Whitepaper zur Cybersicherheit von Mindray Produkten

November 2024

mindray

Inhalt

Executive Summary

Im dynamischen Umfeld des Gesundheitswesens und der Medizinprodukte kann die Bedeutung und Dringlichkeit wirkungsvoller Cybersicherheitsvorkehrungen nicht hoch genug eingeschätzt werden. Je mehr die Branche technologische Neuerungen und Digitalisierung einführt, desto wichtiger wird die Notwendigkeit von sicheren, belastbaren und vertrauenswürdigen Gesundheitsdiensten und medizinischen Geräten. In diesem Whitepaper wird der ganzheitliche Ansatz von Mindray in Bezug auf Cybersicherheit dargelegt. Es werden die Grundsätze, Werte und Praktiken beschrieben, die unsere Bemühungen zur Gewährleistung der Patientensicherheit, zum Schutz der Kundendaten und zur Sicherstellung der Widerstandsfähigkeit und Kontinuität des Betriebs unserer Geräte bestimmen.

Mindray verfolgt in seinen Cybersicherheits-Initiativen die Prinzipien **Transparenz, Verantwortung und kontinuierliche Verbesserung**. Unser Ansatz basiert darauf, unseren Stakeholdern durch klare und offene Kommunikation über Sicherheitsmaßnahmen, Risikobewertungen und den Schutz sensibler Daten eine fundierte Entscheidungsgrundlage zu bieten. Daten fundierte Entscheidungen ermöglichen. Mit Datenschutz und Cybersicherheit, die in jeder Phase des Produktentwicklungszyklus integriert sind, liefert Mindray verantwortungsbewusste Produkte und Dienstleistungen, die Innovation und Zuverlässigkeit vereinen.

Ein starkes **Informationssicherheitssystem im Unternehmen** ist bei Mindray unerlässlich für die Bereitstellung von sicheren und verlässlichen medizinischen **Geräten und Dienstleistungen**. Wir stützen uns dabei auf das Expertenwissen und die einheitliche Vision unserer gut ausgebildeten **Mitarbeitenden**, deren Einsatz für Cybersicherheit unsere Innovationskraft im Bereich Sicherheit stärkt.

Das Engagement von Mindray für die Cybersicherheit geht weit über die bloße **Einhaltung** internationaler Normen und Vorschriften hinaus: Wir pflegen eine Sicherheitskultur, die sämtliche Aspekt unseres Unternehmens und unserer Aktivitäten durchdringt. Von der anfänglichen Designphase bis zum Monitoring nach dem Inverkehrbringen berücksichtigt Mindray Cybersicherheitsaspekte in jeder Phase des Produktlebenszyklus. Die **Erlangung der Zertifizierungen** unterstreicht Mindrays Engagement für ein Höchstmaß an Sicherheit und Datenschutz. Diese Zertifizierungen sind mehr als nur Auszeichnungen. Sie zeugen von unserem kontinuierlichen Streben nach höchster Qualität und unserem Einsatz für den Schutz der Patienten und ihrer vertraulichen Daten, die durch unsere Geräte verarbeitet werden.

Mindray ist sich bewusst, dass Cybersicherheit im Gesundheitswesen im Sinne der **geteilten Verantwortung** nur gemeinsam erreicht werden kann. Wir engagieren uns aktiv mit Gesundheitsdienstleistern, Regulierungsbehörden und anderen Akteuren, um eine sichere Umgebung für die Patientenversorgung zu schaffen. Diese Zusammenarbeit spielt eine zentrale Rolle bei der Erkennung möglicher Schwachstellen, der Bewältigung von Vorfällen und der Stärkung der Sicherheit im globalen Gesundheitssektor. Durch die Förderung einer offenen Kommunikation und Zusammenarbeit wollen wir eine starke Verteidigung gegen die zunehmend raffinierteren Cyberbedrohungen aufbauen.

Die Säulen des **Mindray Produkt-Cybersicherheitsmodells** - Governance und Risikomanagement, sicheres Design und und Datenschutz - spiegeln eine ganzheitliche Strategie wider, die sich mit dem vielschichtigen Charakter der Cybersicherheit befasst. Jede Säule stellt eine wichtige Komponente unseres umfassenden Sicherheitsrahmens dar und gewährleistet, dass unsere Geräte nicht nur den aktuellen Standards entsprechen, sondern auch gegenüber zukünftigen Bedrohungen gewappnet sind.

Wir wissen, dass das in uns und unsere Geräte gesetzte Vertrauen eine Verantwortung darstellt, die wir mit unermüdlichem Einsatz wahrnehmen müssen. Bei der Bewältigung der Komplexität des digitalen Zeitalters wird Mindray auch weiterhin mit Integrität, Innovation sowie einem unerschütterlichen Engagement für den Schutz des Gesundheitswesens seine Führungsrolle wahrnehmen.

ANLEITUNG ZUR DIGITALISIERUNG DES GESUNDHEITSWESENS: EIN WEG ZU SICHERER INNOVATION

Die Gesundheits- und Medizintechnikbranche hat sich in den letzten Jahrzehnten durch technologische Fortschritte und die fortschreitende Digitalisierung fundamental gewandelt. Innovationen wie Telemedizin, tragbare Geräte zur Gesundheitsüberwachung und Ferndiagnose-Instrumente haben die Betreuung von Patienten revolutioniert und sie effizienter, präziser und leichter zugänglich gemacht. Dank individueller Behandlungspläne, kontinuierlicher Gesundheitsüberwachung und minimalinvasiver Eingriffe können Patienten heute bessere Gesundheitsergebnisse und eine höhere Lebensqualität erwarten.

Mit der zunehmenden Vernetzung digitaler Technologien wächst zugleich das Risiko für Cyberangriffe in der Branche. Die Integration medizinischer Geräte in Krankenhausinfrastruktur und Cloud-basierte Plattformen hat zu neuen Schwachstellen geführt, die den dringenden Bedarf an robusten Sicherheitsmaßnahmen verdeutlichen, wenn es gilt, die Zuverlässigkeit der Geräte zu gewährleisten und sensible Patientendaten zu schützen.

In den vergangenen Jahren wurde das Gesundheitswesen, ähnlich wie bei WannaCry, von zahlreichen massiven Cybersicherheits-vorfällen heimgesucht. So legte beispielsweise der Ransomware-Vorfall im Springhill Medical Center[1] die Krankenhaussysteme lahm und trug zum Tod eines Säuglings bei, als wichtige Überwachungssysteme während der Geburt versagten. Als das University of Vermont Health Network[2] 2020 von einem Ransomware-Angriff getroffen wurde, kam es zu erheblichen operativen Störungen - die Patientenversorgung wurde verzögert und die Spitäler mussten auf Papierakten zurückgreifen. Die Medjack-Angriffe[3], deren Ziel medizinische Geräte wie Infusionspumpen und MRT-Scanner waren, machten sich veraltete Software und lückenhafte Sicherheitsmaßnahmen zunutze, um die Kontrolle zu erlangen und in die weitverzweigten Spitalnetzwerke einzudringen. Die NotPetya Ransomware[4] nutzte die EternalBlue[5] - Schwachstelle, um wichtige Daten zu verschlüsseln und verursachte eine ernsthafte Unterbrechung im weltweiten Gesundheitsbetrieb. Diese Vorfälle verdeutlichen die gravierenden Folgen von Cyberangriffen auf Gesundheitssysteme, indem sie die Vertraulichkeit der Patienten kompromittieren und zentrale medizinische Dienste beeinträchtigen.

Angesichts dieser Herausforderungen ist Mindray bestrebt, diesen Weg der Innovation zu beschreiten und dabei ein Gleichgewicht zwischen der Nutzung des technologischen Fortschritts und der Gewährleistung einer soliden Sicherheit unserer Medizinprodukte zu erreichen. Durch die Festlegung strenger Standards, die Einhaltung internationaler Anforderungen und die Förderung von Transparenz und gemeinsamer Verantwortung will Mindray sicherstellen, dass die Vorteile von Innovationen auf sichere und vertrauenswürdige Weise realisiert werden, sodass eine verbesserte Patientenversorgung ohne Abstriche bei der Sicherheit möglich ist.

