Wir bei Dräger entwickeln Technik für das Leben. Diese Technik unterliegt einem ständigen Wandel und die Digitalisierung des Gesundheitswesens schreitet rasant voran. Wir gestalten den Wandel mit, damit sich die digitale Technik positiv auf die Patientenversorgung und die Krankenhausökonomie auswirkt.

1. EINFÜHRUNG

Wir bei Dräger entwickeln Technik für das Leben. Diese Technik unterliegt einem ständigen Wandel und die Digitalisierung des Gesundheitswesens schreitet rasant voran. Wir gestalten den Wandel mit, damit sich die digitale Technik positiv auf die Patientenversorgung und die Krankenhausökonomie auswirkt. Bereits heute werden medizinische Geräte und Systeme in zunehmendem Maße zu Netzwerken verbunden, um miteinander zu interagieren und so neue klinische Anwendungen zu ermöglichen. Diese beinhalten Technologien zur Entscheidungsunterstützung, Fernsteuerungsfunktionen und automatisierte Prozesse. All das muss jedoch in einer sicheren Netzwerkumgebung erfolgen, um die Funktionsfähigkeit und den Datenschutz zu gewährleisten. Krankenhäuser unternehmen massive Anstrengungen, um ihre Netzwerke zu sichern. Die Hersteller sollten zur Umgebungssicherheit beitragen, indem sie Produkte anbieten, die widerstandsfähig gegen Cyber-Angriffe sind und sich sicher in die Krankenhausnetzwerke integrieren lassen.

Da die Bedrohungen und Risiken der Cybersicherheit für interne und externe Gesundheitsumgebungen weiter zunehmen, sind gut etablierte Sicherheitskontrollen für einen angemessenen Schutz von Patienten und Patientendaten erforderlich.

Medizinische Geräte unterscheiden sich von üblichen vernetzten Geräten. Es handelt sich um Geräte mit fester Funktion, die für eine spezielle Aufgabe entwickelt wurden und so optimiert sind, dass sie möglichst wenig Verarbeitungszyklen und Speicher benötigen. Das Sicherheitsniveau, das für ein medizinisches Gerät erforderlich ist, variiert je nach Funktion. Gleichwohl müssen alle Geräte über geeignete Sicherheitskontrollen verfügen, um das Gerät selbst, seine Daten und den verbundenen Patienten vor Cyberangriffen zu schützen.

Dies wird idealerweise erreicht, indem die Sicherheit bereits in den frühen Phasen des Produktlebenszyklus mit einem umfassenden Ansatz in Bezug auf Cybersicherheitsstandards und Best Practices integriert wird. Dieser vielschichtige Ansatz ist bei Dräger tief in die Entwicklungsprozesse sowie in die technische Steuerung verwurzelt.

Unsere medizinischen Geräte und Systeme werden gemäß den aktuellen Best Practices der Cybersicherheit entwickelt, wie in diesem Dokument beschrieben. Dies gilt für alle Produkte, die sich derzeit in der Entwicklung befinden. Es gilt nicht unbedingt für alle derzeit vermarkteten Portfolios. Für diese Portfolios fordern Sie bitte ein MDS2-Formular von Ihrem lokalen Vertriebspartner an.

In diesem Papier erfahren Sie, wie Sicherheit bei der Entwicklung unserer Medizingeräte umgesetzt wird. Weitere Informationen zur Sicherheit von Cloud-basierten Produktlösungen und Diensten stellen wir Ihnen in einem separaten Papier zur Verfügung.

Es liegt in unserer Verantwortung, sicherzustellen, dass unsere Geräte sicher im Krankenhausnetzwerk betrieben werden können. Sie als unser Kunde sind für die Sicherheit in Ihrem Krankenhausnetzwerk verantwortlich. Daher muss Cybersicherheit als gemeinsame Verantwortung verstanden und gemeinsam verwirklicht werden.

