberkriminalität geworden. Am häufigsten sind Erpressungsversuche mit Ransomware, bei denen wichtige Krankenhausdaten verschlüsselt werden und ein hoher Betrag in Kryptowährungen wie Bitcoin als Lösegeld für den Entschlüsselungscode verlangt wird. Allerdings gibt es noch eine ganze Reihe weiterer Cyberangriffe auf Krankenhausnetzwerke (siehe blaue Box).

BEISPIELE FÜR CYBER-ANGRIFFE AUF IT-NETZWERKE:

- Viren, Trojaner, Würmer, Spyware, Spam, Ransomware
- Advanced Persistent Threats: komplexe, gezielte Angriffe auf kritische IT-Infrastrukturen wie medizinische Netzwerke. Der Angreifer infiltriert erst einen Computer und dringt von dort weiter in die lokale IT-Infrastruktur des Opfers vor. Dabei will er möglichst lange unentdeckt bleiben, um über einen langen Zeitraum sensible Informationen auszuspähen oder anderen Schaden anzurichten.
- Botnets: Dabei schleusen Angreifer Trojaner auf Ihren Computer, übernehmen die Kontrolle und fassen die infizierten Systeme zu einem Netzwerk zusammen, das dann per Fernzugriff kontrolliert wird.
- DDoS-Angriffe (Distributed Denial of Service) zielen darauf ab, die Ressourcen eines Servers durch große Mengen gleichzeitiger Anfragen von verschiedenen Orten im Internet so zu überlasten, dass der Server nicht mehr erreichbar ist oder drastisch verlangsamt wird.

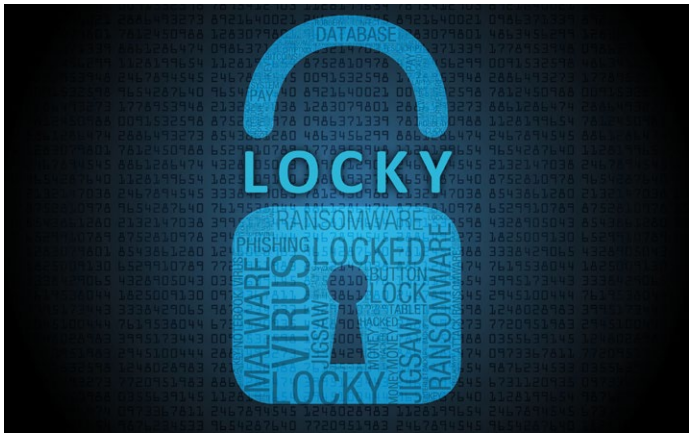
Simulierte Angriffe haben gezeigt, dass Medizingeräte oft nur unzureichend vor Manipulation geschützt sind. Neben der Gefahr für Leib und Leben der Patienten drohen Leistungsausfälle, finanzielle Einbußen, der Verlust sensibler Daten und eine negative Reputation des Krankenhauses.

Um Cyber-Bedrohungen zu entschärfen, müssen Hersteller von Medizinprodukten während des gesamten Entwicklungszyklus weitere Sicherheitsanforderungen hinzufügen.

Im Mai 2017 gab es Berichte über einen weltweiten Cyberangriff, der Krankenhäuser in Großbritannien besonders hart traf[1]. Mehrere Krankenhäuser des National Health Service (NHS) wurden lahmgelegt, darunter die in London, Blackpool, Hertfordshire und Derbyshire. Die IT-Systeme wurden mit sogenannter Ransomware infiziert. Die Verbreitung der Malware über das IT-Netzwerk führte zu einem kompletten Shutdown – die Mitarbeiter waren gezwungen, wieder auf Stift und Papier zurückzugreifen. Mehrere Patienten mussten in andere, nicht betroffene Krankenhäuser überwiesen werden. Viele Krankenhäuser waren mit den Verzögerungen überfordert.

> *„Unsere Dräger-Produkte haben diesen Angriff unbeschadet überstanden und es deutet nichts darauf hin, dass es damit in der Zukunft Probleme geben wird."*
>
> Hannes Molsen, Product Security Manager bei Dräger, über den WannaCry-Ransomware-Angriff 2017[2]

»Ein wesentlicher Grund dafür ist zweifellos, dass wir Sicherheit von Anfang an in unsere Geräte integrieren. Das bietet unseren Kunden – neben der Sicherheit – einen weiteren entscheidenden Vorteil: Die dokumentierten Sicherheitseigenschaften von Dräger-Geräten erleichtern das obligatorische IT-Sicherheits-Risikomanagement, wie es beispielsweise das deutsche IT-Sicherheitsgesetz vorschreibt.« Darüber hinaus, so Molsen, kann Dräger – selbst bei einem unerwarteten Angriff wie dem im Mai – den Kunden alle Informationen liefern, die sie benötigen, um Schutzmaßnahmen zu ergreifen.