[1] https://www.healthcareitnews.com/news/hospital-ransomware-attack -geführte-Kinder-Tod-Klage-behauptet
[2] https://coverlink.com/case-study/uvm-health-network-ransomware-attack/
[3] https://www.trustdimension.com/wp-content/uploads/2015/02/MedJack.4-ilovepdf-compressed.pdf
[4] https://www.cloudflare.com/learning/security/ransomware/petya-notpetya-ransomware/
[5] https://www.avast.com/c-eternalblue

Mindray Cybersecurity-Position

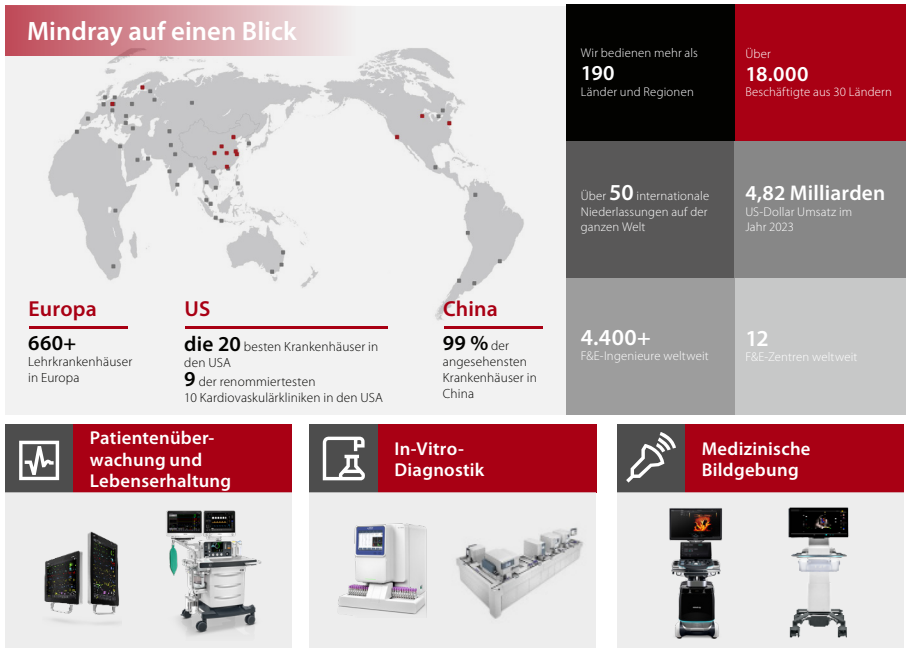
Angesichts steigender Cybersicherheitsrisiken arbeitet Mindray kontinuierlich daran, seine Prozesse und Systeme zu verbessern und Cybersicherheit sowie Datenschutz in allen Bereichen zu integrieren.

- Unternehmensführung mit nachhaltiger Wirkung
- Sicherheit dank Transparenz und Vertrauen
- Bereitstellen einer robusten Sicherheitsbasis
- Einführen und Einhalten von Normen
- Partnerschaftlicher Schutz: Geteilte Verantwortung

Mindray Cybersecurity-Position

Unternehmensführung mit nachhaltiger Wirkung

Mindray zählt zu den weltweit führenden Unternehmen in der Entwicklung, Produktion und Bereitstellung innovativer Medizinprodukte und -lösungen. Unsere Mission: der Menschheit einen besseren Zugang zur Gesundheitsversorgung zu ermöglichen. Seit der Gründung im Jahr 1991 hat sich Mindray auf die Entwicklung von drei Kernproduktlinien spezialisiert: In unserer Unternehmenszentrale in Shenzhen, China, und in 42 internationalen Tochtergesellschaften mit Niederlassungen in 32 Ländern beschäftigen wir rund 7.500 Mitarbeiter, die diverse Anbieter im Gesundheitswesen unterstützen und einen gesellschaftlichen Mehrwert schaffen. Das Engagement für Innovation zeigt sich in unseren 12 globalen F&E-Zentren und einer branchenführenden Investition von 10 % des Jahresumsatzes in Forschung und Entwicklung.



Sicherheit dank Transparenz und Vertrauen

Unsere Grundsätze zur Produktsicherheit demonstrieren ein uneingeschränktes Engagement für die Sicherheit der Patienten, die Zuverlässigkeit unserer medizinischen Geräte und den Schutz vertraulicher Daten. Geleitet von den strengsten internationalen Standards, legen wir den Fokus auf Transparenz, Rückverfolgbarkeit und stetige Verbesserung. Unser Ziel ist die Schaffung eines Gesundheitswesen, das sich durch innovative Technologien und kompromisslose Sicherheit auszeichnet, um die Menschen, die wir unterstützen, bestmöglich zu schützen.

„Vertrauen entsteht durch Transparenz – nicht nur in unseren Maßnahmen, sondern auch in deren Umsetzung." Der transparente Ansatz von Mindray bei der Cybersicherheit bietet unseren Kunden uneingeschränkten Einblick in unsere Sicherheitspraktiken. Klare und transparente Cybersicherheits-Praktiken geben unseren Kunden die Gewissheit, die sie benötigen."

Cheng Minghe
Vice Chairman, Mitglied des Mindray Compliance-Ausschusses

„Bei Mindray ist die Sicherheit Bestandteil der DNA aller von uns hergestellten Geräte, damit wir selbst in den kritischsten Bereichen des Gesundheitswesens Ausfallsicherheit und Zuverlässigkeit gewährleisten können. Cybersicherheit ist nicht bloß ein Feature, sondern ein Grundprinzip, das die Entwicklung, Gestaltung und Implementierung all unserer medizinischen Geräte prägt."

Li Zaiwen
Senior Vice President, Mitglied des Mindray Compliance-Ausschusses

Für uns als Hersteller von Medizinprodukten in der Gesundheitsbranche steht der Begriff „Transparenz" im Mittelpunkt unserer Grundsätze und Werte. Unsere Vision geht über die bloße Compliance hinaus. Sie verkörpert ein tiefgreifendes Engagement und die Verantwortung, der fundierten Entscheidungsfindung durch unsere Benutzer Vorrang einzuräumen. Die FDA[6] plädiert für eine klare und offene Kommunikation über Cybersicherheitsmerkmale und potenzielle Risiken von Geräten, um das Vertrauen von Gesundheitsdienstleistern, Regulierungsbehörden und Patienten zu stärken. Durch verschiedene Formen des Informationsaustauschs, einschließlich Whitepaper, Benutzerhandbücher und technische Dokumentationen, ist Mindray bestrebt, unser Engagement zur Gewährung von Transparenz über die implementierten Sicherheitsmaßnahmen, Risikoüberlegungen und unsere Methoden zum Schutz von Patienten und zum Umgang mit sensiblen Daten kontinuierlich zu verbessern.

Dank Einbettung von Security and Privacy by Design in unseren Entwicklungszyklus stellen wir sicher, dass Cybersicherheit und Datenschutz von Anfang an ein integraler Bestandteil unserer Medizinprodukte sind. So sichern wir die unterbrechungsfreie Verfügbarkeit essenzieller medizinischer Leistungen und wahren die Integrität vertraulicher Daten. Mit unserem detaillierten Risikomanagement überwachen und reduzieren wir fortlaufend mögliche Sicherheitsbedrohungen, wodurch unsere Geräte nicht nur geschützt, sondern auch robust und zuverlässig bleiben. Durch die enge Zusammenarbeit mit Gesundheitsdienstleistern, Aufsichtsbehörden und Branchenpartnern wollen wir eine Sicherheitskultur fördern, die das Vertrauen in das globale Gesundheitswesen stärkt.

Security and Privacy by Design

[6] https://www.fda.gov/media/119933/download

Bereitstellen einer robusten Sicherheitsbasis

Unser Ansatz zur Cybersicherheit durchzieht unser gesamtes Unternehmensethos und fließt in die einzelnen Produkte und Dienstleistungen ein. Wir verstehen, dass eine robuste Informationssicherheit des **Unternehmens** die Basis dafür bildet, Vertrauen in uns und unsere Geräte zu schaffen und aufrechtzuerhalten. Ein so starkes Fundament kann nur durch gut ausgebildete und sorgfältig geschulte **Mitarbeiter** erreicht werden, die sichere und absolut zuverlässige Services und **Produkte** entwickeln und bereitstellen.

Diese umfassende Sicherheitsstrategie, welche die Sicherheitspraktiken unseres Unternehmens, das Fachwissen unserer Mitarbeitenden und unsere Produktinnovationen zyklisch stärkt, veranschaulicht die symbiotische Beziehung, die sowohl unsere Unternehmensabläufe und Produkte als auch unsere Kunden und Interessengruppen vor Cyberbedrohungen schützt.

Einheitliche Sicherheitskultur: Unsere Unternehmenskultur basiert auf einem ausgeprägten Sicherheitsbewusstsein und Best Practices. Sicherheit steht hat höchste Priorität – dieses Bewusstsein prägt alle unsere Mitarbeitenden, von der Geschäftsführung bis in die Entwicklungslabore. Zur Förderung dieser Kultur der Wachsamkeit veranstalten wir regelmäßige Schulungsprogramme, die nicht nur die Grundsätze der Sicherheit und des eingebauten Datenschutzes, sondern auch die allgemeine Informationssicherheit und den Schutz der Privatsphäre, umfassen. Die Schulungen ermöglichen uns die Einbindung fortschrittlicher Sicherheits- und Datenschutzfunktionen in die tägliche Routine und das Produktdesign. Sie verstärken auch die Vertrauenswürdigkeit und Konformität unseres Unternehmens und unserer Produkte.

Unternehmen: Strategische Verteidigung

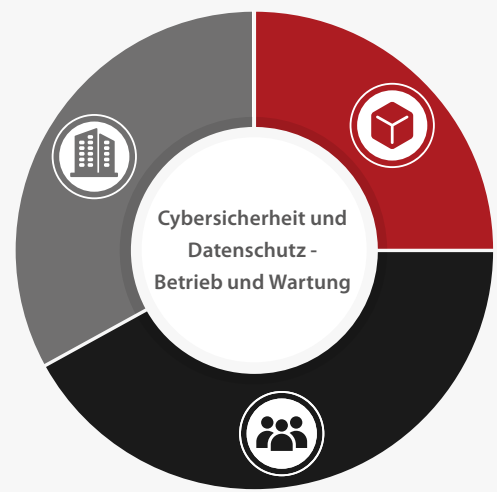
Robuste Unternehmenssicherheit durch umfassende Vorfallreaktionspläne und resiliente Infrastruktur. Dies gewährleistet die Kontinuität des Betriebs und die laufende Verbesserung beim Schutz interner Systeme und Daten.