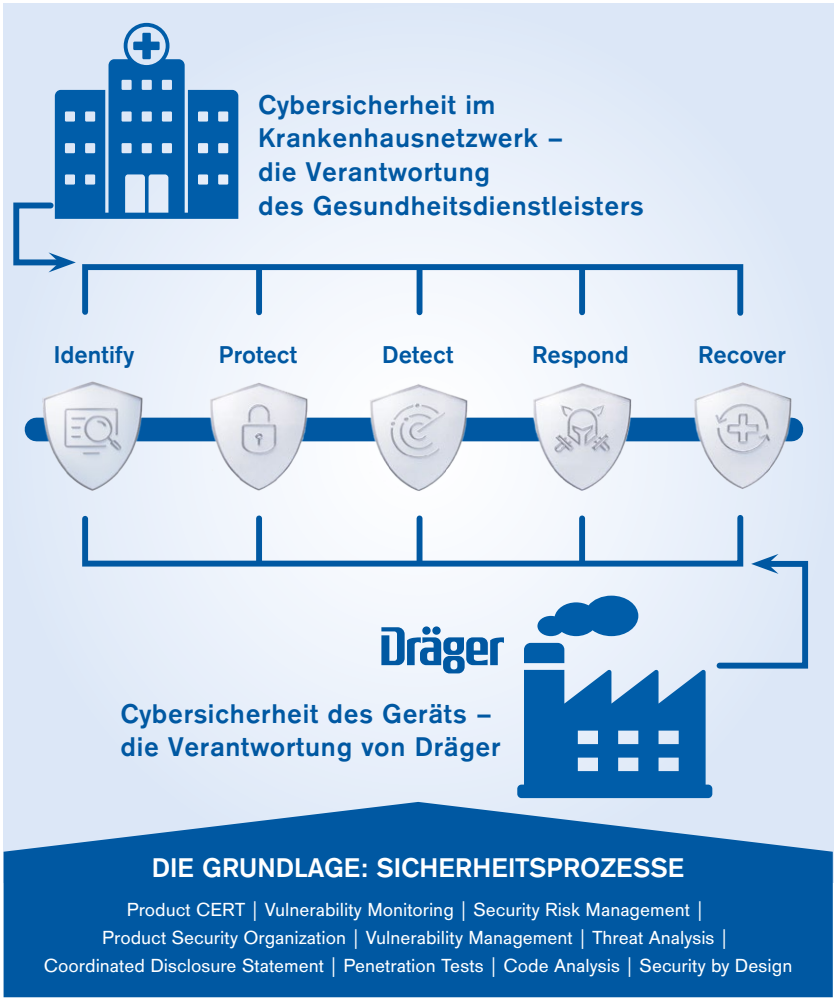
2. CYBERSICHERHEIT – EINE GEMEINSAME VERANTWORTUNG

Es gibt kein ›Patentrezept‹ für Cybersicherheit. Cybersicherheit erfordert umfassende administrative, logische und physische Kontrollen, um medizinische Geräte zu schützen und Risiken für Patienten sowie finanzielle Schäden zu vermeiden. Es handelt sich um kein kurzfristiges oder einmalig zu erledigendes Projekt, sondern um einen kontinuierlichen, vielschichtigen Prozess zur Minimierung der Risiken für Medizingeräte und Patienten.

Mit der zunehmenden Digitalisierung der Gesundheitssysteme wird die Sicherheit von Krankenhausnetzwerken immer wichtiger, um das Risiko durch Angriffe zu minimieren. Wir bei Dräger sind uns über die Notwendigkeit für Krankenhäuser im Klaren, durch Best Practices im Bereich Cybersicherheit ihre Netzwerke und ihre Vermögenswerte zu schützen. Es liegt in unserer Verantwortung als Anbieter vernetzter medizinischer Geräte und Systeme, sicherzustellen, dass unsere Produkte sicher in das Netzwerk Ihrer Kliniken integriert werden können.

DAS SICHERHEITSGERÜST. Unsere vielschichtige Sicherheitsstrategie lässt sich am besten als ›tiefgreifende Verteidigung‹ umschreiben. Statt einer einzelnen Lösung oder eines einzelnen Prozesses für Cybersicherheit verwenden wir eine schichtweise Strategie zur Entwicklung von Abwehrmaßnahmen für alle unsere Geräte und Systeme. Diese Strategie folgt denselben Best Practices für Cybersicherheit, denen auch immer mehr Krankenhäuser in ihren Sicherheitsstrategien folgen, sodass Sie unsere Geräte und Systeme nahtlos in Ihre Netzwerke und Sicherheitskonzepte integrieren können.

DAS MODELL DER GEMEINSAMEN VERANTWORTUNG FÜR MEDIZINGERÄTE



D-45346-2021

Der von uns befolgte Rahmen für bewährte Sicherheitsverfahren beinhaltet die folgenden Funktionen:

– IDENTIFY / IDENTIFIZIEREN

Die ›Identify‹-Funktion hilft bei der Entwicklung eines organisatorischen Verständnisses für das Management von Cybersicherheitsrisiken für Systeme, Menschen, Vermögenswerte, Daten und Fähigkeiten. Sie ermöglicht einer Organisation, ihre Bemühungen zu fokussieren und zu priorisieren, in Übereinstimmung mit ihrer Risikomanagement-Strategie und den Geschäftsanforderungen.

– PROTECT / SCHÜTZEN

Die ›Protect‹-Funktion umreißt geeignete Schutzmaßnahmen, um die Bereitstellung kritischer Infrastrukturdienste zu gewährleisten. Sie unterstützt die Fähigkeit, die Auswirkungen eines potenziellen Cybersicherheits-Ereignisses zu begrenzen oder einzudämmen.

– DETECT / ERKENNEN

Die ›Detect‹-Funktion definiert die geeigneten Aktivitäten zur Erkennung eines Cybersecurity-Ereignisses. Sie ermöglicht somit die rechtzeitige Entdeckung von Cybersecurity-Ereignissen.

