Hippokratischer Eid für vernetzte medizintechnische Geräte

Ich werde das menschliche Leben ehren und schützen und stets zum Nutzen meiner Patienten handeln. Ich erkenne an, dass alle Systeme versagen können; das Auftreten von Defekten des Systems und widrigen Umständen kann nicht verhindert werden. Ressourcen, die das Leben verbessern oder erhalten sollen, können es auch schädigen oder beenden. Wenn Fehlfunktionen die Sicherheit von Patienten beeinträchtigen, muss deren Versorgung widerstandsfähig gegenüber versehentlicher und bösartiger Manipulation sein. Jeder, der eine Funktion im Gesundheitssystem innehat, trägt gemeinsam mit allen anderen die Verantwortung: Als jemand, der das Leben zu erhalten und zu verbessern sucht, darf ich an erster Stelle keinen Schaden anrichten.

Um dieses Ziel zu erreichen, schwöre ich, nach bestem Wissen und Gewissen die folgenden Prinzipien zu befolgen :

1. Konstruktive Cybersicherheit: *Ich respektiere die Fachkenntnisse derer, die vor mir kamen.* ***Ich werde beim Design den Security-Lebenszyklus, die Widerstandsfähigkeit gegenüber Angreifern und sichere Lieferketten berücksichtigen.***
2. Zusammenarbeit mit Dritten: *Ich bin mir bewusst, dass Sicherheitslücken auch mit gewissenhaften Anstrengungen nicht zu vermeiden sind.* ***Ich werde zur Meldung von potenziellen Sicherheitsproblemen ermutigen, die im guten Glauben übermittelt werden.***
3. Sammeln von Daten und Belegen: *Ich werde mich auf unerwartete Ereignisse vorbereiten.* ***Ich werde die Sammlung und Speicherung von Daten und Nachweisen sowie deren Analyse ermöglichen, um daraus Lehren hinsichtlich der Sicherheit der Geräte zu ziehen.***
4. Widerstandsfähigkeit und Eindämmung von Schäden: *Ich erkenne an, dass Fehlfunktionen von Komponenten und in der Umgebung unvermeidlich sind.* ***Ich werde Elemente, die für die Patientenversorgung unverzichtbar sind, unter widrigen Umständen besonders schützen und einen sicheren Zustand mit klaren Zustandsanzeigen aufrechterhalten, wenn eine Fehlfunktion nicht abgewendet werden kann.***
5. Cybersicherheitsupdates: *Ich verstehe, dass Cybersicherheit einem steten Wandel unterworfen ist.* ***Ich werde zeitnahe, agile und sichere Updates unterstützen.***

⚕ Konstruktive Cybersicherheit

Ich respektiere die Fachkenntnisse derer, die vor mir kamen. ***Ich werde beim Design den Security-Lebenszyklus, die Widerstandsfähigkeit gegenüber Angreifern und sichere Lieferketten berücksichtigen.***

Sichere Ergebnisse sind das Resultat systematischer Zielorientierung im gesamten Lebenszyklus eines Gerätes; sie können nicht dem Zufall überlassen werden. Jene, deren Leben und Lebensunterhalt von der Zuverlässigkeit medizinischer Geräte abhängt, sollten in die Lage versetzt werden, das Ausmaß dieser Sicherheit bei Design und Entwicklung der Geräte selbst zu beurteilen. Reife und Konsistenz im Design von Software, in der Entwicklung, beim Testen und in der Instandhaltung führt zu besserer Qualität und verbesserten Ergebnissen für die Patienten.

- **Norm- und standardbasierte Cybersicherheit.** Bestehende internationale und industriespezifische Standards und Normen für sicheres Design und sichere

Entwicklung von Softwarekomponenten sind hoch ausgereift. Hersteller, die diese adaptieren, können schneller sichere Prozesse in der Softwareentwicklung etablieren. Es existiert kein einzelner allgemein anerkannter Standard, aber bewährte Verfahrensweisen können bei der Ausreifung eines Programmes helfen und die Basis darstellen, um später einen bestimmten Standard oder ein Framework zu übernehmen.