Mitarbeitende: Kompetente Sicherheitsexperten

Durch intensive Schulungen zu Sicherheitspraktiken und Datenschutzstandards tragen unsere Mitarbeitenden zur Stärkung unserer sicherheitsorientierten Unternehmenskultur bei.

Produkt: Sichere Innovation

Wir integrieren fortschrittliche Sicherheitsfunktionen in jedes Medizingerät, von der Konzeption bis zur Entwicklung, und stärken so das Vertrauen unserer Kunden.



Widerstandsfähige Infrastruktur: Die Sicherheitsinfrastruktur unseres Unternehmens ist darauf ausgelegt, die operative Stabilität und die Vertraulichkeit der Daten zu gewährleisten, die für die Kontinuität und Zuverlässigkeit unseres Geschäftsbetriebs und unseres Kundensupports entscheidend sind. Durch die Absicherung unserer Rechenzentren, Netzwerke und Softwarearchitekturen gegen Störungen und Sicherheitsverstöße stellen wir sicher, dass die Systeme, die unsere Produktentwicklung und Wartungsdienste unterstützen, stets verfügbar und geschützt sind.

Proaktives Vorfallmanagement und stetige Optimierung: Das dynamische Vorfallmanagement von Mindray sowie die kontinuierlichen Sicherheitsbewertungen gewährleisten ein rasches Eingreifen bei potenziellen Cyberangriffen und Schwachstellen - sowohl auf Unternehmens- als auch auf Produktebene. Diese proaktive Haltung mindert nicht nur die Risiken, sondern dient auch der kontinuierlichen Verbesserung unserer Unternehmens- und Produktsicherheitsfunktionen auf der Grundlage von realen Daten und neuen Bedrohungslagen.

Engagement und Transparenz für die Interessengruppen: Bei Mindray sind wir bestrebt, einen offenen Dialog bezüglich unserer Sicherheitsprozesse und -entwicklungen zu führen. Indem wir unsere Unternehmens- und Produktsicherheitsstrategien transparent machen, wollen wir das Vertrauen unserer Kunden stärken und ihnen die Gewissheit geben, dass wir uns für höchste Sicherheitsstandards, Patientensicherheit und den Schutz ihrer vertraulichen Daten einsetzen.

Einführung und Einhaltung von Normen

Internationale Standards und Zertifizierungen sind für uns unverzichtbar, um die Qualität, Sicherheit und Cybersicherheit unserer Produkte auf höchstem Niveau zu gewährleisten. Mit der Einhaltung dieser Standards geht es uns nicht bloß um rechtliche Konformität oder Zertifizierungen - wir möchten unseren Kunden und Nutzern vor allem ein grundlegendes Gefühl von Vertrauen und Sicherheit vermitteln. Dies gibt unseren Stakeholdern die Gewissheit, dass wir mit äußerster Integrität arbeiten und sicherstellen, dass unsere Produkte strengen Qualitäts- und Sicherheitsmaßstäben genügen. Dieses Vertrauen ist im Gesundheitswesen entscheidend, da sich die Zuverlässigkeit und Sicherheit medizinischer Geräte direkt auf die Patientenversorgung und die Ergebnisse auswirkt. Diese Standards und Zertifizierungen sind ein Beweis für unser Engagement, die Sicherheit unseres Unternehmens und unserer Produkte zu gewährleisten, sowie für unsere Bemühungen um kontinuierliches Wachstum und Verbesserung, die uns dazu motivieren, unsere Praktiken laufend zu verbessern.

Produkte von Mindray sind unter anderen mit folgenden Standards und Anforderungen konform: TIR57, ISO 14971, ISO 31000, IEC/TR 80001-2-2, den FDA-Vorgaben und Richtlinien für Anforderungen vor und nach der Markteinführung, MDCG 2019-16, den Grundsätzen und Praktiken des IMDRF, der Europäischen Datenschutz-Grundverordnung (DSGVO), Health Insurance Portability and Accountability Act (HIPAA) für die USA sowie dem chinesischen Gesetz zum Schutz personenbezogener Daten (PIPL). Diese Standards sind die Richtschnur für unsere Prozesse, vom Risikomanagement und der Cybersicherheit bis hin zur gesamten Produktentwicklung und dem Lebenszyklusmanagement. Durch die Einhaltung dieser Standards stellen wir sicher, dass unsere organisatorischen Risiken gemanagt und unsere Produkte mit einem Höchstmaß an Sicherheit konzipiert, entwickelt und gewartet werden.

Was die Zertifizierungen betrifft, so hat Mindray mehrere renommierte Anerkennungen erhalten, darunter ISO/IEC 27001:2022 für das Informationssicherheitsmanagement und ISO/IEC 27701:2019 für das Management von Datenschutzinformationen. Diese Zertifizierungen decken verschiedene Aspekte unserer Geschäftstätigkeit ab, wie z. B. Forschung und Entwicklung, Vertrieb, Service, IT und mehr, und gewährleisten einen umfassenden Ansatz für Compliance und Sicherheit. Zu den weiteren Zertifizierungen gehören NEN7510 für die Informationssicherheit im Gesundheitswesen, UL2900-2-1 für netzwerkfähige Geräte usw. Die Anwendbarkeit bestimmter Normen und Zertifizierungen hängt vom jeweiligen Produkt und der Region ab. Beispielsweise werden die geltenden FDA-Anforderungen bei Geräten in Übereinstimmung mit den Regelwerken und Vorgaben wie der 510(k) Premarket-Mitteilung erfüllt. Durch gründliche Forschung und Überwachung stellen wir sicher, dass unsere Produkte die für die jeweiligen Märkte und Verwendungszwecke geltenden gesetzlichen Anforderungen erfüllen.

Durch Erreichen und Aufrechterhalten dieser Standards und Zertifizierungen möchte Mindray sein unermüdliches Engagement für herausragende Leistungen demonstrieren, unsere Glaubwürdigkeit stärken und uns selbst zu kontinuierlichen Innovationen und Verbesserungen motivieren, um sicherzustellen, dass wir Gesundheitsdienstleistern und Patienten weltweit stets sichere und zuverlässige medizinische Geräte und Dienstleistungen an die Hand geben.

Mit der Einhaltung dieser Standards geht es uns nicht bloß um rechtliche Konformität oder Zertifizierungen - wir möchten unseren Kunden und Nutzern vor allem ein grundlegendes Gefühl von Vertrauen und Sicherheit vermitteln.

Partnerschaftlicher Schutz: Geteilte Verantwortung

Wir sind der Überzeugung, dass Cybersicherheit in der Gesundheits und Medizintechnik eine gemeinsame Verantwortung ist. Die Vernetzung von Medizingeräten erfordert eine enge Zusammenarbeit zwischen Herstellern und Gesundheitsdienstleistern. Nur so können robuste Cybersicherheitspraktiken gewährleistet werden. Die Verantwortung für sichere Produkte liegt ganz klar bei den Herstellern. Sie müssen sich an die Industriestandards halten, bei Design und Entwicklung solide Sicherheitsfunktionen einbauen, ausgiebige Tests durchführen und zeitnah Software-Updates und Patches zur Behebung von Sicherheitslücken bereitstellen. Des Weiteren müssen sie klare Richtlinien für die sichere Nutzung und Instandhaltung ihrer Geräte anbieten. Doch auch den Gesundheitsdienstleistern kommt eine wichtige Rolle zu, wenn es darum geht, nach der Einbindung neuer Geräte in ihre Systeme die erforderlichen Sicherheitsvorkehrungen zu treffen. Dazu gehören die Implementierung ordnungsgemäßer Netzwerkkonfigurationen, die Kontrolle des physischen Zugangs zu den Geräten und die kontinuierliche Überwachung möglicher Bedrohungen. Einrichtungen des Gesundheitswesens müssen außerdem sicherstellen, dass ihre Mitarbeitenden sich an die besten Sicherheitspraktiken halten, ein grundlegendes Verständnis der technischen Funktionen entwickeln und Protokolle zum Schutz der Geräte und der von ihnen verwalteten sensiblen Daten befolgen. Durch diese gemeinsame Verantwortung tragen sowohl Hersteller als auch Gesundheitsdienstleister zu einem sicheren Ökosystem bei, das Innovation mit Patientensicherheit und Datenschutz in Einklang bringt.

