Sichere Vernetzung

Entwicklerinterview mit Hannes Molsen,
Global Product Security Manager bei Dräger

Der erste wichtige Schritt – einheitliche Standards schaffen.

Die Angriffsfläche für Hacker minimieren

Die Digitalisierung im Healthcare-Sektor schreitet voran. Die Branche strebt nach einer herstellerunabhängigen Interoperabilität. Gleichzeitig mehren sich die Berichte über Cyberattacken auf Krankenhäuser. Was bedeuten diese Entwicklungen?

Eine flächendeckende Vernetzung erhöht zweifelsohne die Angriffsfläche. Die bereits praktizierte Netzwerksegmentierung in Krankenhäusern bietet Sicherheit und soll auch künftig erhalten bleiben. Die Herausforderung besteht darin, die Situation aufzulösen, wonach jeder Gerätehersteller gewissermaßen ein eigenes Netzwerk benötigt. Dazu müssen wir einheitliche Standards schaffen. Als erster wichtiger Schritt ist hierzu im Januar 2019 das neue Kommunikationsprotokoll SDC als Teil der IEEE 11073 Standardserie veröffentlicht worden. Vor diesem Hintergrund ist auch eine Netzwerkzugangskontrolle wichtig, die durch Authentifizierung – beispielsweise durch digitale Sicherheitszertifikate – vom Netzwerk selber oder dem Endgerät verlangt wird. Dabei muss die Verschlüsselung wiederum ausreichend gesichert sein, um einen adäquaten Schutz zu garantieren. Zu den bekannten Angriffen auf Krankenhäuser der letzten Zeit sei gesagt, dass diese nicht zielgerichtet erfolgten, sondern Folge von im Netz kursierender Malware waren. Krankenhäuser trifft es aber besonders oft, da deren Software häufig veraltet ist.

Birgt eine herstellerunabhängige Konnektivität nicht das Risiko einer schnelleren Malware-Ausbreitung auf das gesamte System?

Eine erhöhte Netzkonnektivität ist immer mit einem erhöhten Risiko verbunden. Dem begegnen wir, indem wir auch die

Eigensicherheit jedes einzelnen Endgeräts und nicht nur des Netzwerks berücksichtigen. Die Kernfunktionen der Geräte müssen auch bei einem Angriff erhalten bleiben. Gerade für versorgungsrelevante Medizintechnik gilt die Maxime: Das Netzwerk sollte immer nur eine Zusatzfunktion der Geräte darstellen. Und wenn diese einmal ausfällt, muss die Grundfunktion trotzdem erhalten bleiben. Nur so ist die Patientensicherheit jederzeit gewährleistet.

Welche Rolle nimmt die Reduktion der Angriffsfläche – die „Härtung der Softwarekomponenten" – für die Cybersicherheit bei versorgungsrelevanten Medizintechnikgeräten ein?

Bei medizintechnischen Geräten ist es wichtig, nur so viele nach außen erreichbare Softwarekomponenten zu integrieren, wie für die Funktion wirklich notwendig sind. Entbehrliche Elemente sollten weggelassen werden. Vereinfacht ausgedrückt: Ein Beatmungsgerät, basierend auf einem Windows Betriebssystem, benötigt nicht die gleichen Features wie der PC im Ärztezimmer mit E-Mail-Postfach, Textprogrammen etc. So wird die Angriffsfläche für Hacker deutlich reduziert. Weiter vermindert werden kann diese durch eine modulare Zusammensetzung der Betriebssysteme. Zusammenfassend kann man also sagen: Je weniger Software nach außen sichtbar, desto sicherer ist die Technik.

Auf welchem Stand befindet sich die in Fachkreisen postulierte Forderung nach einer technischen Trennung von Funktions- und Netzwerkkomponenten bei Therapiegeräten?

Das ist in der Tat ein viel diskutiertes Thema. Bei einigen unserer Geräte haben wir dies bereits realisiert. Softwareseitig ist eine strikte Trennung auf jeden Fall notwendig. Schließlich darf Komponente A nicht mitbetroffen sein, sollte Komponente B einmal abstürzen.