– RESPOND / REAGIEREN

Die ›Respond‹-Funktion umfasst geeignete Aktivitäten zur Ergreifung von Maßnahmen bei einem festgestellten Cybersicherheitsvorfall. Sie unterstützt die Fähigkeit, die Auswirkungen eines potenziellen Cybersicherheitsvorfalls einzudämmen.

– RECOVER / WIEDERHERSTELLEN

Die ›Recover‹-Funktion unterstützt die rechtzeitige Wiederherstellung des normalen Betriebs, um die Auswirkungen eines Cybersicherheitsvorfalls zu minimieren.

GEMEINSAME VERANTWORTUNG

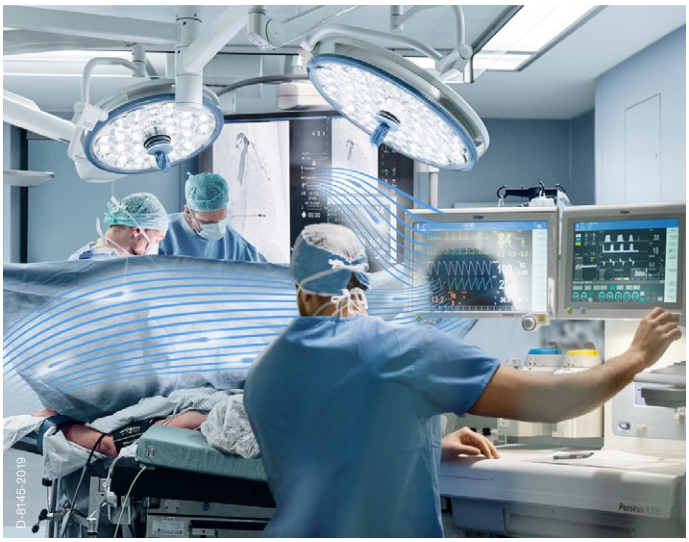
Um einen möglichst effektiven Schutz vor Cyberangriffen zu erreichen, sollten Best-Practice-Schutzmaßnahmen idealerweise auf beiden Seiten implementiert werden: im Krankenhaus, um die Sicherheit des Netzwerks zu gewährleisten, und bei Dräger, um sichere vernetzte medizinische Geräte und Systeme zu entwickeln. Cybersecurity ist also eine gemeinsame Verantwortung. Als Krankenhausbetreiber sind Sie dafür verantwortlich, medizinische Geräte in eine sichere Netzwerkumgebung zu integrieren, basierend auf Ihren Sicherheitsrichtlinien. Unsere Verantwortung als Anbieter von medizinischen Geräten und Systemen besteht darin, die internen Komponenten des medizinischen Geräts bis hin zu seinen Außenbereichen zu schützen, um sicherzustellen, dass die Krankenhäuser Aktivitäten und Änderungen an und von unseren medizinischen Geräten überwachen können. Darüber hinaus müssen wir Ihnen alle Informationen und Unterstützung zur Verfügung stellen, die Sie für die sichere Implementierung in Ihrer Netzwerkumgebung benötigen.

In den folgenden Kapiteln geben wir Einblicke in die technischen Kontrollen, unsere Sicherheitsorganisation und unsere Prozesse entlang des ›Secure Development Lifecycle‹, die zusammen unseren schichtenbasierten Ansatz zur Sicherung unserer medizinischen Geräte und Systeme bilden und die sichere Integration in Ihre Netzwerke nahtlos ermöglichen.

3. TECHNISCHE KONTROLLEN

Wir haben zahlreiche technische Kontrollen und Sicherheitsvorkehrungen in unsere Medizinprodukte eingebaut, um sie vor Cyberangriffen zu schützen und Risiken zu begrenzen. Die Kontrollen basieren auf den in diesem Dokument beschriebenen Best Practices für die Kategorien: Identifizieren, Schützen, Entdecken, Reagieren und Wiederherstellen.

Die Software unserer medizinischen Geräte ist ein geschlossenes System, das sich beim Booten und während des normalen Betriebs selbst verifiziert. Alle ausführbaren Dateien des Teilsystems werden vor der Herstellung des Geräts validiert und das Teilsystem wird gesperrt, um die Ausführung aller weiteren ausführbaren Dateien zu verhindern.



IDENTIFY / IDENTIFIZIEREN

Wir stellen Ihnen als Kunde alle Informationen zur Verfügung, die Sie benötigen, um Ihre Vermögenswerte und die bekannten Cyber-Risiken, die unsere Medizingeräte bedrohen, zu identifizieren. Diese Informationen umfassen:

- eine Software-Stückliste (Software Bill of Material, SBOM), die alle im Produkt verwendeten Softwarekomponenten von Drittanbietern auflistet
- die Offenlegung von Sicherheitshinweisen, falls neue Schwachstellen des Produkts gefunden werden
- Gebrauchsanweisungen, die unter anderem Aspekte der Cybersicherheit bei der Integration des Geräts in das Kundennetzwerk beschreiben
- die Offenlegungserklärung des Herstellers für Medizinprodukte-Sicherheit (MDS2), um Kunden bei der Bewertung der Sicherheitsrisiken im Zusammenhang mit der Verwaltung von Medizingeräten zu unterstützen

PROTECT / SCHÜTZEN

Wir verfolgen einen Security-by-Design-Ansatz zum Schutz unserer medizinischen Geräte vor Cyber-Bedrohungen. Das Ziel von Security-by-Design ist es, die Angriffsfläche, die die Geräte bieten, zu minimieren. Die Schutzkontrollen sind vorbeugende Maßnahmen, um das Risiko zu verringern, dass ein Gerät im Falle eines Angriffs kompromittiert wird.