Dieser Grundsatz wird nicht nur von Mindray allein vertreten, sondern auch von zahlreichen Forschungseinrichtungen, Hochschulen und Branchenkollegen unterstützt. Laut dem International Medical Device Regulators Forum (IMDRF)[7] erfordert die Cybersicherheit von Medizinprodukten eine enge Zusammenarbeit zwischen Geräteherstellern und Gesundheitsdienstleistern, was die Anwendbarkeit der gemeinsamen Verantwortung während des gesamten Lebenszyklus der Geräte unterstreicht. Dieser Ansatz gewährleistet, dass alle an der Verwendung und Verwaltung von Medizinprodukten beteiligten Parteien imstande sind, Cyberbedrohungen vorzubeugen und so die allgemeine Widerstandsfähigkeit zu verbessern. Die FDA[8] betont außerdem, dass der Schutz vor und die Reaktion auf Cyberangriffe eine gemeinsame Verantwortung für das gesamte Ökosystem der Medizinprodukte ist, einschließlich der Gesundheitseinrichtungen, Patienten, Anbieter und Gerätehersteller. Diese Zusammenarbeit hilft bei der Identifizierung und Minderung von Risiken sowie bei der Reaktion auf und der Bewältigung von Vorfällen auf effektivere Weise.

Durch die Befürwortung des Konzepts der gemeinsamen Verantwortung strebt Mindray eine enge Zusammenarbeit mit allen relevanten Interessengruppen an, insbesondere mit den Gesundheitsdienstleistern. Ziel ist es, alle Beteiligten mit präventiven und reaktionsschnellen Cybersicherheits-Maßnahmen auszustatten und letztlich Gesundheit, Wohlergehen und Sicherheit der Patienten zu schützen.

[7] https://www.imdrf.org/sites/default/files/docs/imdrf/final/technical/imdrf-tech-200318-pp-mdc-n60.pdf
[8] https://www.fda.gov/media/119933/download

Cybersicherheitsmodell für Mindray Produkte

Mindray setzt ein robustes, intern entwickeltes Rahmenwerk ein, um einen umfassenden Schutz medizinischer Geräte zu gewährleisten und die Bemühungen um Cybersicherheit in den verschiedenen Teams und Abteilungen von Mindray zu lenken und aufeinander abzustimmen.

- Governance und Risikomanagement
- Sicheres Design und Entwicklung
- Schutzmaßnahmen und -kontrollen
- Wartungs- und Lebenszyklusmanagement
- Vorfallmanagement
- Datenschutz

Cybersicherheitsmodell für Mindray -Produkte

Die Produktcybersicherheit von Mindray basiert auf dem Mindray Produkt-Cybersicherheitsmodell, einem robusten, intern entwickelten Framework, das den umfassenden Schutz unserer Medizinprodukte sicherstellt und die Cybersicherheitsaktivitäten aller Teams und Abteilungen von Mindray koordiniert. Dieses Modell basiert auf den Grundsätzen des NIST Cybersecurity Framework (LIQUOR)[9], bei dem sechs Kernelemente im Vordergrund stehen: **Steuern, Identifizieren, Schützen, Erkennen, Reagieren und Wiederherstellen**. Aufbauend auf diesem bewährten Fundament haben wir unser Modell speziell auf die Herausforderungen und Anforderungen der Medizintechnikbranche zugeschnitten.

Das Modell beinhaltet 6 Säulen und 17 Elemente. Jede Säule ist auf internationale Standards und regulatorische Anforderungen abgestimmt, um eine gründliche Abdeckung aller kritischen Aspekte der Cybersicherheit von Produkten zu gewährleisten.

Die Säule **„Governance und Risikomanagement"** gewährleistet einen strukturierten Ansatz für das Management von Cybersecurity-Risiken, der mit den Branchenstandards und den regulatorischen Anforderungen in Einklang steht. **Sicheres Design und sichere Entwicklung** integriert Sicherheitspraktiken in den Produktlebenszyklus von Anfang an, wobei bewährte Verfahren wie sichere Kodierung und strenge Tests eingesetzt werden. **Schutzmaßnahmen und Kontrollen** implementieren technische Sicherheitsvorkehrungen wie Zugangskontrollen und Systemhärtung zum Schutz vor unbefugtem Zugriff und Cyberbedrohungen. Das **Wartungs- und Lebenszyklusmanagement** konzentriert sich auf die kontinuierliche Verwaltung der Gerätesicherheit durch effektives Schwachstellenmanagement und sichere Außerbetriebnahme. Die Säule „**Vorfallmanagement**" legt Prozesse für die Erkennung, Reaktion und Analyse von Cybersicherheitsvorfällen fest und betont die gemeinsame Verantwortung von Mindray und Gesundheitsdienstleistern. Die Säule „**Datenschutz**" schließlich gewährleistet die Vertraulichkeit, Integrität und Verfügbarkeit von Patientendaten durch „Privacy by Design", Datenschutz-Folgenabschätzung, Verschlüsselung und robuste Kontrollen der Datenverarbeitung.

Mit diesem umfassenden Rahmenwerk verpflichten wir uns, unternehmensweit robuste Cybersicherheitsstandards aufrechtzuerhalten, die Sicherheit und Zuverlässigkeit unserer medizinischen Geräte zu gewährleisten und unsere Anwender und deren Daten zu schützen. Mit diesem Modell streben wir nicht nur danach, die globalen behördlichen und branchenspezifischen Standards zu erfüllen, sondern auch zu übertreffen, und positionieren Mindray als proaktiven Vorreiter auf dem Gebiet der Cybersicherheit von Medizinprodukten.

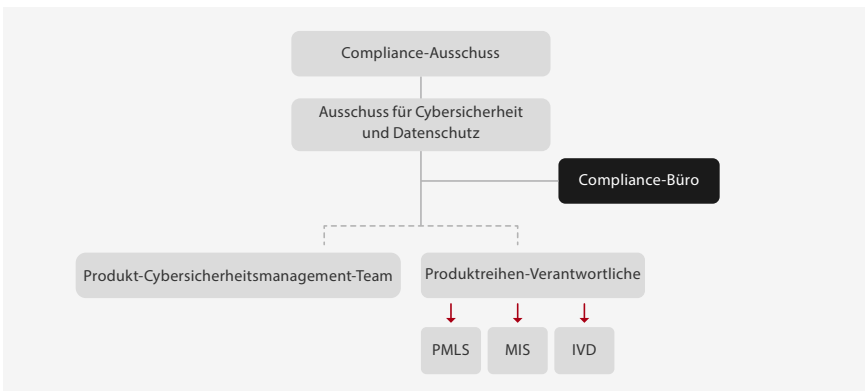
[9] https://www.nist.gov/cyberframework

Governance und Risikomanagement

Die Cybersicherheit der Produkte von Mindray basiert auf einem soliden Fundament aus strukturierten Governance-Richtlinien, Risikomanagement-Rahmenwerken und Methoden zur Überwachung der Einhaltung von Vorschriften.

Governance-Struktur und Richtlinien

Durch die Optimierung der strategischen Entscheidungsfindung und der Richtlinienumsetzung haben wir klare Verantwortlichkeiten und Kommunikationswege etabliert.



Der Compliance-Ausschuss, der sich aus der höchsten Führungsebene des Unternehmens zusammensetzt, leitet und überwacht die Cybersicherheit bei Mindray. Er beaufsichtigt verschiedene Bereiche, darunter Strategien und Pläne für die Einhaltung von Vorschriften zur Cybersicherheit und zum Schutz der Privatsphäre. Der Ausschuss leitet die übergreifenden Initiativen des Unternehmens und die Einhaltung der einschlägigen Vorschriften und trifft Entscheidungen über die wichtigsten Vorhaben.

Der Ausschuss für Cybersicherheit und Datenschutz formuliert die Grundsätze und Ziele des Unternehmens für Cybersicherheit und Datenschutz, einschließlich Cybersicherheit und Datenschutz sowohl auf Unternehmens- als auch auf Produktebene. Dieser Ausschuss leitet und überprüft die einschlägigen internen Richtlinien und Rahmenbedingungen und leitet und überwacht die vollständige Umsetzung in den Geschäftseinheiten in allen Regionen.

Das Compliance Office unterstützt die tägliche Arbeit der Ausschüsse, hält das Team über die verschiedenen Gesetze und Vorschriften auf dem Laufenden und koordiniert die Formulierung von Strategien und Rahmenvorgaben. Dieses Büro unterstützt die Ausschüsse bei der Überwachung und Prüfung der ordnungsgemäßen Umsetzung von Maßnahmen zur Cybersicherheit und zum Schutz der Privatsphäre und übernimmt die praktische Führung bei der Sicherstellung der wirksamen Anpassung der Richtlinien durch die Geschäftsbereiche und Abteilungen in den Regionen.

Das Product Cybersecurity Management Team, spielt eine entscheidende Rolle bei der Unterstützung des Ausschusses und des Compliance Office, indem es sich mit den technischen Aspekten der Cybersicherheit von Geräten befasst. Dieses Team ist zuständig für die Festlegung interner Anforderungen und Standards für die Cybersecurity. Zu den wichtigsten Aufgaben gehören die Identifizierung, Förderung und Anwendung grundlegender Cybersicherheitstechnologien und Testmethoden, Überwachung und Bewertung von Schwachstellen und Bereitstellung technischer Unterstützung für die Forschung in kritischen Bereichen wie die Reaktion auf Schwachstellen und die Entwicklung sicherer Software.

