Nur für Sie bestimmt

Cybersicherheit und Datenschutz für CardioSoft™ Belastungs-EKG Arbeitsplatz

CardioSoft ist der sicherste Belastungs-EKG Arbeitsplatz, den wir je gebaut haben. Es soll Patienten und Anbietern die Gewissheit geben, dass ihre Informationen sicher und geschützt sind.

gehealthcare.com

Medizinische Cybersicherheit ist mehr als nur Virenschutz

Der Schutz unserer Einrichtungen, Mitarbeiter und Patienten erfordert mehr als nur Virenschutz. Er erfordert Strategie und Zusammenarbeit. Durch die Zusammenarbeit können wir nicht nur einzelne Geräte schützen, sondern auch die allgemeine Systemsicherheit.

Das Grundgerüst

Bei der Entwicklung des CardioSoft-Systems haben wir einen umfassenden Ansatz für die Cybersicherheit entwickelt:

- Patientendaten und Produktsicherheit
- Stetige Wachsamkeit aus Sicherheitsgründen
- Kundenkommunikation
- Der strategische Ansatz von GE Healthcare, bekannt als DEPS (Design Engineering for Privacy and Security), bei dem Datenschutz und Sicherheit im Zentrum der Designtechnologie stehen, sowie Softwareentwicklungsreife

Aufrechterhaltung der Patientendaten-sicherheit

Der Schutz der Systeme vor Malware und anderen Angriffen ist ein Teil der Systemsicherheit, wobei es jedoch auch wichtig bleibt, die in diesem System gespeicherten Patienteninformationen zu schützen.

Schritt 1: Verschlüsselung der Patientendaten

Schritt 2: Benutzername und Passwort-Authentifizierung

Als zusätzliche Sicherheitsstufe bietet CardioSoft die Möglichkeit, einen Benutzernamen und ein Kennwort zu erstellen.

Sicherheitsprotokollierung

CardioSoft überwacht und zeichnet nützliche, sicherheitsrelevante Aktivitäten auf. Dies umfasst Benutzeranmeldungen, Netzwerkverbindungen usw. Im unwahrscheinlichen Fall einer Sicherheitsverletzung können wir diese Informationen verwenden, um zwei wichtige Dinge zu bestimmen:

- Wie kam es zum Verstoß und welcher Schaden könnte angerichtet worden sein.
- Wie kann ein ähnlicher Verstoß bei zukünftigen Sicherheitsupdates des Systems verhindert werden.

Mit diesen Informationen können Benutzer die Sicherheitsfunktionen des CardioSoft-Systems voll ausnutzen.

Produktsicherheit

Zum Schutz der Patientendaten muss das System vor Malware und anderen Angriffen auf Softwaredienste geschützt werden.

Minimieren der Angriffsfläche

Ein Schlüsselprinzip ist die Minimierung der Teile des Systems, die Bedrohungen ausgesetzt sind. Bei CardioSoft werden Softwaredienste, die in das Betriebssystem eingebettet sind und nicht explizit zum Ausführen der medizinischen Anwendungen benötigt werden, entfernt oder deaktiviert. Kurz gesagt, lässt eine geringere Anzahl an Netzwerkfunktionen potenziellen Angreifern weniger Möglichkeiten.

Immer auf dem neuesten Stand

Eine der einfachsten Möglichkeiten, ein Computersystem zu schützen, besteht darin, sicherzustellen, dass die letzten Sicherheitsupdates für das Betriebssystem installiert sind.

Lassen Sie bei Interaktionen Vorsicht walten

Bei der Installation von CardioSoft wird empfohlen, eine Firewall zu verwenden, um unerwünschten Netzwerkverkehr zu blockieren. CardioSoft-Besitzer können einschränken, welche Netzwerkgeräte eine Verbindung herstellen können und Geräte blockieren, die unbekannt und möglicherweise unsicher sind.

Stetige Wachsamkeit aus Sicherheitsgründen

Wie Sie sehen, haben wir viel getan, um das CardioSoft-System sicherer zu machen, aber die Sicherheitswelt entwickelt sich ständig weiter, sodass wir wachsam bleiben müssen.

Überwachung und Ausmachen neuer Bedrohungen

Einer der Vorteile eines großen Unternehmens wie GE Healthcare ist, dass wir ein starkes zentrales Sicherheitsteam haben, das ständig nach neuen Sicherheitsbedrohungen Ausschau hält. Dieses zentrale Team steht in regelmäßigem Kontakt mit unseren Ingenieuren für diagnostische EKGs, um bei Bedarf die richtigen Maßnahmen zur Behebung von Sicherheitslücken zu ergreifen.

Sicherheits-Patches

Wenn neue Sicherheits-Patches benötigt werden, werden Sie von GE über deren Verfügbarkeit informiert.

Kundenkommunikation

Cybersicherheit und Datenschutz sind ein Mannschaftssport. Wir tun alles, um Sicherheitsbedrohungen abzuwehren.

Handbuch zu Datenschutz und Sicherheit

Wir veröffentlichen die technischen Details unserer Sicherheitselemente als Teil des CardioSoft-Benutzerhandbuchs und der Wartungsunterlagen.**

MDS2-Formular

Der MDS2-Fragebogen bietet Antworten auf eine Liste von Standardsicherheitsfragen, die für Cybersicherheitsexperten wichtig sind und branchenweit verwendet werden.*

Softwareentwicklungsreife

Da Sicherheit für alle von uns entwickelten Produkte grundlegend ist, können wir Produkte intelligenter und sicherer machen.

