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 o□ene 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 scha□en. 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 o□enen Kommunikation und Zusammenarbeit wollen wir eine starke Verteidigung gegen die zunehmend ra□nierteren 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.

Mindray Cybersecurity-Position

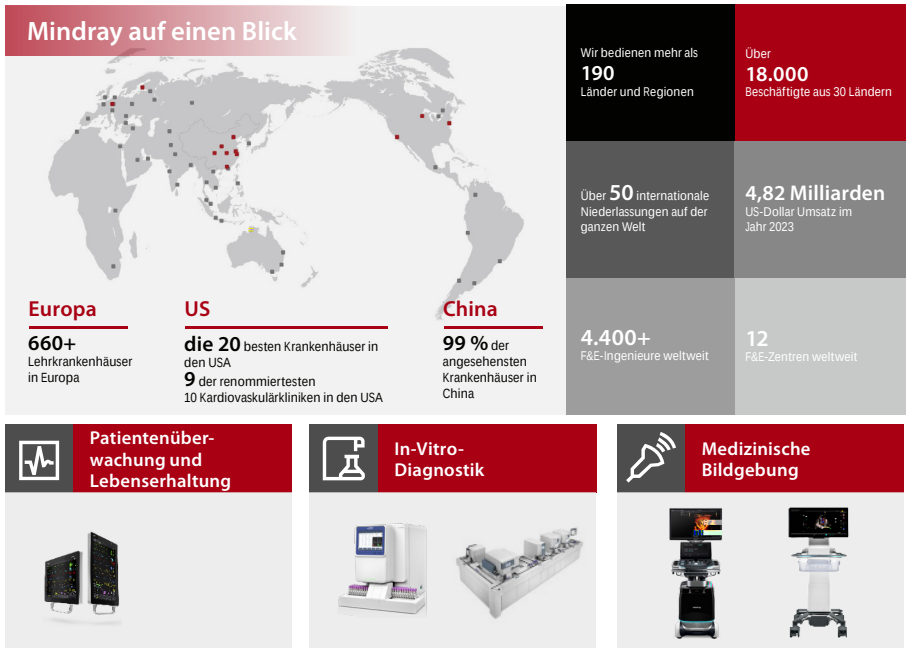
Angesichts steigender Cybersicherheitsrisiken arbeitet Mindray kontinuierlich daran, seine Prozesse und Systeme zu verbessern und Cybersicherheit sowie Datenschutz in allen Bereichen zu integrieren.

- 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.

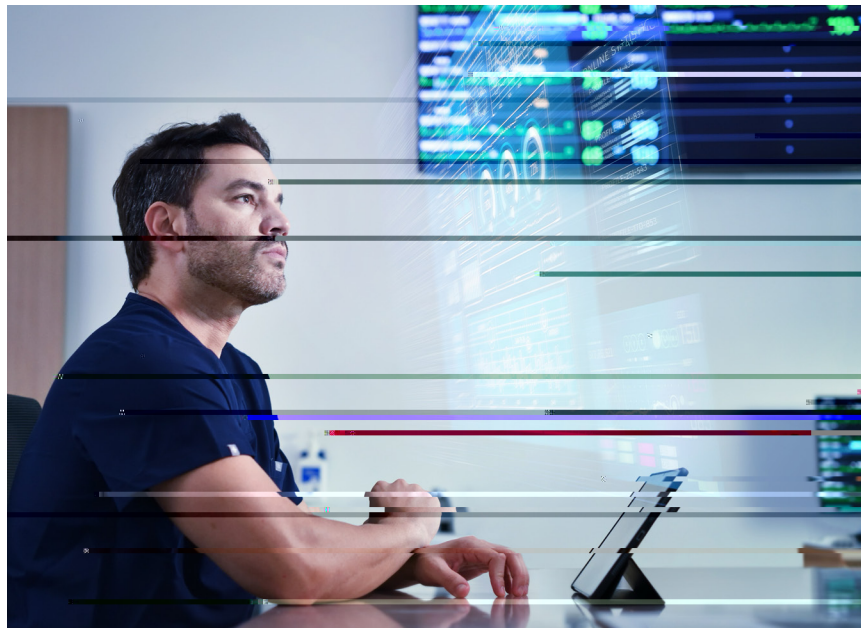
„Vertrauen entsteht durch Transparenz – nicht nur in unseren Maßnahmen, sondern auch in deren Umsetzung.“ Der transparente Ansatz von Mindray bei der Cybersicherheit bietet unseren Kunden uneingeschränkten Einblick in unsere Sicherheitspraktiken. Klare und transparente Cybersicherheits-Praktiken geben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

