



Schutz vor fremden Blicken

Cybersicherheit und Datenschutz beim MAC™ 5
Elektrokardiographie-System

Der MAC 5 baut auf der sichersten Ruhe-EKG-Plattform auf, die wir je entwickelt haben. Bei seiner Entwicklung wurde besonderer Wert auf den Datenschutz gelegt, damit sich Patienten und medizinische Dienstleister um den Verbleib ihrer Daten keine Sorgen machen müssen.

gehealthcare.com



Cybersicherheit in der Medizin bedeutet mehr als lediglich Schutz vor Computerviren

Der Schutz unserer Einrichtungen, unseres Personals und der Patienten geht weit über Schutzmaßnahmen gegen Viren hinaus. Er erfordert Strategie und Zusammenarbeit. Eine gute Zusammenarbeit ermöglicht neben dem Schutz der einzelnen Geräte auch die Sicherheit des gesamten Systems.

Der Rahmen

Für das Design des MAC 5 EKG-Systems haben wir einen umfassenden Ansatz im Hinblick auf die Cybersicherheit verfolgt:

- Ein strategisches GE Healthcare Gesamtkonzept mit der Bezeichnung DEPS (Design Engineering for Privacy and Security)
- Ausgereifte Softwareentwicklung
- In der Konzeption berücksichtigte Produktsicherheit
- Kontinuierliche Sicherheitsüberwachung
- Kommunikation mit Kunden

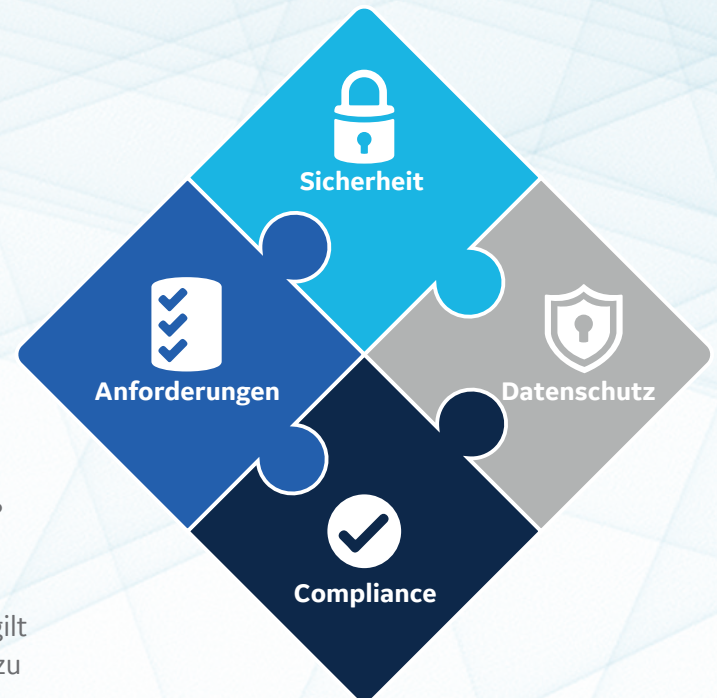
DEPS – ein umfassendes Sicherheitskonzept

Design Engineering for Privacy and Security (DEPS) ist die Bezeichnung des strategischen Rahmens, den sich GE für alle seine Produkte einschließlich MAC 5 gesteckt hat.

DEPS beginnt mit der Einschätzung, der mit der Systemnutzung verbundenen Risiken und liefert dem Entwicklungsteam Anweisungen zur Implementierung geeigneter Sicherheits- und Datenschutzkontrollen. Hierzu werden Fragen gestellt wie:

- Ist der Fernzugriff möglich?
- Sind Elemente des Systems mit der Cloud verbunden?
- Handelt es sich um ein mobiles Gerät?
- Werden auf dem Gerät persönliche Gesundheitsinformationen erfasst, verwendet oder gespeichert?
- Wird es in medizinischen Notfällen (mit weniger strengen Zugriffskontrollen) verwendet?
- Ist eine hohe Verfügbarkeit notwendig?
- Ist Datenintegrität für die Patientenversorgung kritisch?
- Ist eine drahtlose Vernetzung des Geräts möglich?
- Wird es zwischen mehreren Abteilungen transportiert?
- Wird es zusammen mit Wechseldatenträgern, wie etwa USB-Sticks verwendet?

Anhand dieser Untersuchung kann das erforderliche Sicherheitsniveau ermittelt werden. Im Falle des MAC 5 lautet die Antwort auf viele dieser Fragen „Ja“. Deshalb gilt es als ein System mit hohem Sicherheitsrisiko. Um ein ausreichendes Schutzniveau zu bieten, haben wir zahlreiche Kontrollen im Gerät eingerichtet.