Im gesamten Kontext der Digitalisierung und Interoperabilität im Healthcare-Bereich stellt sich – neben den von Ihnen erwähnten Maßnahmen zur Cybersicherheit – die Frage nach der Rolle softwaregestützter Sicherheitslösungen, z. B. Firewalls.

Da sprechen Sie einen wichtigen Punkt an, der kontrovers gesehen wird. Fest steht: Firewalls und Antivirusprogramme sind für Consumer-PCs, etwa im Ärztezimmer oder der Verwaltung, unverzichtbar. Auf Medizingeräten ist ihre Relevanz dagegen eher untergeordnet. Firewalls verhindern lediglich das Ansprechen bestimmter Softwarekomponenten auf Signale. Dies setzt aber voraus, dass diese Komponenten überhaupt vorhanden sind. Genau das ist jedoch bei der Medizintechnik oft nicht der Fall. Hier erinnere ich an das Prinzip der gehärteten Systeme, also das Minimieren von Softwareelementen auf das für die Funktionalität des Geräts unbedingt notwendige Maß. Auch Antivirusprogramme sind eher für dynamische Systeme mit vielfältigen Applikationen, wie PCs, gedacht. In Zukunft wird die Menge an Applikationen auch auf Medizingeräten zunehmen, sodass sich die Anforderungsprofile an Sicherheitssoftware ändern können. Dann gewinnen auch in diesem Zusammenhang Firewalls und Sicherheitssoftware möglicherweise an Bedeutung. Ein realistisches Szenario wäre zum Beispiel: Die mit einem Therapiegerät erzeugten Daten werden durch ein Netzwerk auf den PC im Ärztezimmer übertragen, dort analysiert, in einen Anwendungsbefehl – zum Beispiel „Änderung der Medikation" – konvertiert und zurück an das Therapiegerät geschickt.

Es scheint, als ließe sich die Cybersicherheit also vor allem durch eine Reduktion der potenziellen Angriffsfläche erhöhen. In IT-Kreisen hört man aber in diesem Zusammenhang auch immer wieder von der Bedeutung des Schnittstellenmanagements. Wo kommt dies ins Spiel?

Physikalische Schnittstellen verändern sich ständig. In der Medizintechnik ist das Thema noch nicht richtig angekommen. Hier wird nach wie vor sehr konservativ gearbeitet, und das wird auch noch eine ganze Weile so andauern. Zum Beispiel wird häufig noch das klassische serielle Kabel anstelle eines Netzwerkkabels genutzt. Die physikalischen Schnittstellen verlieren aber vermutlich an Bedeutung, weil immer mehr Datenaustausch über Netzwerke abgewickelt wird. Nichtsdestotrotz gilt auch hier: Die Wahrscheinlichkeit von Angriffen über Schnittstellen kann reduziert werden, wenn die Systeme gehärtet sind.

Bei all dem rasanten Fortschritt: Wie kann das nicht IT-ausgebildete Krankenhauspersonal Schritt halten?

Zum Beispiel haben Schulungen eine große Bedeutung. Hier wird der Umgang mit E-Mail-Anhängen, USB-Sticks und Links erlernt. Auch das Verhalten in öffentlichen Internetforen ist Inhalt dieser Veranstaltungen. Besonders wichtig ist es aber zu vermitteln, was passiert, wenn die Technologie einmal ausfällt, und woran Fehlfunktionen erkannt werden können. Je größer und dynamischer die Netzwerke sind, desto größer ist das Risiko von Fehlern oder Ausfällen. Der Umgang mit technischen Störungen muss erlernt werden, und sei es nur, dass jemand versehentlich über ein Kabel stolpert und dieses herausreißt. Wichtig ist dann, Panik zu vermeiden. Gibt es ein gut abgestimmtes Cybersicherheits-Konzept mit gehärteten Systemen, sicheren Netzwerken und geschultem Personal, kommt diese aber erst gar nicht auf.

IMPRESSUM

Drägerwerk AG & Co. KGaA
Moislinger Allee 53-55
23558 Lübeck
Tel +49 (0) 451 / 882 0
Fax +49 (0) 451 / 882 2080
E-Mail: info@draeger.com
www.draeger.com

PDF-9312 | 19.06.1