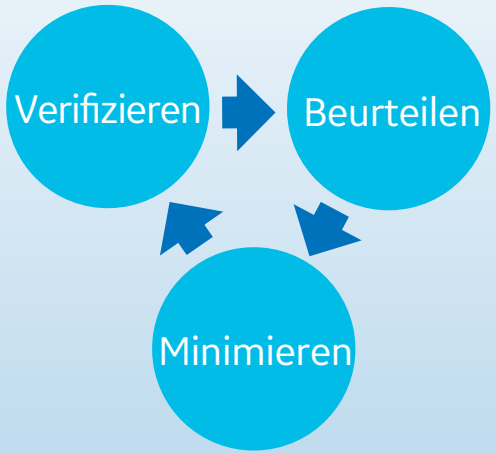
Dies beginnt bei den Softwareentwicklern

Unsere talentierten Softwareingenieure sind mit modernsten Software-Engineering-Tools ausgestattet und auf Sicherheitsfragen geschult. Darüber hinaus überwacht das zentrale Cybersicherheitsteam von GE ständig, ob neue Bedrohungen vorliegen und schult das Ingenieurspersonal anhand dieser Informationen.

Ein System der gegenseitigen Kontrolle

Mithilfe von Tools, die sich mit der von unseren Ingenieuren erstellten Software befassen, prüfen wir, ob Schwachstellen vorliegen, durch die die Software für Risiken anfällig wird.

Schließlich überprüfen unsere erfahrensten Ingenieursteammitglieder die Software sowohl auf architektonischer als auch auf Implementierungsebene. Auch in der Cyberwelt besteht noch ein Bedarf an menschlichem Fachwissen.



*Verfügbar auf Anfrage. Wenden Sie sich an Ihren GE-Vertriebsmitarbeiter vor Ort.

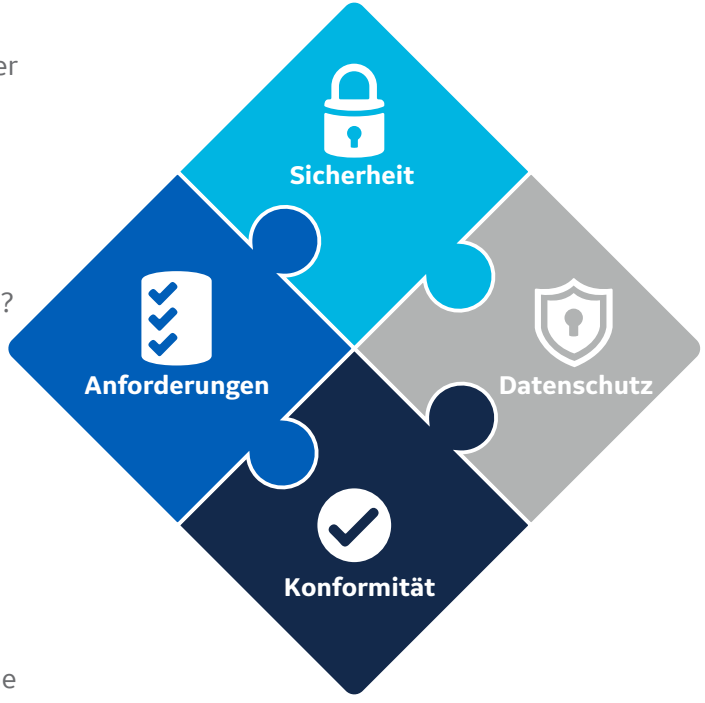
DEPS – Ein umfassender Sicherheitsansatz

Design Engineering for Privacy and Security ist der strategische Rahmen, den GE für alle seine Produkte, einschließlich CASE, festgelegt hat.

DEPS beginnt mit der Bewertung des mit der Verwendung des Systems verbundenen Risikos und gibt dem Ingenieursteam Anleitungen zur Implementierung angemessener Sicherheits- und Datenschutzkontrollen, indem Fragen gestellt werden wie:

- Ist ein Fernzugriff möglich?
- Sind Designelemente mit der Cloud verbunden?
- Handelt es sich um ein mobiles Gerät?
- Sammelt, verwendet oder speichert es persönliche Gesundheitsinformationen?
- Wird es in medizinischen Notsituationen eingesetzt (niedrige Zugangsbarrieren)?
- Ist eine hohe Verfügbarkeit erforderlich?
- Ist die Datenintegrität für die Patientenversorgung von entscheidender Bedeutung?
- Gibt es eine drahtlose Verbindung?
- Wird es zwischen mehreren Standorten hin- und hertransportiert?
- Besitzt es Wechselmedien wie USB-Sticks?

Diese Bewertung hilft zu identifizieren, welches Sicherheitsniveau erforderlich ist. Im Fall von CardioSoft lautet die Antwort auf viele dieser Fragen „Ja“, sodass das System als System mit hohem Sicherheitsrisiko behandelt wird. Zudem haben wir eine Vielzahl von Kontrollen eingeführt, um den notwendigen Schutz zu gewährleisten.



Imagination at work

JB66792XXb