Unsere technischen Kontrollen sind so konzipiert, dass eine unbefugte Nutzung verhindert wird, indem der unbefugte Zugriff verweigert wird und die Prinzipien ›need to know‹ und ›least privilege‹ berücksichtigt werden.

Authentifizierungs- und Autorisierungskontrollen für medizinische Geräte werden auf Basis folgender Best Practices entwickelt:

- **Eingeschränkter Fernzugriff.** Diese Best Practice wird empfohlen, um jeglichen Zugriff, insbesondere den Fernzugriff, einzuschränken und so das Risiko eines unbefugten und nicht authentifizierten Zugriffs auf das medizinische Gerät oder System zu begrenzen.
- **Authentifizierter Zugang.** Ein authentifizierter Zugang ist erforderlich. Unsere Geräte sind so konzipiert, dass sie die Anforderungen an eine sichere Authentifizierung mit den Anforderungen an die Benutzerfreundlichkeit zur Unterstützung der Arbeitsabläufe in der Akutmedizin in Einklang bringen.
- **Passwörter.** Passwörter bilden die erste Verteidigungslinie gegen unbefugten Zugriff auf Dräger-Geräte und -Systeme. Wenn möglich, sollten sichere Passwörter verwendet werden.
- **Session-Timeouts,** wenn eine bestimmte Zeit lang keine Aktivität stattfindet. Diese Konfiguration trägt dazu bei, das Risiko zu begrenzen, dass ein medizinisches Gerät oder System unbefugtem Zugriff ausgesetzt ist. Ein unzureichender Session-Ablauf durch eine medizinische Anwendung, ein medizinisches Gerät oder System erhöht die Anfälligkeit für andere Session-basierte Angriffe, wie die Wiederverwendung einer gültigen Session-ID oder die Kaperung der zugehörigen Session. Je kürzer das Session-Intervall ist, desto weniger Zeit hat ein Angreifer, die gültige Session-ID zu verwenden.
- **Ändern von Standardpasswörtern.** Standardpasswörter sind vorkonfigurierte Passwörter für medizinische Geräte und Software, die leicht im Internet zu finden sind. Die Änderung eines Standardpassworts kann sicherstellen, dass der Zugang geschützt und auf autorisierte Personen oder Systeme beschränkt ist. Solche Passwörter sind die Standardkonfiguration für viele bestehende Geräte und stellen, wenn sie unverändert bleiben, ein ernsthaftes Sicherheitsrisiko dar. Viele Standardpasswörter sind öffentlich dokumentiert und weithin verfügbar. Standardpasswörter sollten geändert werden, bevor die Geräte oder Systeme an ein Netzwerk angeschlossen werden.
- **Verschlüsselte Authentifizierung.** Um sicherzustellen, dass Benutzerkennungen und Kennwörter bei der Übertragung über das Netzwerk nicht ausgespäht werden können, wird auf dem medizinischen Gerät eine verschlüsselte Authentifizierung verwendet.

Durch folgende Techniken stellen wir sicher, dass nur von uns signierte, vertrauenswürdige Software auf unserem Medizingerät ausgeführt werden kann:

- Sichere / vertrauenswürdige Bootchain, die die Integrität der auf dem medizinischen Gerät laufenden Firmware und Software gewährleistet. Auf diese Weise kann ein medizinisches Gerät vor bösartigen Angriffen, Rootkits und nicht autorisierten Software-Updates geschützt werden, die vor dem Start des Betriebssystems (OS) erfolgen könnten. Dräger verwendet Secure Boot, um seine medizinischen Geräte und Systeme vor Angriffen zu schützen. Secure Boot erkennt Manipulationen an Bootloadern, am Betriebssystem-Kernel sowie an ausführbaren Dateien und statischen Konfigurationsdateien, indem es deren digitale Signaturen prüft.
- Interne Verwaltung der Kodierungsschlüssel, einschließlich des Schutzes der Schlüssel in einem internen sicheren Schlüsselspeicher.
- Software-Integrität, d. h., dass der Code das tut, was er soll: Er ist getestet, verfügt über Sicherheitsfunktionen, ist robust und lässt sich leicht editieren und aktualisieren, ohne neue Fehler einzuführen. Software-Integrität ist für Dräger wichtig, weil sie die Sicherheit und Wartungsfreundlichkeit unseres Geräte- und Systemcodes demonstriert. Die Integrität unserer Software ist entscheidend für die Einhaltung von Kodierungsstandards und Branchenvorschriften.