Monitoring-Geräte beschleunigen den Digitalisierungstrend

Der Grad der Digitalisierung ist von Land zu Land noch sehr unterschiedlich. Die USA und Skandinavien führen diese unaufhaltsame Entwicklung an. Molsen stellt fest: »In den skandinavischen Ländern verzeichnen wir europaweit mit Abstand den höchsten Digitalisierungsgrad.«

Selbst in Ländern, in denen die Digitalisierung noch nicht so weit fortgeschritten ist, wie zum Beispiel Deutschland, gibt es einige sehr sensible Bereiche in Krankenhäusern. So werden Röntgen- und MRT-Daten inzwischen weitgehend digital erfasst. In Deutschland ist die in Betrieb befindliche medizinische Ausrüstung wie Anästhesie- und Beatmungsgeräte bisher nur selten an ein Netzwerk angeschlossen. Mittelfristig wird sich dies sicherlich ändern. Insgesamt sind europäische Krankenhäuser jedoch immer noch deutlich weniger vernetzt als US-amerikanische Gesundheitseinrichtungen.

Die klinische Überwachung hat den Trend zur Digitalisierung deutlich beschleunigt. Sensible Monitoringdaten aus der Intensivstation werden in das Patientendatenmanagement-System (PDMS), das OP-System oder sogar in das Anästhesiesystem eingegeben. In den USA ist die elektronische Erfassung von Patientendaten vorgeschrieben. Angesichts wachsender Patientenzahlen stellt dies eine große Herausforderung für Softwareunternehmen dar, da das Produktionsvolumen hoch ist. »Ich bezweifle, dass der Cybersicherheit bei diesem Tempo genügend Aufmerksamkeit geschenkt werden kann«, kommentiert Molsen diese Entwicklung und fährt fort: »Dräger engagiert sich für Cybersecurity, seit medizinische Geräte in einem Netzwerk miteinander verbunden sind.« Inzwischen gehört klinische Cybersicherheit zu den wichtigsten Qualitätsmerkmalen des Dräger-Portfolios.

WELTWEIT WERDEN IMMER MEHR ANGRIFFE AUF DIE DIGITALE STRUKTUR VON KRANKENHÄUSERN VERZEICHNET. HIER ZWEI BEISPIELE AUS DEM FEBRUAR 2016:

- Das Hollywood Presbyterian Medical Center in Los Angeles war von Ransomware betroffen und musste Lösegeld für seine IT-Systeme zahlen. Nach Angaben des Krankenhausdirektors wurden 40 Bitcoins im Wert von damals rund 15.000 Euro[3] gezahlt. Die betroffenen Systeme waren nach einer Woche Stillstand wieder betriebsbereit.

- Als Krankenhäuser in Deutschland angegriffen wurden, mussten sie Methoden aus dem letzten Jahrhundert anwenden. Patientendaten wurden mit Papier und Stift erfasst, Dokumente per Fax verschickt und Patienten mussten ihre Untersuchungsergebnisse persönlich abholen, anstatt sie per E-Mail zu erhalten.

Sicherheitssysteme: Standardanforderungen an unsere Geräte

Bis vor wenigen Jahren wurde die Absicherung medizinischer Geräte gegen Cyberangriffe eher im Rahmen von Einzelprojekten vorgenommen. Heute ist die Systemsicherheit in unserem umfassenden Anforderungskatalog enthalten und tief in unsere Entwicklungsprozesse eingebettet. Die Patientensicherheit steht bei Dräger ganz oben auf der Agenda und sollte jederzeit oberste Priorität haben. Dabei spielt es keine Rolle, ob das entsprechende Gerät direkt über WLAN oder über ein notdürftiges Netzwerk im täglichen Krankenhausbetrieb angebunden ist: »Wir haben unsere Denkweise geändert. Wir erkennen an, dass unsere Geräte irgendwann angegriffen werden. Und egal, ob der Angriff gezielt oder zufällig erfolgt, die Patientensicherheit muss gewahrt bleiben«, erklärt Molsen. Jede Stelle, an der Daten in ein Gerät gelangen können, ist ein möglicher Angriffspunkt. Dazu gehören zum Beispiel Schnittstellen, über die ein Angreifer das Gerät manipulieren kann, wie die Benutzeroberfläche, die Netzwerkintegration oder die USB-Anschlüsse.