Die Produktlinienbeauftragten sind als erste Instanz für die Produktentwicklung verantwortlich für die Umsetzung der vom Ausschuss, dem Büro und dem Product Cybersecurity Management Team formulierten Anforderungen und Standards während des gesamten Produktlebenszyklus - Entwicklung, Produktion, Wartung usw. Sie sorgen dafür, dass die festgelegten Cybersicherheitsmaßnahmen in jedes Produkt integriert werden. Sie liefern außerdem zeitnahe Rückmeldungen an die Geschäftsleitung bezüglich Cybersicherheitsanforderungen und -problemen und spielen eine aktive Rolle bei der Stärkung der gruppenweit eingesetzten Cybersicherheits-Managementkompetenzen.

Risikomanagement-Framework

Ein solides Risikomanagement-Framework bildet das Fundament der Cybersicherheitsstrategie von Mindray, die es uns ermöglicht, potenzielle Cybersicherheitslücken während des gesamten Produktlebenszyklus systematisch zu identifizieren, zu bewerten und zu beheben.

Unser Rahmenwerk für das Risikomanagement beginnt mit detaillierten Bedrohungsanalysen unter Verwendung des STRIDE-Bedrohungsmodells, das potenzielle Bedrohungen im Zusammenhang mit Spoofing, Manipulation, Repudiation, Informationsoffenlegung, Denial of Service und Elevation of Privilege kategorisch identifiziert. Durch diesen Prozess verstehen wir mögliche Bedrohungsszenarien vollständig und können deren potenzielle Folgen für die Sicherheit der Geräte beurteilen.

Unsere Bemühungen im Bereich Risikomanagement erstrecken sich auf die Erstellung eines detaillierten Risikomanagementplans, einer Software-Stückliste (SBOM), einer Risikobewertung bekannter Schwachstellen sowie von Penetrations- und Scanning-Testberichten. Diese Dokumente bieten einen umfassenden Überblick über die implementierten Sicherheitsmaßnahmen und dienen als Beleg für unser Engagement für die Produktsicherheit. Die Ergebnisse dieser Analysen helfen uns, unsere Risikokontrollen besser zu gestalten, welche in spezifische Produktsicherheitsanforderungen einfliessen und die nachfolgenden Design- und Testphasen steuern.

Unsere Cybersecurity-Risikoanalyse ist nicht bloss eine einmalige Maßnahme, sondern ein fortlaufender Prozess während des gesamten Produktlebenszyklus. So stellen wir sicher, dass mögliche Bedrohungen frühzeitig identifiziert und eingeschränkt werden, was das Risiko von Sicherheitsverletzungen nach der Implementierung reduziert.

Compliance Management für regulatorische und interne Anforderungen

Bei Mindray ist die Überwachung der Einhaltung gesetzlicher Vorschriften eine wichtige Komponente unserer Cybersicherheitsstrategie, dank der wir sicherstellen, dass die internen Standards den gesetzlichen Anforderungen und den Erwartungen an die Branche entsprechen. Der Ausschuss sorgt dafür, dass die rechtlichen Anforderungen kontinuierlich bewertet und alle relevanten Änderungen umgehend in die Normen und Anforderungen für die Produktentwicklung integriert werden. Mindray geht über die reine Einhaltung von Standards hinaus und führt fortlaufend Forschung sowie Vergleiche mit den besten Branchenpraktiken durch. Dank dieses proaktiven Ansatzes sind unternehmenseigenen Sicherheitsmaßnahmen des Unternehmens äußerst robust und entsprechen dem neuesten Stand der Technik sowie den Entwicklungen im Bereich der Cybersicherheit.

Um sicherzustellen, dass die festgelegten Sicherheitsstandards wie beabsichtigt umgesetzt werden, verwendet Mindray auch eine systematische „R&D Cybersecurity and Data Compliance Matrix“, um zu überprüfen, ob die Entwicklungs- und Herstellungspraktiken den festgelegten Richtlinien und Anforderungen entsprechen. Diese Matrix dient als Checkliste für interne Audits zum Zweck der Qualitätskontrolle.

Sicheres Design und Entwicklung

Security by Design

Wie bereits aufgezeigt, ist „Sicherheit durch Design" Mindrays grundlegendes Prinzip, bei dem Sicherheitsprinzipien und -anforderungen von Anfang an und in jeder Phase der Produktentwicklung integriert sind. Diese Kernphilosophie spiegelt sich in unseren robusten Systemen und Richtlinien wider, die sicherstellen, dass Sicherheitsspezifikationen von Anfang an berücksichtigt werden und in der Produktdesignkultur verankert sind. Die Aktivitäten im Rahmen des Sicherheitsentwicklungszyklus (Security Development Lifecycle, SDL) sind tief in unseren gesamten Produktentwicklungsprozess integriert und dienen uns als Leitfaden für die besten Verfahren zur Entwicklung von Cybersicherheitsprodukten.

Eine Schlüsselkomponente unseres Security-by-Design-Ansatzes, der als Grundlage für alle unsere Produkte dient, ist das Prinzip „**Defence in-Depth**". Diese mehrschichtige Verteidigungsstrategie stellt sicher, dass selbst bei einem Ausfall einer Sicherheitsmaßnahme weitere Schutzschichten vorhanden sind, die das Gerät und seine Daten sichern.

Sichere Programmierpraktiken und Qualitätskontrolle

Aufbauend auf den Grundsätzen von „Security by Design" haben wir **umfassende und systematische Standards für die sichere Softwareentwicklung** etabliert, basierend auf den Normen der International Electronic Commission (IEC), den Best Practices der Branche und unseren umfangreichen Erfahrungen in der Softwareentwicklung. Unsere Standards für sichere Kodierung decken verschiedene kritische Aspekte der Kodierung ab, darunter Eingabevalidierung, Fehlerbehandlung und Authentifizierung. Diese Grundsätze ermöglichen es, potenzielle Sicherheitsmängel bereits in der Kodierungsphase zu beheben und so das Risiko von Sicherheitslücken in unseren Endprodukten erheblich zu verringern.

Die **Standards** für **Prozesskontrolle** und **Qualitätssicherung** sind ebenfalls wichtige Bestandteile der sicheren Kodierung. Durch unser **dreistufiges Code-Review-Verfahren**, das eine Checklisten-Bewertung unter Verwendung der etablierten Basisstandards, eine statische Code-Überprüfung mithilfe fortschrittlicher Tools und eine manuelle Validierung durch den Menschen umfasst, stellt Mindray sicher, dass alle Software-Entwicklungsingenieure während des gesamten Entwicklungsprozesses die Standards für sichere Codierung einhalten.

Wir legen Wert auf kontinuierliche Lernprozesse und Wissensaustausch unter den Entwicklern. Sie alle werden regelmäßig in sicheren Kodierungstechniken geschult und bleiben so auf dem neuesten Stand, was Sicherheitslücken und Abhilfemaßnahmen angeht. Dieser proaktive Ansatz stellt sicher, dass unsere Ingenieure für die Bewältigung neuer Risiken bestens gerüstet sind.

Sicherheitsbewertung und Tests

Abgesehen von sicheren Programmierpraktiken führt Mindray solide Sicherheitsbewertungen und -tests durch, die gewährleisten, dass potenzielle Schwachstellen identifiziert und beseitigt und implementierte Sicherheitsmaßnahmen getestet und validiert werden.

Scannen auf Schwachstellen:
Mithilfe fortschrittlicher Tools werden unsere Produkte und Systeme regelmäßig auf potenzielle Schwachstellen gescannt, um Risiken proaktiv und effizient zu erkennen und die erforderlichen Korrekturen umgehend anzuwenden.

Penetrationstests:
Zum Testen der Widerstandsfähigkeit der Geräte unter realen Bedingungen werden umfassende Cyberangriffs-Simulationen durchgeführt.

Sicherheitsbewertung durch Dritte:
Sicherheitsbewertungen werden von unabhängigen Dritten vorgenommen, die eine zusätzliche Validierungs- und Sicherheitsebene bieten und gewährleisten, dass unsere Produkte den Branchen- und Regulierungsstandards entsprechen.

Durch die Integration rigoroser Sicherheitsbewertungs- und Testverfahren in unsere Konstruktionsprinzipien gewährleistet Mindray, dass unsere medizinischen Geräte von vornherein sicher und widerstandsfähig gegen potenzielle Cyberbedrohungen sind. Dieser umfassende Ansatz unterstreicht unser Engagement für die Bereitstellung sicherer, zuverlässiger und konformer Medizinprodukte und gibt unseren Anwendern Vertrauen in die sich in ständigem Wandel befindliche Cybersicherheitslandschaft.

SCHUTZMASSNAHMEN UND -KONTROLLEN

Im Einklang mit dem Konzept der geteilten Verantwortung liegt die Bereitstellung der erforderlichen Sicherheitsfunktionen und -fähigkeiten innerhalb der Konfigurationen medizinischer Geräte in der Hauptverantwortung von Mindray als dem Gerätehersteller.