- **Analyse der Widerstandsfähigkeit gegenüber Angreifern.** Bei ansonsten identischen Voraussetzungen hat eine gründlich geprüfte Komponente oder ein gründlich geprüftes System weniger unbekannte Mängel oder Sicherheitslücken. Bedrohungsanalysen, Sicherheitstests und andere auf *Safety* basierenden Praktiken der Cybersicherheit helfen, mögliche Fehlfunktionen und den Missbrauch durch Angreifer zu berücksichtigen. Beurteilungen sollten durch qualifiziertes Personal vorgenommen werden und unabhängig von Design und Entwicklung sein.
- **Vermeidung von ungeschütztem Remote-Zugang.** Fähigkeiten und Funktionen, die in den Händen qualifizierter Personen Leben retten können, können dieses Leben durch Versehen oder in den Händen von Angreifern in Gefahr bringen. Hartkodierte, wiederverwendete Zugangsdaten (Passwörter, Schlüssel etc.) und undokumentierte Zugänge können dazu führen, dass Therapien durch nicht vertrauenswürdige Befehle, Informationen oder Personen beeinflusst werden. Ein offener Remote-Zugang kann zu einer großflächigen Unfall- und Angriffsgefahr werden. Dort, wo eine solche Risikolage besteht, müssen entsprechende Maßnahmen getroffen werden, um Schaden zu verhindern.
- **Konsequenz in der Lieferkette.** Verantwortungsvoll verwaltete, nachvollziehbare Hardware- und Software-Lieferketten führen zu vorhersehbarer Qualität und Herkunft von Gerätekomponenten. Eine vertrauenswürdige Lieferkette ermöglicht eine bessere Widerstandsfähigkeit und agilere Reaktionen auf Unfälle und Angriffe. Handelsübliche Hardware- und Software-Lösungen, wenn sie nach entsprechend konsequenten Kriterien ausgewählt wurden, können die Verlässlichkeit erhöhen, die Kosten senken und die Zeit zur Marktreife verkürzen.
- **Vermeidung bekannter Fehler.** Software-Komponenten von Dritten, die bekannte Sicherheitslücken haben, sollten zugunsten weniger anfälliger Lösungen vermieden werden, wenn die Funktion darunter nicht leidet. Es sollte in Betracht gezogen werden, eine Liste der verwendeten Materialien als Begleitdokumentation anzubieten, sodass Stakeholder ihre eigenen Entscheidungen bezüglich eines akzeptablen Risikolevels fällen können, auch über die erwartete Lebenszeit des Geräts hinaus.
- **Geteilte Verantwortlichkeiten.** Das Ergebnis jeder Therapie ist eine Kombination der Funktionen des Geräts und ihrer Anwendung durch die betreuende Person in der jeweiligen Umgebung. Die beste Patientenversorgung wird erreicht, wenn die speziellen Fähigkeiten sowohl des Geräts als auch des Anwenders genutzt werden. Wenn keine expliziten Vorgaben gemacht werden, werden die Anwender nur durch glücklichen Zufall die beste Umgebung für die Anwendung des Geräts schaffen. Die erwarteten Einsatzbedingungen eines Geräts sollten daher klar kommuniziert werden, ebenso wie bekannte Umstände, die zu Fehlfunktionen führen, Betriebsanforderungen, Designannahmen, Elemente der Architektur, Referenz-Umsetzungsrichtlinien , spezifische Warnungen oder Verbote und andere wichtige Informationen.

$ Zusammenarbeit mit Dritten

Ich bin mir bewusst, dass Sicherheitslücken auch mit gewissenhaften Anstrengungen nicht zu vermeiden sind. ***Ich werde zur Meldung von potenziellen Sicherheitsproblemen ermutigen, die im guten Glauben übermittelt werden.***

I Am The Cavalry

Die Erkennung von Fehlern in Software, bevor sie sicherheitsrelevant werden, verschafft den Verteidigern einen Vorteil. Hersteller mit der Fähigkeit, derartige Fehler früh entgegenzunehmen und abzuklären tragen weiter zu diesem Vorteil bei. Diejenigen, die Berichte über Fehler aus unabhängigen Quellen ermutigen und Konsequenzen aus diesen ziehen, können Kosten und negative Aufmerksamkeit reduzieren, und zwar über das Maß hinaus, das allein durch interne Revision möglich ist. Wertschöpfung aus der Zusammenarbeit zwischen Forschern und Herstellern hat dazu geführt, dass Hersteller Forschung durch Anerkennungs- und Belohnungsprogramme fördern.