D-45341-2021

Datenübertragungen zu und von den Geräten werden durch die Verwendung verschlüsselter Transportkanäle und kryptografischer Prüfsummen geschützt. So kann die Vertraulichkeit und Integrität der ausgetauschten Daten gewährleistet werden, und unsere Geräte sind vor böswilligen Angriffen, Datenexfiltration und anderen Sicherheitsrisiken geschützt.

Durch das Weglassen unnötiger Softwarekomponenten und die Deaktivierung aller nicht genutzten Netzwerkports wird die Gerätekonfiguration gehärtet, um die Angriffsfläche zu verringern.
›Deny all by default‹ stellt sicher, dass undefinierte Ports nicht für den Zugriff auf das medizinische Gerät oder System verwendet werden können. Dräger stellt sicher, dass offene TCP/IP-Ports so eingeschränkt werden, dass Zugriff und Kommunikation nur autorisiert möglich sind.

DETECT / ERKENNEN

Zusätzlich zu den präventiven technischen Kontrollen, die ein Gerät vor Angriffen schützen, ist es wichtig, dass Versuche, ein Gerät zu kompromittieren, erkannt werden können. Die Fähigkeit, anomale Aktionen oder Cybersecurity-Ereignisse rechtzeitig zu erkennen, ist entscheidend für eine wirksame Reaktion im Falle eines Angriffs.

Medizinische Geräte von Dräger führen ein Sicherheitsereignisprotokoll, das alle sicherheitsrelevanten Ereignisse enthält, die ein Administrator zur Analyse potenzieller Kompromittierungen und für forensische Beweise benötigt. Zu den möglichen Sicherheitsereignissen gehören unter anderem Authentifizierungs-, Softwareinstallations- und Konfigurationsereignisse sowie Netzwerkanomalien.

Um Manipulationen zu verhindern, wird jeder einzelne Protokolleintrag von einer kryptografischen Prüfsumme (Hash-basierter Nachrichtenauthentifizierungscode) begleitet, die aus der Protokollnachricht und einem gerätespezifischen geheimen Schlüssel gebildet wird. Dieser Ansatz ermöglicht es, Manipulationen von Protokolleinträgen, einschließlich Änderungen und Löschungen, zu erkennen.

Im Falle von Sicherheitsereignissen mit Auswirkungen auf die Geräteintegrität und einer möglichen Beeinflussung der Therapie erhält der klinische Anwender des Geräts dringende Warnungen, die darauf hinweisen, dass das Gerät nicht für den klinischen Einsatz geeignet ist.

Sicherheitsereignisse, die auf ein anormales technisches Verhalten hinweisen, werden dem administrativen Benutzer des Geräts oder der IT-Abteilung des Krankenhauses gemeldet.

Benachrichtigungen über Konfigurationsänderungen. Eine Änderung der Geräte- oder Systemkonfiguration kann sich auf die Leistung, Sicherheit, Verfügbarkeit und den Betrieb auswirken. Änderungsbenachrichtigungen in Form von Alarmen können sich als lebensrettend erweisen, da sie den Administrator in Echtzeit über die Änderungen und deren Details informieren.

RESPOND / REAGIEREN

Damit Sie als unser Kunde schnell und effektiv auf ein erkanntes Cybersecurity-Ereignis reagieren können, enthält jede Ereignisbenachrichtigung, die an Ihre IT-Administratoren gesendet wird, Informationen über die Ursache des Sicherheitsereignisses und empfohlene Maßnahmen.

Unsere Geräte enthalten eine Komponente namens System Health Monitor (SHM), die den Ressourcenverbrauch der auf dem Gerät laufenden Software während des Betriebs misst. Der SHM misst zum Beispiel kontinuierlich die Speichernutzung und die Prozessorauslastung. Wenn der Verbrauch die vom SHM festgelegten Grenzwerte überschreitet, wird als letzter Ausweg ein Neustart des Systems durchgeführt. Während des Neustarts werden verschiedene Überprüfungen durchgeführt, bevor das System erneut gestartet wird.