Zugriffskontrolle

Die Zugriffskontrolle, einschließlich Mechanismen wie **Authentifizierung, Autorisierung und Abrechnung**, ist eine entscheidende Sicherheitskomponente für medizinische Geräte, die gewährleistet, dass nur autorisierte Personen auf kritische Informationen und Systemfunktionen zugreifen können. Mindray Medizingeräte sind mit einer **rollenbasierten Zugriffssteuerung (RBAC)** ausgestattet, bei der Zugriffsberechtigungen auf Grundlage der Rollen einzelner Benutzer innerhalb der Organisation zugewiesen werden. Dadurch können Unternehmen Benutzern ausschließlich minimale Zugriffsrechte entsprechend ihrer Betriebsanforderungen erteilen und somit das Risiko von unerlaubten Dateizugriffen oder willkürlichen Konfigurationsänderungen reduzieren.

Mindray Geräte, verfügen über mehrere zusätzliche Schutzmaßnahmen, die je nach Modell variieren können, um die Zugriffssicherheit zusätzlich zu erhöhen. Dazu gehören unter anderem:

Sperrmechanismus	Nach mehreren aufeinanderfolgenden vergeblichen Anmeldeversuchen wird das Gerät automatisch gesperrt, um unerlaubte Zugriffe durch Brute-Force-Attacken zu unterbinden.
Automatische Abmeldung	Nach einer Phase der Inaktivität werden Sitzungen automatisch beendet, um unbefugten Zugriff auf unbeaufsichtigte Geräte zu verhindern.
Passwortverwaltung	Mindray Geräte ermöglichen anpassbare Passwortrichtlinien. Außerdem empfehlen wir, Passwörter regelmäßig zu ändern.
Zentralisierte, sichere Authentifizierung	Mindray nutzt fortschrittliche, hochgradig sichere Systeme, um Anmeldeinformationen zu speichern und die Authentifizierung durchzuführen. Diese verwenden Verschlüsselungstechnologien zum Schutz der Anmeldedaten und zur Verwaltung von Berechtigungen, um eine sichere Authentifizierung zu gewährleisten und das Risiko des Diebstahls oder Missbrauchs von Anmeldedaten zu verringern.
Kontrollierte größere Konfigurationsänderungen	Größere Änderungen, wie z. B. Upgrades des Betriebssystems, werden durch strenge Zugangskontrollen gesteuert, sodass nur befugtes Personal die Aufrüstung durchführen kann.

Systemhärtung und Konfigurationssteuerung

Systemhärtung schützt unsere Geräte durch die Minimierung der Angriffsfläche. Zu den wichtigsten Komponenten der Mindray Systemhärtungspraktiken, die je nach Modell variieren können, gehören:

Leitfaden zur Härtung des Betriebssystems (OS)	Für verschiedene Funktionen des Betriebssystems werden detaillierte Konfigurationsmethoden und -anforderungen festgelegt. Dies stellt sicher, dass das Betriebssystem in allen Entwicklungsteams einheitlich konfiguriert wird und die Anforderungen effektiv und strukturiert umgesetzt werden.
Whitelisting von Anwendungen und Prozessen	Auf den Geräten dürfen nur zugelassene Anwendungen und Prozesse ausgeführt werden. Dies verhindert die Ausführung von nicht autorisierter Software und von riskanten Aktivitäten.
Antiviren- und Malware-Programme	Mindray Geräte sind so konzipiert, dass sie nahtlos mit branchenüblichen Antiviren- und Malware-Schutzprogrammen zusammenarbeiten und so einen kontinuierlichen Schutz vor schädlicher Software gewährleisten.
Firewall	Microsoft Windows-basierte Mindray Geräte nutzen die integrierte Firewall, um den externen Zugriff zu beschränken und die auf dem Gerät laufenden Anwendungen zu steuern.
Ausschalten unnötiger Risiko-Vektoren	Je nach Geschäftsanforderungen und -umständen werden unnötige Dienste, Ports und Funktionen, wie z. B. Remote-Anmeldung und USB-Autostart, deaktiviert, um die Anfälligkeit für potenzielle Angriffe zu minimieren.
Kiosk-Modus	Geräte mit Kiosk-Modus reduzieren die Angriffsfläche erheblich: Sie beschränken den Benutzerzugriff auf die wesentlichen Funktionen, verhindern nicht autorisierte Aktivitäten und reduzieren den Zugriff auf vertrauliche Patientendaten auf ein Minimum.
Kontrollierte Betriebssystem- und Software-Upgrades	Upgrades des Betriebssystems und der Gerätesoftware dürfen ausschließlich über kontrollierte, von Mindray geprüfte und freigegebene Upgrade-Pakete erfolgen. Dies darf nur durch autorisiertes Personal geschehen. Automatische Betriebssystem-Upgrades sind deaktiviert, um unbefugte Änderungen zu verhindern.

Transparenter Informationsaustausch

Wir arbeiten kontinuierlich daran, noch transparenter über die Sicherheitsmaßnahmen in unseren Geräten zu informieren. Unsere Maßnahmen zur Förderung der Transparenz umfassen unter anderem Folgendes:

Whitepaper zur Cybersicherheit

Für jede Produktlinie stellen wir detaillierte Whitepaper zur Verfügung, die unsere Cybersicherheitsmaßnahmen, -kontrollen und -praktiken ausführlich beschreiben und allen Beteiligten einen transparenten Einblick in unsere Cybersicherheitsbestrebungen ermöglichen. Bitte kontaktieren Sie Mindray für das Whitepaper zu Ihrem spezifischen Produkt.

Produkt-Benutzerhandbücher

Unsere Benutzerhandbücher enthalten detaillierte Beschreibungen und Empfehlungen für die Cybersicherheitsfunktionen unserer Produkte, sodass die Benutzer die vorhandenen Sicherheitsmechanismen verstehen und sie optimal nutzen können.

Herstellererklärung zur Medizinprodukte-Sicherheit (MDS2)

Mindray stellt die Herstellererklärung zur Medizinprodukte-Sicherheit (MDS2) auf Anfrage zur Verfügung, um Gesundheitsdienstleister bei der Bewertung der mit unseren Geräten verbundenen Cybersicherheitsrisiken und -abwehrmaßnahmen zu unterstützen. Die MDS2 beschreibt die Sicherheitsfunktionen unserer Medizinprodukte und informiert auf transparente Weise, wie unsere Produkte die notwendigen Sicherheitsanforderungen und die branchenüblichen Standards einhalten.

Software-Stückliste (SBOM)

Für entsprechende Geräte stellen wir auf Anfrage auch die Stückliste (SBOM) zur Verfügung. Dies ist eine detaillierte Liste der Softwarekomponenten, die in unseren Medizinprodukten verwendet werden. Sie ermöglicht es den Beteiligten, Bibliotheken von Drittanbietern oder Abhängigkeiten zu identifizieren, die ein Risiko darstellen könnten. Diese Transparenz ist entscheidend für das Verständnis potenzieller Schwachstellen und die Wahrung der Integrität der Softwarearchitektur des Geräts.

Unterstützung bei Implementierungsplänen

Wir unterstützen Gesundheitsdienstleister bei der Planung ihrer Implementierung und stellen sicher, dass die Sicherheitsfunktionen unserer Geräte korrekt in die bestehende Umgebung integriert und effektiv verwaltet werden. Diese Unterstützung umfasst Anleitungen zur Installation, Konfiguration und laufenden Instandhaltung und Wartung.

Wartungs- und Lebenszyklusmanagement

Die Wartung nach der Markteinführung unterstreicht Mindrays Verpflichtung zum Schutz der Patienten, ihrer Daten und des Gesundheitswesens - von der Implementierung bis zur Außerbetriebnahme.

Sicherheitslücken- und Patch-Management nach Inverkehrbringen

Die Mindray Produkte nutzen Betriebssysteme von Drittanbietern wie Microsoft Windows und Linux. Unsere **umfassende Patch-Management-Strategie** stellt sicher, dass die Verwendung dieser Betriebssysteme keine Risiken birgt. Relevante Schwachstellen werden kontinuierlich überwacht, ihre Auswirkungen auf unsere Geräte analysiert und Patches zur Behebung von möglichen Problemen bereitgestellt.

Bei Produkten, die unter Microsoft Windows laufen, beginnt die Bewertung der Auswirkungen neu veröffentlichter Sicherheitspatches und Hotfixes in der Regel innerhalb von 48 Stunden, nachdem Mindray von einem neuen Sicherheitspatch in Kenntnis gesetzt wurde. Wir evaluieren die Auswirkungen von Patches und entscheiden, ob diese umgehend installiert werden müssen oder in geplante Updates eingebunden werden können. Für kritische Patches, die keinen Aufschub dulden, stellen wir **detaillierte Anweisungen für eine sofortige Aktualisierung zur Verfügung**. So wird gewährleistet, dass akute Schwachstellen zeitnah und sicher behoben werden. In anderen Fällen werden Patches innerhalb weniger Wochen freigegeben, wobei die Gerätebenutzer unverzüglich informiert werden, sodass unsere Geräte weiterhin geschützt sind. Für unsere Linux-basierten Produkte führen wir alle sechs Monate eine Analyse durch. Da Linux-Plattformen in medizinischen Geräten für konkrete Anwendungen individuell angepasst sind, erfolgt die Patch-Freigabe üblicherweise als komplettes Software-Update. Wenn die Bedrohung nicht allein durch die Installation von Betriebssystem-Patches behoben werden kann, wird möglicherweise ein System-Software-Update veröffentlicht.