- **Norm- und standardbasiert**. Veröffentlichte Richtlinien, Strategien und Programme in der Softwareindustrie können als effektive Beispiele für die Hersteller von Medizintechnik dienen. Die Nutzung bewährter Standards (beispielsweise der FDA Consensus Standards wie ISO 30111 und ISO 29147) und Praktiken beschleunigen die Reifung einer Organisation und stellen vorhersehbare und normierte Schnittstellen für Problemberichte sicher.
- **Existierende Mechanismen**. Die Verwendung existierender Prozesse und Strukturen verkürzt die benötigte Zeit, ein effektives Programm zu entwickeln, verbessert die Beteiligung und verringert die Verwaltungslast. Bereits implementierte Prozesse und Richtlinien für das Entgegennehmen von und die Antwort auf sicherheitsrelevante Meldungen können auch für die Meldung von potenziellen Cybersicherheits- oder Datenschutzvorfällen übernommen werden.
- **Bekannte Schnittstellen**. Externe Koordinatoren für die Meldung von Sicherheitslücken haben die Schnittstellen zwischen Herstellern und Forschern normiert. Dies vermittelt Vertrauen auf allen Seiten und verringert den benötigten Aufwand.
- **Schaffung von Anreizen.** Patientensicherheit sollte im Interesse aller Beteiligten liegen. Positive Anreize, beispielsweise in der Form von Anerkennung und finanziellen Prämien, führen zu früherer und qualitativ höherwertiger Berichterstattung. Das verringert Kosten, Zeitaufwand und negative Außenwirkung bei der Eliminierung von Sicherheitslücken. Gleichzeitig beeinträchtigt es die Möglichkeiten der Angreifer, die Ergebnisse ihrer Attacken finanziell zu verwerten. Durch negative Anreize können diese Effekte nicht für Patienten und das Gesundheitssystem nutzbar gemacht werden.

⚕ Sammeln von Daten und Belegen

Ich werde mich auf unerwartete Ereignisse vorbereiten. ***Ich werde die Sammlung und Speicherung von Daten und Nachweisen sowie deren Analyse ermöglichen, um daraus Lehren hinsichtlich der Sicherheit der Geräte zu ziehen.***

Sicherheitsuntersuchungen und die Aufzeichnung des Betriebs von Geräten machen unerwartete Ergebnisse sichtbar. Diese Belege können Fehlerursachen offensichtlich machen, seien es Fehlfunktionen, Designfehler, menschliches Fehlverhalten oder böswillige Angriffe. Ohne Belege bleiben die Ursachen unerwünschter Ereignisse unklar, und Gegenmaßnahmen basieren nur auf Spekulationen.

- **Unabhängige Überprüfbarkeit**. Unabhängige Überprüfung von Gerätefehlern oder Sicherheitsberichten ermöglichen den Beteiligten, unerwünschte Ereignisse zeitnah zu untersuchen und somit die Transparenz der Ergebnisse zu verbessern und Verantwortlichkeiten nachzuvollziehen. Hersteller sollten Richtlinien bereitstellen, um

Untersuchungen durch Organisationen der Gesundheitsversorgung, spezialisierte Dienstleister, Forscher und Agenturen zu unterstützen.