Zu den Sicherheitsaspekten eines Geräts gehört auch die Umgebung, in der es betrieben wird. Angriffe auf aktiv genutzte Medizingeräte wurden bislang jedoch noch nicht bekannt und dürften auch

in Zukunft die Ausnahme bilden. Wesentlich höher ist das Risiko von Kollateralschäden durch Viren und Malware, wie die oben erwähnte Ransomware. Um sich davor zu schützen, werden Betriebssysteme in Medizingeräten meist ›gehärtet‹: Sie bestehen nur aus reduzierten, spezifischen Komponenten und bieten Viren dadurch weniger Angriffsfläche.

Hackerangriffe erfolgreich abwehren

Wenn ein Kliniknetzwerk als Intranet fungiert und somit nicht auf das öffentliche Internet zugreift, wie sind dann Hackerangriffe überhaupt möglich? Molsen beantwortet diese Frage und weist auf mögliche ›Lecks‹ hin:

- »Viele Krankenhäuser verwenden ein drahtloses internes Netzwerk. Hier kann das Sicherheitsniveau extrem variieren. Im schlimmsten Fall kann ein Angreifer mit entsprechender Ausrüstung interne Krankenhausdaten von außerhalb des Gebäudes aufzeichnen, manipulieren oder illegal weitergeben.«
- »Aber auch IT-Konfigurationsfehler oder einfache Fahrlässigkeit können dazu führen, dass die Sicherheit gefährdet und eigentlich abgeschottete Systeme von außen infiltriert werden.«
- »Innerhalb des Krankenhauses gibt es auch die Möglichkeit, über eine Netzwerkdose unerkannt auf das Intranet zuzugreifen.«

Dräger bietet vielfältige Schutzmaßnahmen gegen Netzwerkschäden durch solche Angriffe. Ziel ist es, den bestmöglichen Kompromiss zwischen Sicherheit und Benutzerfreundlichkeit (Usability) zu finden. »Allerdings sind es natürlich diese Kompromisse, die Hackern Chancen bieten«, erklärt Product Security Manager Hannes Molsen. Problematisch ist auch, dass IT-Abteilungen und Medizintechnik noch relativ unabhängig voneinander agieren. Da die Anforderungen vor dem Hintergrund der zunehmenden Digitalisierung immer stärker verschmelzen, sollte die Zusammenarbeit deutlich ausgebaut und optimiert werden.

AUF STANDARD-WLAN-BASIS

Wie Patientensicherheit, Gerätesicherheit und Vernetzung vereint werden können, zeigt das Beispiel des Sunderby Hospital in Luleå, Schweden. Dräger hat dort ein krankenhausweites Patientenmonitoring-system implementiert. Sorgfältige Planung und moderne Technik stellten sicher, dass die Qualität der Patientenversorgung verbessert und ein optimierter klinischer Arbeitsablauf für das Personal erreicht wurde. Im Video https://youtu.be/yLQ-BZ6dnHc erläutern die Mitarbeiter der IT-Abteilung des Sunderby Hospital die Vorteile – aber auch die Herausforderungen – der Implementierung eines neuen Patientenmonitoring- und Telemetriesystems in das bestehende hauseigene LAN- und WLAN-Netzwerk.

Dräger Secure Development Lifecycle: mehrschichtiger Schutz

Wir konzipieren unsere Geräte so, dass das System nur eine sehr begrenzte Angriffsfläche bietet. Das konsequente Weglassen unnötiger Softwarekomponenten führt dazu, dass viele der bereits bekannten und/oder noch bekannt werdenden Schwachstellen nicht ausgenutzt werden können. Dies reduziert auch die Anzahl der notwendigen Patches und damit die Wartungskosten der Geräte.

Dies lässt sich am Beispiel der Beatmung veranschaulichen: Während ein Patient beatmet wird, werden verschiedene Servicefunktionen automatisch deaktiviert und sind somit auch über das Netzwerk nicht verfügbar. Der Inbound-Zugriff über die Schnittstelle ist nur bei ausgeschalteter Beatmung möglich. Auf diese Weise kann das Risiko einer möglichen Schädigung des Patienten durch äußere Manipulationen auf ein absolutes Minimum reduziert werden.