Upgrade-Pakete werden vor der Installation einem **Prüfsummentest** unterzogen. Dies gewährleistet die Integrität und Authentizität des Upgrade-Pakets und verhindert unbefugte Änderungen. Der Upgrade-Prozess wird bei uns streng überwacht, sodass ausschließlich autorisiertes Personal mit einem passwortgeschützten Mindray Tool Upgrades vornehmen kann. Automatische Betriebssystem-Upgrades sind deaktiviert, um unerlaubte Änderungen zu verhindern.

Unterstützung bei End-of-Life und Außerbetriebnahme

Wir stellen unseren Kunden gegen Ende der Lebensdauer eines Produkts unaufgefordert detaillierte **End-of-Life (EOL)-Dokumente** bereit. Diese enthalten wichtige Informationen über die Einstellung der Reparaturdienste, die Verfügbarkeit von Ersatzteilen und die Fristen für den technischen Support, damit unsere Kunden ausreichend Zeit haben, Ersatz oder Aufrüstungen zu planen. Dieser transparente Ansatz stellt sicher, dass Kunden gut informiert sind und den Betrieb während der Umstellung von älteren Modellen aufrechterhalten können. Dies unterstreicht Mindrays Engagement für vorbildlichen Service und Kundenbetreuung.

Wenn Geräte außer Betrieb genommen werden, ist eine sichere und verantwortungsvolle Abwicklung unerlässlich, um empfindliche Daten vor unberechtigtem Zugriff zu schützen und sicherzustellen, dass die ausgedienten Geräte keine Gefährdung darstellen. Durch persönliche Anleitungen oder Benutzerhandbücher zu sicheren Entsorgungspraktiken, z. B. Anweisungen zum Datenlöschverfahren, unterstützen wir Gesundheitsdienstleister bei der sicheren Außerbetriebnahme unserer Geräte. Außerdem beraten wir Gesundheitsdienstleister bei der Einhaltung lokaler Vorschriften und internationaler Richtlinien, einschließlich derjenigen der FDA und des NIST, in Bezug auf die Entsorgung elektronischer Geräte, um sicherzustellen, dass ausgemusterte Geräte sicher und rechtskonform entsorgt werden.

VORFALLMANAGEMENT

Im Gesundheitswesen und in der Medizintechnik wird das Vorfallmanagement als gemeinsame Verantwortung verstanden. Eine wirksame Vorbeugung und Reaktion auf Cyberangriffe kann nur durch die Zusammenarbeit zwischen den Leistungserbringern im Gesundheitswesen und den Herstellern von Medizinprodukten erreicht werden. Mit den folgenden Ansätzen wollen wir die Zusammenarbeit im Bereich der Cybersicherheit fördern und sicherstellen, dass sowohl Mindray als auch die Gesundheitsdienstleister bestens gerüstet sind, um auf potenzielle Sicherheitsbedrohungen zu reagieren und diese zu entschärfen.

Protokollierung von Vorfällen

Eine **zuverlässige Erfassung von Vorfällen** ist ein wichtiges Element, das Hersteller von Medizinprodukten anbieten können.
Die medizinischen Geräte von Mindray sind mit speziellen Protokollen zur Aufzeichnung sicherheitsrelevanter Vorgänge ausgestattet. Dies ermöglicht eine lückenlose Aufzeichnung von Aktivitäten, was für die Analyse von Vorfällen und die optimale Reaktion darauf maßgebend sein kann. Wir arbeiten eng mit Gesundheitsdienstleistern zusammen, wenn es um den Export, die Verwaltung und die Analyse von Sicherheitsprotokollen in ihrem Umfeld geht.

Unsere Geräte sind außerdem mit verschiedenen Backup- und Wiederherstellungsmechanismen ausgestattet, die dafür sorgen, dass sicherheitsrelevante Informationen erhalten bleiben und bei Systemausfällen und sonstigen Vorfällen zügig wiederhergestellt werden können. Diese Ausfallsicherheit trägt dazu bei, die Integrität und Verfügbarkeit der Sicherheitsprotokolle aufrechtzuerhalten und unterstützt die laufenden Sicherheitsmaßnahmen.

Vorfallreaktion und Support

Bei Mindray sind spezialisierte Teams im Einsatz, die für das Vorfallmanagement zuständig sind und potenzielle Bedrohungen für unsere Geräte kontinuierlich beobachten und analysieren. Wird ein Sicherheitsvorfall erkannt oder gemeldet, bewerten die Teams in Zusammenarbeit mit den Geschäftsbereichen die Risiken, erstellen Reaktionspläne und leiten Abhilfemaßnahmen ein. Unsere „Cybersecurity Incident Response Guideline" gewährleistet ein standardisiertes und einheitliches Vorgehen aller Beteiligten. Wenn eine gesetzliche Meldepflicht besteht, arbeiten wir eng mit den zuständigen Behörden zusammen, um die zeitnahe und effiziente Kommunikation zu gewährleisten. Dabei stehen wir während des gesamten Prozesses in engem Kontakt mit unseren Kunden. Gemeinsam arbeiten wir an der schnellen Beurteilung der Situation und der Implementierung der Abhilfemaßnahmen, um die Auswirkungen minimal zu halten und die Gerätesicherheit zu wahren.

Die Medizingeräte von Mindray sind mit Funktionen zur Gewährleistung der Geschäftskontinuität ausgerüstet – selbst bei cybersicherheitsrelevanten Vorfällen. Je nach Funktionalität setzen bestimmte Geräte Mechanismen wie Datennachführung und Datensynchronisation ein, damit während eines Netzwerkausfalls keine kritischen Patienteninformationen verloren gehen. Manche Geräte verfügen zudem über eine mehrschichtige Netzwerkarchitektur, die eine Risikoabgrenzung zwischen dem Gerät und dem Krankenhaus-Netzwerk gewährleistet. Durch den Betrieb in einer redundanten kabelgebundenen und kabellosen Netzwerkumgebung können die Geräte auch bei Ausfall eines Netzwerkgeräts ihren normalen Betrieb aufrechterhalten.

Durch die Unterstützung von Gesundheitsdienstleistern mit systematischen Maßnahmen zur Reaktion auf Vorfälle und technischem Support versetzt Mindray seine Partner in die Lage, Vorfälle im Bereich der Cybersicherheit effektiv zu bewältigen und zu entschärfen sowie die betriebliche Widerstandsfähigkeit zu verbessern.

DATENSCHUTZ

Privacy by Design

Mindray orientiert sich an internationalen Standards und bewährten Branchenpraktiken und hat ein risikobasiertes Managementsystem für Informationssicherheit und Datenschutz etabliert. Dieses System verwaltet den gesamten Lebenszyklus der Daten, einschließlich der Erfassung, Übermittlung, Verwendung, Weitergabe, Speicherung und Löschung, und hält sich dabei an die Grundsätze der Rechtmäßigkeit, Fairness, Ehrlichkeit, Offenheit und Transparenz, mit dem Ziel, die **Vertraulichkeit, Integrität und Genauigkeit** aller bei Mindray verarbeiteten personenbezogenen Daten zu schützen. Mittels seines robusten Managementsystems hat Mindray die Zertifizierungen ISO/IEC 27001 und ISO/IEC 27701 erworben und verfeinert seine Datenschutzanforderungen kontinuierlich.

Auf der Grundlage einer solchen Unternehmenskultur und des Bewusstseins für den Schutz der Privatsphäre und mit der Verpflichtung, die Privatsphäre und die Daten unserer Kunden und Patienten zu schützen und zu respektieren, hat Mindray die Kernprinzipien „**Privacy by Design**“ und „**Privacy by Default**“ in den Produktentwicklungsprozess integriert (siehe Abbildung auf Seite 6.). Diese Grundsätze sind bereits in der Konzipierungs- und Planungsphase durch Basisrichtlinien für Berechtigungen, Protokollierung, Verschlüsselung und De-Identifizierung/Anonymisierung usw. integriert. Indem wir den Schutz der Privatsphäre von Anfang an in das Design einbeziehen, stellen wir sicher, dass Maßnahmen zum Schutz der Privatsphäre nicht einfach nur ein zusätzliches Element sind, sondern integraler Bestandteil der Produktarchitektur. So schaffen wir Vertrauen und halten uns an die regulatorischen Anforderungen.

Mindray macht den Schutz persönlicher Daten zum zentralen Bestandteil des kompletten Produktentwicklungsprozesses.

Durch unser Prinzip „Privacy by Design“ konnten wir bei Gesundheitsdienstleistern und Patienten eine Vertrauensbasis schaffen, die eine Behandlung sensibler Nutzerdaten nach höchsten Sicherheits- und Datenschutzstandards sicherstellt.