- **Manipulationssichere, forensisch belastbare Belege.** Logbücher und andere Informationen über unerwartete Ereignisse sollten rechtsverwertbar abgelegt sein, sodass Veränderungen daran verhindert oder rückverfolgbar erkannt werden können.
- **Berücksichtigung von Vertraulichkeit und Datenschutz**. Sicherheitsuntersuchungen sind auf Aufzeichnungen angewiesen, welche die Folgen einer Fehlfunktion festhalten. Die Vorteile dieser Aufzeichnungen können genutzt werden, ohne zu Datenschutz- und Überwachungsproblemen zu führen, indem Sicherheits- und Integritätsaufzeichnungen von Patientendaten entkoppelt werden.
- **Anwendung neu gewonnenen Wissens.** Das Verstehen der Ursachen von Sicherheitslücken, Fehlfunktionen und Schäden ist zwar notwendig, um diese zu beheben, dies ist jedoch nur der erste Schritt. Die hier gewonnenen Einsichten müssen auf alle Aspekte der Medizintechnik und Patientenversorgung zurückwirken und sollten zur Förderung des Gemeinwohls mit der medizinischen Gemeinschaft geteilt werden.

⚕ Widerstandsfähigkeit und Eindämmung von Schäden

Ich erkenne an, dass Fehlfunktionen von Komponenten und in der Umgebung unvermeidlich sind. ***Ich werde Elemente, die für die Patientenversorgung unverzichtbar sind, unter widrigen Umständen besonders schützen und einen sicheren Zustand mit klaren Zustandsanzeigen aufrechterhalten, wenn eine Fehlfunktion nicht abgewendet werden kann.***

Medizintechnik ermöglicht Patientenversorgung in Form eines Systems aus voneinander abhängigen Systemen. Diese Komplexität führt zu Stärken, die jedoch nicht dazu führen sollten, dass Patienten in Gefahr geraten. Einzelne Systeme müssen unabhängig vom Status anderer Systeme sicher betrieben werden können. Fehlfunktionen sollten sichtbar sein, abhängige Eingaben sollten validiert und Ausgaben geschützt werden.

- **Minimale, ausgewählte Angriffsfläche.** Vernetzung kann eine Voraussetzung für wichtige Funktionen von Medizingeräten sein, erhöht jedoch auch die Angriffsfläche gegenüber gefährlichen Bedingungen im Umfeld und Angreifern. Solche Arten von Exposition, die die Funktion des Geräts nicht wesentlich verbessern, erhöhen lediglich die Zugriffsmöglichkeiten für Angreifer (beispielsweise NFC gegenüber Bluetooth bei der Programmierung von Implantaten). Es sollten daher sicherere und preiswertere Designs angestrebt werden, die diese Angriffsfläche minimieren.
- **Isolation und Aufteilung.** Unerwartete oder feindliche Interaktionen zwischen Medizingeräten und ihrer Umgebung führen mit größerer Wahrscheinlichkeit zu Schäden, als erwartbare und gut dokumentierte Interaktionen. Sicheres Design und sichere Implementierung haben zum Ziel, Komponenten und Systeme von Angreifern und unerwarteten Umgebungsbedingungen abzuschirmen.
- **Absicherung und Sichtbarkeit von Fehlfunktionen**. Fehlfunktionen sollten Patienten keinem unnötigen Schadensrisiko aussetzen und sollten klar sichtbar sein. Unerwartete Betriebszustände oder bekannte Fehlfunktionen sollten einen „Fail Safe“ oder „Safe Mode“ auslösen, der verhindert, dass die Fehlfunktion eines Geräts oder einer Softwarekomponente sich im System ausbreitet. Beteiligte sollten auf Indikatoren und bekannte Umstände, die zu Fehlerzuständen führen können, hingewiesen werden.

- **Vertrauenswürdige Eingaben.** Manipulationssichere Technik und solche, mit der eine Manipulation klar nachgewiesen werden kann, schützt gegen falsche überlebensrelevante Entscheidungen oder Handlungen, die auf nicht vertrauenswürdigen Informationen beruhen (beispielsweise Medikamentendatenbanken, HL7-Codes, Behandlungspläne), im besten Fall mit Echtzeit-Rückmeldungen.
- **Integrität von Patientendaten.** Entscheidungen über Patientenversorgung beruhen auf korrekten Aufzeichnungen über Anamnese, Diagnose und Therapie. Diese Aufzeichnungen sollten gegenüber Manipulation, Verlust und Unvollständigkeit geschützt sein. Mögliche Maßnahmen sind großzügig bemessener Speicherplatz, Bestätigung nach Übertragung, Integritätsvalidierung und Beachtung des Datenschutzes.