Ausgereifte Softwareentwicklung

Indem wir die Sicherheit bei allen Entwicklungen als Grundlage voraussetzen, können wir Produkte schaffen, die intelligenter und sicherer sind.

Es beginnt bei der Softwareentwicklung

Unsere kompetenten Softwareentwickler werden mit modernsten Softwareentwicklungstools ausgestattet und speziell im Hinblick auf Sicherheitsaspekte geschult. Zudem ist das zentrale Cybersicherheits-Team von GE damit beauftragt, die Umgebungen auf neue Bedrohungen zu überwachen und die Entwicklerteams über die neuesten Informationen aufzuklären.

Ein System mit vielschichtigen Kontrollen

Mithilfe von Tools, die die von unseren Entwicklern geschaffene Software überprüfen, decken wir mögliche Schwachstellen auf, die die Software anfällig gegenüber Cyberrisiken machen könnte.

Anschließend wird die Software einer Reihe von Tests unterzogen, die Bedrohungen aus der realen Welt simulieren. Werden Risiken festgestellt, nehmen wir entsprechende Korrekturen vor.

Und schließlich prüfen unsere erfahrensten Mitglieder des Entwicklerteams die Software sowohl auf der Architektur- als auch auf Implementierungsebene. Auch die Cyberwelt erfordert menschliches Fachwissen.



Produktsicherheit



Minimierung der Angriffsfläche

Ein Grundprinzip besteht darin, die Teile des Systems zu minimieren, die Bedrohungen ausgesetzt sind. Im Falle des MAC 5 wurden sämtliche im Betriebssystem integrierten Softwaredienste entfernt oder deaktiviert, die nicht ausdrücklich zum Ausführen der medizinischen Anwendungen benötigt werden. Denn weniger Netzwerkfunktionen bedeuten weniger Angriffspunkte für potentielle Cyber-Attacks.



Unverzögliche Aktualisierung

Eine der einfachsten Methoden, um ein Computersystem zu schützen, besteht darin, darauf zu achten, dass stets die jüngste Version des Betriebssystems installiert ist. Wir achten kontinuierlich auf das Auftreten neuer Sicherheitsprobleme und stellen Betriebssystem-Patches und Softwareaktualisierungen bereit, um den MAC 5 zu einem der sichersten EKG-Systeme des Marktes zu machen.



Lassen Sie bei Interaktionen Vorsicht walten

Der MAC 5 nutzt eine Firewall, um ungebetene Netzwerkzugriffe zu unterbinden. Der Betreiber des MAC 5 kann festlegen, welche Geräte über das Netzwerk mit dem System kommunizieren können, und den Zugriff durch unbekannte und potentiell unsichere Geräte verhindern.



Smarterer USB-Anschluss

Der MAC 5 bietet Schutz gegen USB-Attacks: Ein Administrator kann die Verwendung von USB-Ports erlauben/sperrern. Ein Ausführen von auf USB-Speichersticks befindlichen Programmen ist nicht möglich.

Bewahrung der Sicherheit von Patientendaten

Systeme vor Malware- und sonstigen Attacken zu schützen, ist eine Komponente der Systemsicherheit, jedoch ist es ebenso wichtig, die auf dem System gespeicherten Patientendaten zu schützen.



Schritt 1: Patientendatenverschlüsselung

Alle auf dem MAC 5 gespeicherten Patientendaten werden mit Verschlüsselungssoftware von Weltrang verschlüsselt.



Schritt 2: Authentifizierung mittels Benutzername und Kennwort

Als zusätzliche Sicherheitsvorkehrung bietet das MAC 5 EKG-System die Möglichkeit, einen Benutzernamen und ein Kennwort zu erstellen.



Schritt 3: Sichere Netzwerkverbindungen

Der MAC 5 nutzt Single-Sign-On mittels LDAP. Auf diese Weise können Benutzer mit denselben Anmeldedaten auf das System zugreifen, die sie auch für andere Systeme der klinischen Einrichtung verwenden.

Der MAC 5 kommuniziert mit einem standardmäßig sicheren LDAP (LDAPS).

Das MAC 5 EKG-System unterstützt Wireless Security der Enterprise-Klasse, um den Datenverkehr zu schützen.

Sicherheitsprotokollierung

Der MAC 5 überwacht und zeichnet relevante Sicherheitsereignisse auf. Dies gilt für Benutzeranmeldungen, Netzwerkverbindungen usw. Im unwahrscheinlichen Fall einer Sicherheitsverletzung können wir anhand dieser Informationen zwei wichtige Dinge ermitteln:

- Wie kam es zu der Sicherheitsverletzung und welchen Schaden hat sie angerichtet?
- Wie kann eine erneute Sicherheitsverletzung dieser Art durch zukünftige Sicherheitsaktualisierungen des Systems verhindert werden?