security-Position



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

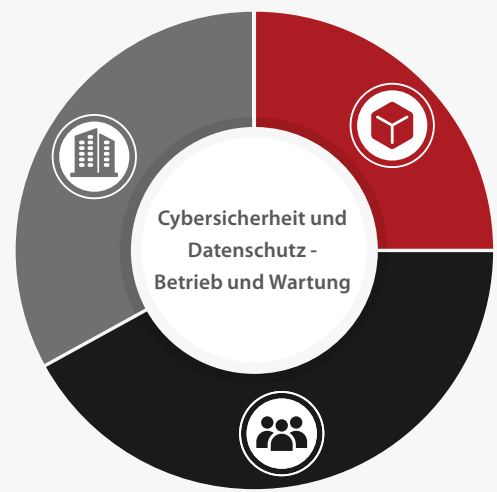
Robuste Unternehmenssicherheit durch umfassende Vorfallreaktionspläne und resiliente Infrastruktur. Dies gewährleistet die Kontinuität des Betriebs und die laufende Verbesserung beim Schutz interner Systeme und Daten.

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.

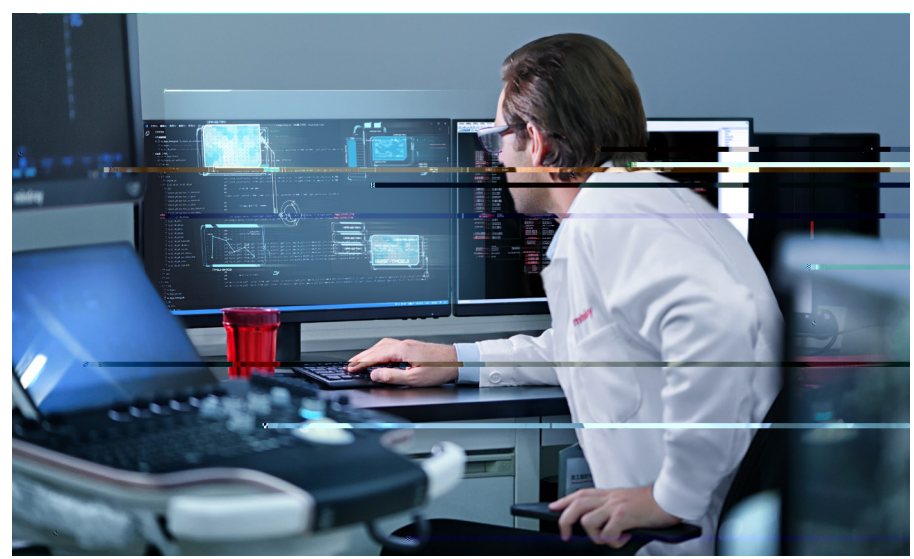
Was die Zertifizierungen betri□t, so hat Mindray mehrere renommierte Anerkennungen erhalten, darunter ISO/IEC 27001:2022 für das Informationssicherheitsmanagement und ISO/IEC 27701:2019 für das Management von Datenschutzinformationen. Diese Zertifizierungen decken verschiedene Aspekte unserer Geschäftstätigkeit 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

UL Solutions

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

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

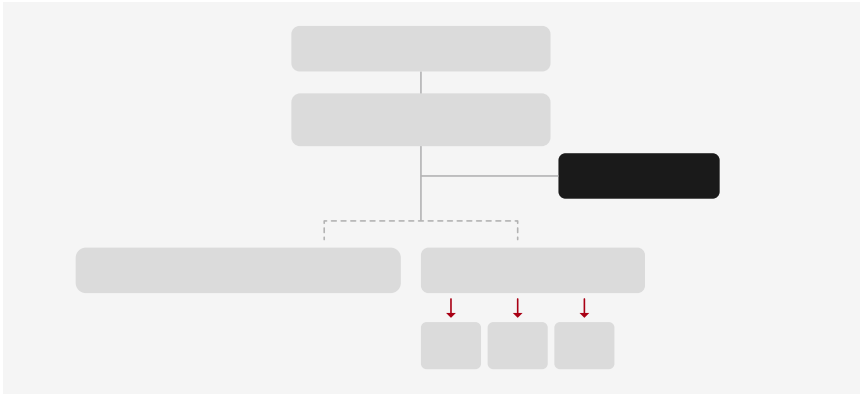
Cybersicherheitsmodell für Mindray Produkte

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

Governance und Risikomanagement

Governance-Struktur und Richtlinien



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, Informationso□enlegung, 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 werdeniens (t)-31.9 (r)-9.2 Tw 0 -1.5 Tdv9 (l)0.7 (l).8 (ie)-3.

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 e□zient zu erkennen und die erforderlichen Korrekturen umgehend anzuwenden.

Penetrationstests:
Zum Testen der Widerstandsfähigkeit der Geräte unter realen Bedingungen werden umfassende Cyberangri□s-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.