Datenschutz-Folgenabschätzung

Für Mindray ist die Einhaltung der Datenschutzbestimmungen nicht nur eine rechtliche Verpflichtung, sondern ein Eckpfeiler, der uns hilft, die mit Datenschutzverletzungen verbundenen Risiken zu mindern und das Vertrauen unserer Interessengruppen zu stärken. Die Datenschutz-**Folgenabschätzung (Privacy Impact Assessment, PIA)** ist im Produktentwicklungsprozess integriert, wirksame Kontrollmaßnahmen wurden gemäß einschlägigen Compliance-Anforderungen umgesetzt. Der PIA-Prozess umfasst eine gründliche Analyse und das Dokumentieren von potenziellen Risiken für die Privatsphäre, gefolgt von der Umsetzung geeigneter Abhilfestrategien. Eine solche robuste Bewertungs- und Kontrollimplementierung ermöglicht es nicht nur Mindray, sondern auch unseren Kunden, einschlägige Gesetze und Vorschriften wie die **GDPR**, **HIPAA oder PIPL** einzuhalten. Wir haben auch ein detailliertes **Whitepaper zur Datenschutzgrundverordnung**[10] veröffentlicht, das zeigt, wie Mindray einen der strengsten internationalen Standards für den Datenschutz einhält. Das Whitepaper gewährt Einblicke in Mindrays Unternehmensführung sowie in interne Kontrollmechanismen und Verfahren zur Verarbeitung personenbezogener Daten.
Es beschreibt, wie wir unserer Verpflichtung zur Einhaltung hoher Standards im Bereich Datensicherheit und Datenschutz nachkommen.

[10] https://www.mindray.com/content/dam/xpace/en/legal/GDPR.pdf

Datenverschlüsselung

Aufbauend auf den Grundsätzen von Privacy by Design, ist die Datenverschlüsselung der Eckpfeiler des Datenschutzkonzepts von Mindray. Sie dient als wichtiger Schutzmechanismus, um kritische Informationen vor unbefugten Zugriffen und Sicherheitsverletzungen zu schützen. Mindray verwendet umfassende Verschlüsselungsmethoden, die speziell für die Datensicherheit während des Transfers und der Speicherung entwickelt wurden. Sämtliche Produktlinien von Mindray verwenden die für ihr jeweiliges Gerätedesign und ihre spezifischen Geschäftsanforderungen optimalen Protokolle und Methoden, wodurch ein angemessener Schutz aller Daten gewährleistet ist.

Daten in Transit

Bei der Datenübertragung werden DICOM- und HL7-Standards verwendet, die eine Vielzahl von Verschlüsselungsprotokollen unterstützen, darunter TLS 1.2 mit AES-256-Verschlüsselung. Für die drahtlose Kommunikation unterstützen die Mindray Geräte WPA/WPA2 Enterprise, das eine zuverlässige Verschlüsselung der über Wi-Fi-Netzwerke übertragenen Daten gewährleistet.

Daten im Ruhezustand

Mindray Geräte nutzen bei Bedarf sichere Verschlüsselungsalgorithmen wie AES-256 zum Schutz gespeicherter Daten vor unbefugtem Zugriff, wobei wir gleichzeitig bestrebt sind, die Erfassung und Speicherung persönlicher Daten auf das Notwendigste zu beschränken.

Datenvisualisierung

Persönlich identifizierbare Informationen (PII) auf dem Bildschirm oder in exportierten Berichten können so konfiguriert werden, dass sie ausgeblendet werden, also unsichtbar sind. Diese Flexibilität ermöglicht ein optimiertes Management des Zugriffs auf personenbezogene Daten.

Datenexport

Für Backups auf USB wird 7z-Komprimierung mit starker Verschlüsselung verwendet, um die archivierten Daten zu schützen und sicherzustellen, dass die Datensätze sicher komprimiert und gespeichert werden. Mindray Geräte unterstützen auch Anonymisierungs- und Pseudonymisierungstechniken beim Export und Backup von wichtigen Daten auf Festplatten.

Durch den Einsatz fortschrittlicher Verschlüsselungstechnologien und die Einhaltung strenger Datenschutzstandards ermöglichen Mindray Geräte den Nutzern jederzeit einen angemessenen Datenschutz. Dies gilt sowohl für die Übermittlung, Speicherung und Anzeige als auch für den Export von Daten.

Datenverwaltung bei Wartungsarbeiten

Bei notwendigen Wartungsarbeiten kann es erforderlich sein, dass unser Personal Zugang zu den Geräten bekommt oder dass diese an unsere Reparaturwerkstätten geschickt werden. Für den Fall, dass die Daten auf den Geräten nicht vollständig gelöscht, anonymisiert oder desensibilisiert werden, hat Mindray strenge Protokolle und robuste interne Vorschriften für den Umgang mit Daten während der Wartung eingeführt. Dies stellt sicher, dass sensible Informationen ordnungsgemäß geschützt oder vernichtet werden, um unbefugten Zugriff zu verhindern.

Mindray bietet Gesundheitsdienstleistern eine umfassende Anleitung zur risikofreien Datenverwaltung während der Wartung. Eine wichtige Maßnahme ist die zuverlässige Datenlöschfunktion, die dringend empfohlen wird, um sicherzustellen, dass keine sensiblen Informationen auf den gewarteten Geräten verbleiben.

In jeder Region dienen die lokalen Teams als erste Instanz zur Beurteilung, ob die Probleme auf ihrer Ebene gelöst werden können.
In Regionen, in denen die Rücksendung von Geräten und Protokollen nach China verboten ist, werden alle Fragen vor Ort geklärt. In Fällen, in denen die Rücksendung von Geräten und Protokollen nach China zur Fehlerbehebung nicht verboten und unvermeidlich ist, führt das Team vor Ort eine gründliche Überprüfung durch, um zu bestätigen, dass sensible Daten ordnungsgemäß gelöscht wurden, um die Einhaltung des internationalen Datenschutzes und der grenzüberschreitenden Transferbestimmungen zu garantieren. Alternativ können Methoden zur Desensibilisierung von Daten angewandt werden, bei denen sensible Informationen so verändert werden, dass sie nicht mehr auffindbar oder identifizierbar sind, ihr Nutzen für die Diagnose jedoch erhalten bleibt. Dies kann die Maskierung oder Änderung persönlich identifizierbarer Details beinhalten, wobei Anonymisierungstests sicherstellen, dass die verbleibenden Daten nicht mit individuellen Patienten in Verbindung gebracht werden können.

Unser Personal verfolgt eine **strenge Zugangskontrolle** unter Einhaltung des Prinzips der minimalen Privilegien (POLP). Dies stellt sicher, dass nur autorisierte Mitarbeitende auf das Gerät und die gespeicherten Daten zugreifen können, wobei der Zugriff strikt auf die für ihre Funktion notwendigen Bereiche beschränkt ist. Alle Mitarbeitenden des Unternehmens sowie auch autorisierte Dritte sind zur Vertraulichkeit verpflichtet, um sicherzustellen, dass sie die verbleibenden Daten mit einem Höchstmaß an Vertraulichkeit und Sicherheit behandeln.

Bei der Fernwartung verwendet Mindray sichere Tools, die vom Risiko- und Kontrollmanagementteam streng überwacht werden. Vor Durchführung von Fernwartungsaktivitäten ist eine Genehmigung durch den Kunden erforderlich. Außerdem wird nach dem Grundsatz der minimalen Notwendigkeit lediglich auf die für die Wartung erforderlichen Daten zugegriffen, um das Risiko der Datenexposition möglichst gering zu halten. Für eine sichere Verwaltung und Beendigung von Fernzugriffssitzungen sind entsprechende Kontroll- und Abschlussverfahren implementiert.

Mindray hat sich verpflichtet, während des gesamten Lebenszyklus seiner medizinischen Geräte die höchsten Datenschutzstandards einzuhalten. Diese Herangehensweise schützt nicht nur vertrauliche Daten, sondern stärkt auch das Vertrauen der Benutzer in unsere Geräte. Dies entspricht Mindrays Zielsetzung, medizinische Technologien voranzubringen und gleichzeitig die Sicherheit unserer Kunden und Anwender in den Mittelpunkt zu stellen.

Schlussbemerkung

Auch in Zukunft bleibt Mindray seinem Ziel treu, medizinische Technologien voranzutreiben und gleichzeitig die höchsten Standards der Cybersicherheit zu gewährleisten. Wir wissen, dass das in uns und unsere Geräte gesetzte Vertrauen eine Verantwortung darstellt, die wir mit unermüdlichem Einsatz wahrnehmen müssen. Durch die kontinuierliche Verbesserung unserer Cybersicherheitsmaßnahmen und die Vorreiterrolle bei neu aufkommenden Bedrohungen sind wir bestrebt, Lösungen für das Gesundheitswesen anzubieten, die nicht nur innovativ, sondern auch zuverlässig und sicher sind.

Zusammenfassend zeigt dieses Whitepaper den ganzheitlichen und vorausschauenden Ansatz von Mindray in puncto Cybersicherheit. Es unterstreicht unser Engagement für den Schutz von Patientendaten, die Gewährleistung der Integrität unserer Medizinprodukte und die Förderung einer Sicherheitskultur, die integraler Bestandteil unserer Mission ist. Bei der Bewältigung der Komplexität des digitalen Zeitalters wird Mindray auch weiterhin mit Integrität, Innovationsgeist und einem unerschütterlichen Engagement seine Führungsrolle für den Schutz des Gesundheitswesens wahrnehmen.