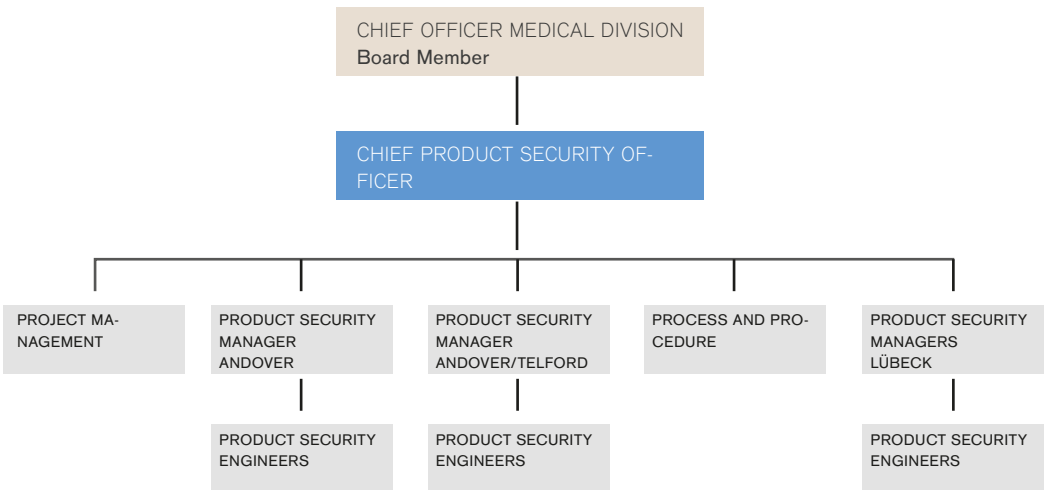
Die durch den Schnittstellenverkehr verursachte Systembelastung wird durch Überwachung der vom Netzwerkprotokollstapel des Geräts verwendeten Ressourcen gemessen. Übersteigt die Ressourcennutzung ein bestimmtes Niveau, so dass das Laufzeitverhalten anderer Systemteile beeinflusst werden könnte, wird der Netzwerkadapter automatisch bis zum nächsten Neustart deaktiviert.

RECOVER / WIEDERHERSTELLEN

Nachdem ein Cyberangriff erfolgreich abgewehrt wurde, muss das Gerät wieder »gesund« werden, um den normalen Betrieb fortsetzen zu können. Unsere medizinischen Geräte unterstützen die Wiederherstellung durch die folgenden Sicherheitsvorkehrungen:

- Das Gerät unterstützt die Speicherung von klinischen Konfigurationen auf USB-Massenspeichergeräten für Verteilungs- und Sicherungszwecke.
- Stellt das Gerät einen durch einen Cyberangriff verursachten Software-Laufzeitfehler fest, leitet es einen Neustart des Systems ein, um es in einen bekannten guten Zustand zu versetzen.
- Als letztes Mittel kann der Dräger Service Hardware- und/oder Softwarekomponenten wiederherstellen.

4. DIE ORGANISATION FÜR PRODUKTSICHERHEIT VON DRÄGER



Unsere Organisation für Produktsicherheit wendet einen mehrschichtigen Schutzansatz an, um die Sicherheit unserer Produkte zu gewährleisten und zu kontrollieren.

Die Organisation für Produktsicherheit ist von der Produktentwicklung getrennt und in den USA und Europa angesiedelt. Dadurch ist die Organisation für die Produktsicherheit autonom und kann sich unabhängig vom Produktentwicklungsprozess ganz auf die Sicherheit konzentrieren.

Der Chief Product Security Officer ist für alle Dräger-Produkte verantwortlich und berichtet direkt an den Vorstand, der die übergreifende Verantwortung und Rechenschaftspflicht hat, um sicherzustellen, dass Dräger-Produkte sicher sind, wenn eine Gesundheitsorganisation sie in ihrer Umgebung implementiert.

Die Product Security Manager berichten an den Chief Product Security Office und sind für die Sicherheit aller Produkte verantwortlich.

Die Product Security Engineers berichten an die Product Security Manager und sind für alle Sicherheitskontrollen und -prozesse innerhalb eines bestimmten Produkts verantwortlich.

D-45342-2021, D-45343-2021, D-45344-2021

5. SECURE PRODUCT DEVELOPMENT LIFECYCLE

Unser ›Secure Product Development Lifecycle‹ stellt die Sicherheit in den Mittelpunkt des Entwicklungsprozesses von medizinischen Geräten und Firmware. Von den Anforderungen bis zum Design und von der Entwicklung bis zum Testen sind wir bestrebt, die Sicherheit bei jedem Schritt des Entwicklungsprozesses in unsere medizinischen Geräte und Firmware zu integrieren.
Wir haben sechs Schlüsselkomponenten in unseren ›Secure Product Development Lifecycle‹ integriert:

– Training
– Design
– Entwicklung
– Verifizierung / Testing
– Freigabe
– Wartung / Überwachung

SCHULUNG

Für jeden sicheren Produktentwicklungszyklus ist eine technische Schulung der beteiligten Mitarbeiter erforderlich. Sie umfasst zahlreiche Themen mit Fokus auf sicheres Design, sichere Kodierung und die Minimierung von Risiken und Bedrohungen für Firmware. Sichere Produkte entstehen nicht, indem Sicherheitsanforderungen einfach zu einem Medizinprodukt und die Firmware hinzugefügt werden. Diese Art der Entwicklung kann zusätzliche Risiken und Schwachstellen bei der Entwicklung von Produkten mit sich bringen. Die Integration von Sicherheitsanforderungen zur Risikobegrenzung unserer Produkte ist das Ergebnis von Teamarbeit. Jedes Teammitglied von Dräger ist sich der Risiken in unserer stark vernetzten Welt bewusst. Darüber hinaus verfügen unsere Teammitglieder über die Ausbildung, um diese Risiken zu neutralisieren und robustere Sicherheit in das Medizinprodukt einzubauen. Zur kontinuierlichen Verbesserung der Sicherheitsschulung haben wir ein mehrstufiges Schulungskonzept etabliert, das eine fundierte Ausbildung ermöglicht.