Mit diesen Informationen kann der Betreiber die Sicherheitsmerkmale des MAC 5 optimal nutzen.



Kontinuierliche Sicherheitsüberwachung

Wie Sie sehen, haben wir viel für die Sicherheit des MAC 5 EKG-System unternommen; da sich Sicherheitsbelange jedoch ständig weiterentwickeln, müssen wir wachsam bleiben.

Überwachung auf neue Bedrohungen

Einer der Vorteile eines großen Unternehmens wie GE Healthcare liegt darin, dass wir ein solides zentrales Sicherheitsteam haben, das fortwährend nach neuen Sicherheitsbedrohungen Ausschau hält. Dieses zentrale Team steht in regelmäßigem Kontakt zu den Entwicklern unserer EKG-Systeme, sodass das Entwicklungsteam des MAC 5 bei Bedarf zusätzliche Sicherheitspatches herausgeben kann, um mögliche Schwachstellen zu beheben.

Systemwiederherstellungsplan

MAC 5 ist mit einem Sicherheitsprotokollierungssystem ausgestattet, das für die Wiederherstellung nach einer Sicherheitsverletzung äußerst hilfreich sein kann. Anhand der Protokollierungsdaten können die Art der Sicherheitsverletzung und der Schadensumfang ermittelt werden. Sie und Ihre Mitarbeiter sollten jedoch auch über einen Systemschutz- und -wiederherstellungsplan verfügen. Bei der Aufstellung eines solchen Plans sind folgende Aspekte zu berücksichtigen:

- Schützen Sie Ihren EKG-Arbeitsplatz durch sichere Benutzernamen und Kennwörter vor unbefugtem Zugriff. Um einen raschen Zugriff auf das MAC 5 EKG-System zu ermöglichen, können Sie sich auch für begrenzte Sicherheitsmaßnahmen entscheiden. Diese Flexibilität ermöglicht es Ihnen, die Sicherheitsstufe des Systems an Ihre spezifischen Anforderungen anzupassen.
- Sorgen Sie für sichere physische Bedingungen. In manchen Fällen bedeutet dies, dass das System an einem Ort mit Zugangsbeschränkung aufbewahrt wird, sodass unbefugte Nutzer keinen Zugang zum System erhalten.
- Konfigurieren Sie Ihr System so, dass EKG- und Patientendaten sofort nach jeder Untersuchung in Ihr MUSE™- oder ePA-System übertragen werden und löschen Sie lokale Kopien. So brauchen Sie Patientendaten nur an einem Ort zu schützen, statt an zwei.
- Speichern Sie die Konfigurationseinstellungen des MAC 5 auf Sicherungsmedien, um das Setup von weiteren MAC 5 Systemen zu erleichtern.

Kommunikation mit Kunden

Cybersicherheit und Datenschutz sind auf gute Teamarbeit angewiesen. Wenn die Besitzer und Entwickler von MAC 5 EKG-Systemen zusammenarbeiten, können wir Ihnen zusichern, dass wir alles in unserer Macht Stehende unternehmen werden, um Sie vor Sicherheitsbedrohungen zu schützen.

Kommunikationsplan für MAC 5 Besitzer und Entwickler



Handbuch zu Datenschutz und Sicherheit

Wir veröffentlichen die technischen Details zu unseren Sicherheitselementen in der Bedienungsanleitung und Wartungsdokumentation des MAC 5. Um bei Bedarf ein Exemplar anzufordern, wenden Sie sich an den zuständigen GE-Kundendienst.



MDS2-Formular

Der MDS2-Fragebogen liefert Antworten auf eine Liste von Standardsicherheitsfragen, die für die Cybersicherheit eine wichtige Rolle spielen und branchenweit Anwendung finden.

Eine spezielle Version für MAC 5 ist auf Anfrage erhältlich.



Der MAC 5 ist ein medizinisches Gerät mit CE-Kennzeichnung. Der MAC 5 ist nicht in allen Märkten verfügbar und hat keine 510K-Zulassung.*
Diese Funktion wird in China nicht unterstützt.

© 2022 General Electric Company – Alle Rechte vorbehalten.

GE Healthcare behält sich das Recht vor, die genannten Spezifikationen und Funktionen zu einem beliebigen Zeitpunkt und ohne vorherige Ankündigung oder Verpflichtung zu ändern oder die Herstellung der Produkte einzustellen. Aktuelle Informationen und Auskünfte zur Verfügbarkeit erhalten Sie von Ihrer GE-Healthcare-Vertriebsniederlassung. GE, das GE-Monogramm, MAC und MUSE sind Marken der General Electric Company. GE Healthcare, ein Geschäftsbereich der General Electric Company.

JB01784DE