Zur Erhöhung der Cybersicherheit ergreifen wir die folgenden Maßnahmen:

- Bewertung des Datenschutzes und der Datensicherheit unserer Lösungen
- Penetrationstests durch unabhängige Experten (White Hats)*
- Sicherheitsschulungen für Mitarbeiter, die am Entwicklungslebenszyklus beteiligt sind
- Ein internes Cybersicherheitsteam, das unser Engagement auf globaler Ebene koordiniert

Ein weiterer wichtiger Bestandteil unserer Sicherheitsstrategie ist die »Coordinated Vulnerability Disclosure Policy«, eine Art direkter Draht zu unseren Sicherheitsexperten, über den entdeckte potenzielle Schwachstellen gemeldet werden können.

Note: on our website https://www.draeger.com/cybersecurity we provide you with further information about cybersecurity in hospitals.
We also provide you with security information on current threats on our Coordinated Disclosure Statement page (https://static.draeger.com/security).

Die Bedeutung ständiger Weiterbildung

Allen Fachkräften im Krankenhaus sollte bewusst sein, dass es potenzielle Schwachstellen gibt und wie diese von Cyberkriminellen ausgenutzt werden können. Außerdem sollten sie ihr Wissen regelmäßig auffrischen, beispielsweise zu folgenden Themen:

- Umgang mit E-Mail-Anhängen
- Umgang mit Passwörtern
- Verhalten in öffentlichen Internetforen
- Umgang mit USB-Sticks

Da die Cybersicherheit im Gesundheitswesen ein dauerhaftes Anliegen ist, sollten auch IT-Spezialisten und Medizintechniker regelmäßig geschult werden. Schließlich ist aktuelles Wissen der Schlüssel, um die Sicherheit aufrecht zu erhalten.

Cybersicherheit neu denken

Die Zusammenarbeit zwischen Medizintechnik und IT hinsichtlich Sicherheitsfragen sollte sich in den nächsten Jahren weiter intensivieren. Ein Indiz dafür ist der internationale Standard IEC 80001-1 »Risikomanagement für medizinische IT-Netzwerke«, der insbesondere für Betreiber und Anwender gilt und auf eine partnerschaftliche Zusammenarbeit mit den Herstellern ausgerichtet ist. Einen weiteren Hinweis auf steigende Sicherheitsanforderungen liefert die US-amerikanische Food and Drug Administration (FDA). Diese verweist auf die Richtlinien des NIST (National Institute of Standards and Technology) zur Absicherung kritischer Infrastrukturen gegen Cyberangriffe[4]. Die FDA hat im Oktober 2014 erstmals eine »Premarket Guidance« mit IT-Sicherheitsanforderungen für die Entwicklung und Vermarktung von Medizinprodukten veröffentlicht. Ende 2016 wurde eine 30-seitige »Postmarket Guidance« veröffentlicht, ein Leitfaden zum Management von IT-Sicherheitsrisiken für vernetzte Medizinprodukte nach deren Markteinführung. In Deutschland hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) im Jahr 2013 den Leitfaden »Schutz kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT« veröffentlicht[5].

Fazit: Wirksamer Schutz vor Cyberkriminellen kann nur erreicht werden, wenn alle Beteiligten zusammenarbeiten: Systemadministratoren, Softwarehersteller, Medizinproduktehersteller, Anwender und Datenschutzbeauftragte. Es ist an der Zeit, Cybersicherheit neu zu denken.

*Penetrationstests für ausgewählte Produkte seit 2015 durchgeführt, verpflichtend für alle Produktneuentwicklungen seit 2019developments since 2019

IMPRESSUM

DEUTSCHLAND
Drägerwerk AG & Co. KGaA
Moislinger Allee 53–55
23542 Lübeck

www.draeger.com

DMC-101010

SOURCES:

(1) NHS cyber-attack: GPs and hospitals hit by ransomware at http://www.bbc.com/news/health-39899646 (downloaded on 26/07/2017).

(2) Expertengespräch Hannes Molsen, Product Security Manager, Drägerwerk AG & Co. KGaA, 19/05/2017

(3) http://hollywoodpresbyterian.com/default/assets/File/20160217%20Memo%20from%20the%20CEO%20v2.pdf (downloaded on 26/07/2017).

(4) FDA outlines cybersecurity recommendations for medical device manufacturers, www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm481968.htm (downloaded on 26/07/2017)

(5) www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Kritis/RisikoanalyseKrankenhausIT_Leitfaden_pdf.pdf?_blob=publicationFile ((downloaded on 26/07/2017)