Die Dräger Product Security Engineers sind verpflichtet, über aktuelle Sicherheitsthemen und -entwicklungen auf dem Laufenden zu bleiben, damit Dräger nicht von plötzlichen Vorfällen überrascht wird, die die Sicherheit unserer Kunden gefährden.

DESIGN

Sicherheit gehört von Anfang an zu den Produktanforderungen im Designprozess. Eine durchdachte Sicherheitsarchitektur ist die Grundlage für die Widerstandsfähigkeit und den sicheren Betrieb unserer Produkte. Auch wenn Schwachstellen nie komplett ausgeschlossen werden können, investieren wir enormen Aufwand in die Sicherung unserer Geräte, damit sie den Risiken in einer vernetzten Umgebung standhalten.

Mit unseren zehn Leitprinzipien für Cybersicherheit sorgen wir dafür, dass die Sicherheit bei jeder Gestaltungsentscheidung berücksichtigt wird. Diese Gebote enthalten die zehn wichtigsten Punkte, die bei der Integration von Cybersicherheit in unsere Produkte und Systeme zu beachten sind. Unsere Produkte sollen:

– nicht mit abgekündigten, nicht unterstützten oder anfälligen Komponenten geliefert werden (oder auf diese angewiesen sein)
– mit den geringstmöglichen Berechtigungen arbeiten
– standardmäßig im sichersten Zustand geliefert werden
– nicht mit hartcodierten Anmeldeinformationen geliefert werden
– von Anfang an über eingebaute Sicherheit verfügen
– widerstandsfähig gegen unerwartete Eingaben über jede ihrer Schnittstellen sein
– so gestaltet sein, dass Daten im Ruhezustand und während der Übertragung geschützt sind
– keine versteckten Hintertüren, Debug-Ports oder unnötige Software haben
– darauf ausgelegt sein, Sicherheitspatches zu erhalten
– kritische Funktionen vor unbefugtem Zugriff schützen

Wir stellen sicher, dass unsere Produkte und Systeme auf diese Weise für das gewünschte Sicherheitsniveau ausgelegt sind. Wir erstellen Bedrohungsmodelle – also eine Analyse des Systems aus Sicht eines Angreifers –, indem wir Best Practices befolgen. Wir ermitteln auch mögliche Motive und nutzen das STRIDE1-Framework, um mögliche Sicherheitsschwachstellen und -probleme zu identifizieren. Dadurch können Sicherheitsbedrohungen frühzeitig in der Entwicklungsphase der Systeme bewertet und abgeschwächt werden.

ENTWICKELN

Ein Papier zur Sicherheitsproduktarchitektur zu schreiben, garantiert noch keine sichere Entwicklung eines Produkts oder Systems. Sicherlich hilft die Dokumentation, die Gefährdung durch Schwachstellen im Produkt oder System zu minimieren, wenn es

gemäß den Anforderungen entwickelt wird. Sie kann jedoch nicht verhindern, dass Schwachstellen während der Entwicklungsphase im System entstehen. Steve McConnell gibt an, dass der Branchendurchschnitt bei 15 bis 50 Programmierfehlern pro 1.000 Zeilen Quellcode liegt. Die meisten dieser Fehler haben keinen Einfluss auf die Sicherheit des Produkts oder Systems, aber einige führen zu Sicherheitslücken. Diese Bandbreite an Schwachstellen von Pufferüberläufen bis hin zu Cross-Site-Scripting, von Denial-of-Service-Fehlern bis hin zu fehlerhaften Zugriffskontrollen sind immer noch in vielen Produkten und Systemen vorhanden. Wir haben mehrere Schritte unternommen, um die Anzahl dieser Sicherheitslücken zu minimieren.

Bei Dräger wird keine Codezeile ungeprüft ausgeliefert. In den meisten unserer Teams wird das Vier-plus-Eins-Prinzip (4+1) befolgt: Vier (4) ist die Mindestanzahl von Personen, die den gelieferten Code in Peer-to-Peer- oder Gruppen-Code-Reviews gesehen, überprüft und genehmigt haben. Plus eins (+1) steht für die statische Codeanalyse-Software, mit der wir Code auf automatisch erkennbare Fehler überprüfen.

Durch diese Anstrengungen können wir die Anzahl der Sicherheitslücken auf ein Minimum reduzieren.