⚕ Cybersicherheitsupdates

Ich verstehe, dass Cybersicherheit einem steten Wandel unterworfen ist. ***Ich werde zeitnahe, agile und sichere Updates unterstützen.***

Sobald bekannt ist, dass ein Problem die Patientenversorgung beeinträchtigen könnte, wird sich eine kurze Reaktionszeit positiv auf die Gesundheitsversorgung auswirken. Software-Updates sind schneller und preiswerter als der Austausch von Hardware; automatisierte Remote-Software-Updates sind am effizientesten. Die Zunahme an Angriffsfläche hierbei wird kompensiert durch die Geschwindigkeit und Skalierbarkeit der Korrektur von Fehlern und Sicherheitslücken, die ohne geeignete Maßnahmen zu nachteiligen Ergebnissen in der Patientenversorgung führen könnten.

- **Automatisierung und Dokumentation.** Automatisierte und kontrollierte Update-Prozesse sind weniger anfällig für Fehler, Verzögerungen, böswillige Eingriffe, Fehlinterpretationen und andere Probleme. Die Prozessdokumentation sollte klare Rollenbeschreibungen und Verantwortlichkeiten für alle Beteiligten beinhalten und die Entwicklung von entsprechenden Prozessen in den Stakeholder-Gruppen ermöglichen.
- **Sicherer Update-Prozess.** Prozesse sollten die Authentizität und Integrität von Software-Updates sicherstellen, um bösartige oder unbeabsichtigte Manipulationen zu verhindern. Die Möglichkeit zu Remote-Updates kann zu Kostensenkungen und Vorteilen im Hinblick auf Außenwirkung und Geschwindigkeit führen, wenn sie auf eine bewiesenermaßen geeignete Art implementiert wird.
- **Kommunikation mit Beteiligten.** Kommunikation mit Beteiligten sollte prompt, transparent und ehrlich erfolgen. Hersteller sollten Stakeholder darüber informieren, wann und wo Fehler existieren, sowie über deren Schweregrad, die Inhalte des Updates und die Anleitungen für jede Rolle. Updates können auch lediglich aus Mitteilungen über Umgehungslösungen, Warnungen, unsichere Bedingungen, Beschriftung, Bedienungsanleitungen oder anderen relevanten Informationen bestehen.
- **Unterstützung von Sicherheitsupdates von Software-Abhängigkeiten**. Die Sicherheit von Medizintechnik hängt von der Integrität von Drittanbieter-Software ab. Patientensicherheit darf weder durch Sicherheitslücken dieser Plattformen gefährdet werden noch durch die Anwendung von Updates, um diese zu schließen. Ein geeigneter Verifikationsprozess für entsprechende *off-the-shelf* Software-Updates führt zu schnelleren und agileren Reaktionen.

Wenn die Technologie, von der wir abhängig sind, sich auf die öffentliche Sicherheit und die Sicherheit menschlichen Lebens auswirkt, ist unsere äußerste Aufmerksamkeit und Sorgfalt gefragt. Unsere Medizintechnik verdient diese Art der Aufmerksamkeit. Die hier beschriebenen Fähigkeiten stellen eine Grundlage für Cybersicherheit dar. Menschen in medizinischen Berufen sind Meister in ihrem Bereich, wir Cybersicherheitsforscher sind Meister in unserem. Dort, wo die Bereiche unseres Wissens überlappen, können wir in schneller gemeinsam bessere Ergebnisse erzielen.

Hersteller von Medizintechnik, Organisationen der Gesundheitsversorgung, Ärzte, Patienten, Versicherer und andere interessierte Parteien können sich mit I Am The Cavalry unter info -at- iamthecavalry.org in Verbindung setzen.