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 Zugri□skontrolle, einschließlich Mechanismen wie Authentifizierung, Autorisierung und Abrechnung, ist eine entscheidende Sicherheitskomponente für medizinische Geräte, d37z.875 l65 Td[(e8753[(e3 (74.3 (s)-)-16s)-]TJ (l)0.9l3.6)34-3.3 (r)-1g3K (t)-14.3 (g3)l (l)4 (e (s)7.5 ((f)-138 (e)-16.5 ()-1.8 (e)0.5,d)-6.3aie)-siesicicha-3.6 s44n5 fi4.1 (r)-11.9 (s)-17.4 9n
Mine

f5 (d (R (ia)5.7B9 (e)-1.AC2 (5)13))/T1_0 1

Systemhärtung und Konfigurationssteuerung

Systemhärtung schützt unsere Geräte durch die Minimierung der Angri□sfläche. 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 e□ektiv 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 Zugri□ 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 Angri□e zu minimieren.

Kiosk-Modus

Geräte mit Kiosk-Modus reduzieren die Angri□sfläche erheblich: Sie beschränken den Benutzerzugri□ auf die wesentlichen Funktionen, verhindern nicht autorisierte Aktivitäten und reduzieren den Zugri□ auf vertrauliche Patientendaten auf ein Minimum.

Kontrollierte Betriebssystem- und Software-Upgrades

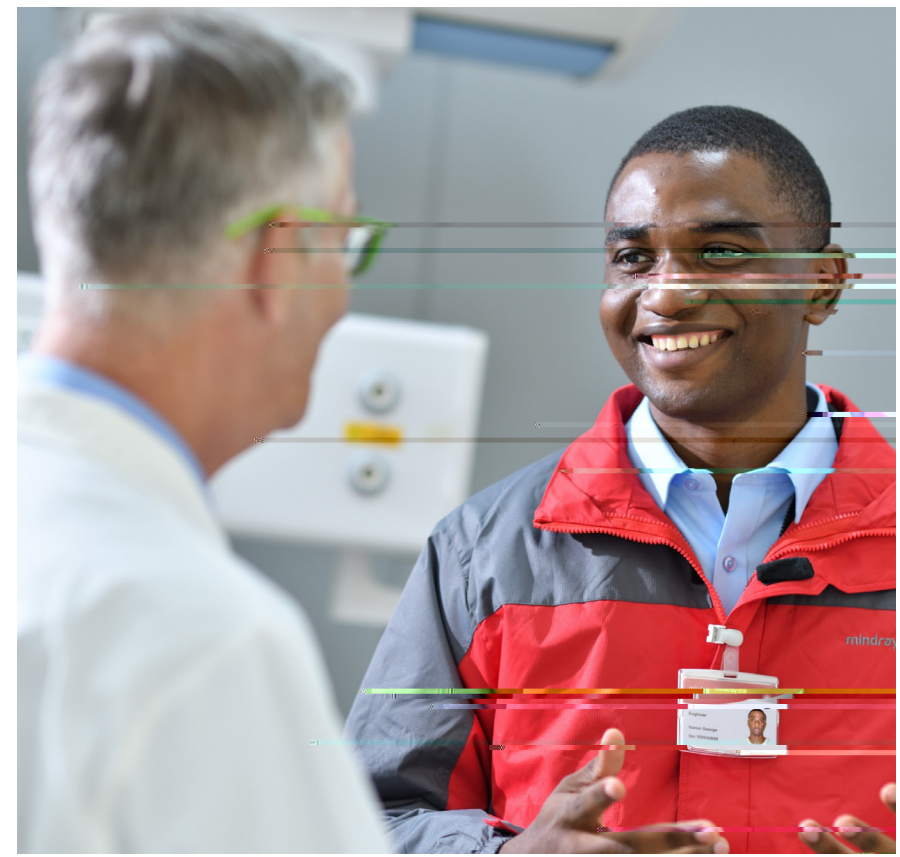
Upgrades des Betriebssystems und der Gerätesoftware dürfen ausschließlich über kontrollierte, von Mindray geprüfte und freigegebene Upgrade-Pakete erfolgen. Dies darf nur durch autorisiertes Personal geschehen. Automatische Betriebssystem-Upgrades sind deaktiviert, um unbefugte Änderungen zu verhindern.

Die Wartung nach der Markteinfüm634lQB34l.224 34.4l0.2087694. l691.386 36.076 38.316 697 8 0 0 .443 37.98 712.3447697 8087.QB3-4712.346712. 3(nf8M)-2.54(ar)8 0 0 .i354(a 34.34 6.076 (d34444334 a)77 12yt)-367 80 Mnf9Mar3566 3

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 Zugri 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.



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, O□enheit 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 scha□en 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] veröentlicht, 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

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 Zugri 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 au ndbar 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 Zugri 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 zugegri en, um das Risiko der Datenexposition möglichst gering zu halten. Für eine sichere Verwaltung und Beendigung von Fernzugri ssitzungen sind entsprechende Kontroll- und Abschlussverfahren implementiert.

Mindray hat sich verpflichtet, während des gesamten Lebenszyklus seiner medizinischen Geräte die höchsten Datenschutzstandards

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.