ÜBERPRÜFEN / TESTEN

In der Phase der Codeverifizierung stellen wir sicher, dass das neu entwickelte oder verbesserte Produkt oder System so funktioniert wie in der Entwurfsphase vorgesehen. Dabei liegt der Schwerpunkt nicht nur auf der eigentlichen Funktionalität, sondern auch auf den Sicherheitsfunktionen. Als Teil des Verifizierungs- und Freigabeprozesses verwenden wir auch eine Reihe systematischer Testmethoden wie Fuzz-Testing von Eingängen und Schnittstellen, automatisierte Schwachstellen-Scanner und statische Code-Analyse-Software.

Als letzte Stufe der Prüfung und Verifizierung beauftragen wir unabhängige externe Sicherheitsexperten mit der Durchführung von Penetrationstests an unseren medizinischen Geräten und Systemen. Bei diesen Tests versuchen professionelle White-Hats, in das medizinische Gerät oder System einzudringen, ohne von dem Hintergrundwissen der Dräger-Entwickler, gepaart mit ihrer hohen Expertise in Hardware- und Software-Sicherheitstechnologie, beeinflusst zu werden. Sollten Schwachstellen gefunden werden, können wir diese beheben, bevor das Medizingerät oder -system auf den Markt kommt. Diese Tests sind auch eine unabhängige Bestätigung für die Zuverlässigkeit unserer Produkte und des ›Dräger Secure Development Life Cycle‹ – und ein Qualitätsnachweis für Sie als Kunde.

FREIGABE

Nachdem unser Team die Verifizierungen abgeschlossen hat und die Korrekturen vorgenommen und erneut verifiziert wurden, führt das Software-Engineering-Team die Freigabephase unserer Produkte durch: Die Dräger-Produkt- und Systemdokumentation wird finalisiert und eine Software-Stückliste (Software Bill of Material / SBOM) erstellt. Darüber hinaus verknüpft die SBOM die Versionen der Softwarekomponenten mit dem Dräger-spezifischen Release und ermöglicht uns eine effektive Schwachstellenüberwachung. Der endgültige Software-Build wird eingefroren und zusammen mit der Dokumentation gebündelt, signiert, um unbefugte Änderungen zu verhindern, und zur Verteilung an unsere Kunden freigegeben.

RODUKTWARTUNG UND ÜBERWACHUNG AUF SICHERHEITSLÜCKEN

Wir wissen, wie wichtig es ist, öffentliche Informationen über Schwachstellen aufmerksam zu beobachten. Unser Produktsicherheitsteam überprüft kontinuierlich eine Vielzahl von Informationsquellen auf veröffentlichte Sicherheitsschwachstellen in Komponenten von Drittanbietern und ordnet diese den möglicherweise betroffenen Dräger-Produkten zu.

Zu unseren Quellen gehören die National Vulnerability Database (NVD), die CVE-Liste von MITRE, VulnDB sowie verschiedene herstellerspezifische RSS-Feeds, Mailinglisten und Websites. Darüber hinaus ist Dräger Mitglied der ›Allianz für Cybersicherheit‹, die aktuelle Informationen zu Bedrohungen und Schwachstellen bereitstellt.

[1] STRIDE-Sicherheit ist das Kürzel für sechs Bedrohungskategorien: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service und Elevation of Privilege.

Wir unterhalten eine Produktsicherheitsseite unter

HTTPS://draeger.com/security

um Kontaktdaten und Informationen zu den Verfahren bereitzustellen, die beim Testen und Melden von Schwachstellen oder Sicherheitsproblemen zu befolgen sind. Auf dieser Seite finden Sie auch Informationen zu den Verfahren, die nach einem Vorfall und öffentlichen produktbezogenen Sicherheitshinweisen einzuhalten sind.

6. SCHLUSSBEMERKUNG UNSERES CHIEF PRODUCT SECURITY OFFICER SECURITY OFFICER

Dräger ist sich seiner Verantwortung gegenüber Patienten und Krankenhäusern zutiefst bewusst. Deshalb arbeiten mein Product Security Team und ich leidenschaftlich daran, sicherzustellen, dass Cyber-Angriffe auf Krankenhäuser nicht die Versorgung der Patienten oder die Integrität der Patientendaten auf unseren medizinischen Geräten und Systemen beeinträchtigen. Als Spezialisten für die Intensivpflege unterstützen wir Sie und Ihr Krankenhaus dabei, unsere medizinischen Geräte sicher in Ihren Netzwerken zu betreiben.

Wir haben es uns zur Aufgabe gemacht, Best Practices für Cybersicherheit in unsere Lösungen zu implementieren, um branchenführenden Schutz und Sicherheit zu bieten. Auf diesem Weg streben wir danach, das vernetzte Gesundheitswesen von morgen sicherer zu machen. Unsere persönlichen Werte wie Ehrlichkeit, Integrität, Professionalität und gegenseitiger Respekt spielen dabei eine zentrale Rolle. Dafür stehen ich und mein Team.

Jeff Moore, Chief Product Security Officer

Discover more on our website https://www.draeger.com/cybersecurity

IMPRINT

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

www.draeger.com

9111147