Dokumentacja techniczna cyberbezpieczeństwa produktów firmy Mindray

Listopad 2024

mindray

Spis treści

Streszczenie

W dynamicznie rozwijającym się sektorze ochrony zdrowia i urządzeń medycznych kluczową rolę odgrywają niezawodne cyberzabezpieczenia. Ponieważ branża niezmiennie korzysta z postępu technologicznego i cyfryzacji, konieczność zapewnienia bezpiecznych, odpornych i godnych zaufania usług opieki zdrowotnej i urządzeń medycznych zyskuje nadrzędne znaczenie. Niniejszy dokument przedstawia kompleksowe podejście firmy Mindray do cyberbezpieczeństwa, wyszczególniając zasady, wartości i praktyki, które kierują naszymi wysiłkami na rzecz zapewnienia bezpieczeństwa pacjentów, ochrony danych klientów oraz zapewnienia odporności i ciągłości działania naszych urządzeń.

Zasady i wartości leżące u podstaw inicjatyw Mindray w zakresie cyberbezpieczeństwa podkreślają wagę **przejrzystości, odpowiedzialności i ciągłego doskonalenia**. W Mindray wierzymy, że kluczem do zdobycia zaufania naszych interesariuszy jest umożliwienie im podejmowania świadomych decyzji poprzez przejrzystość w zakresie środków bezpieczeństwa wdrożonych w naszych urządzeniach, ustaleń dotyczących ryzyka i procedur przetwarzania danych wrażliwych. Poprzez wdrażanie ochrony prywatności i praktyk cyberbezpieczeństwa na każdym etapie rozwoju naszych produktów, Mindray dostarcza produkty i usługi nie tylko innowacyjne, ale również odporne na ataki.

Dla Mindray silny **program bezpieczeństwa informacji w przedsiębiorstwie** to podstawa dostarczania bezpiecznych i niezawodnych **urządzeń oraz usług** medycznych. Fundament ten opiera się na specjalistycznej wiedzy i jednolitej wizji naszych wykwalifikowanych **pracowników,** których zaangażowanie w cyberbezpieczeństwo umożliwia bezpieczne wprowadzanie innowacji.

Zaangażowanie firmy Mindray na rzecz cyberbezpieczeństwa wykracza poza zwykłą **zgodność** z międzynarodowymi normami i przepisami. Chodzi o kultywowanie kultury bezpieczeństwa, która przenika każdy aspekt naszej organizacji. Mindray ma cyberbezpieczeństwo na względzie na każdym etapie cyklu życia produktu — od początkowej fazy projektowania aż po nadzór po wprowadzeniu produktu na rynek. **Certyfikaty przyznane firmie Mindray** są dowodem naszego zaangażowania w zapewnianie najwyższego poziomu bezpieczeństwa i ochrony prywatności. Certyfikaty te nie są zwykłymi wyróżnieniami. Są one świadectwem naszego nieustannego dążenia do doskonałości oraz zaangażowania w ochronę dobrostanu pacjentów i ochrony ich wrażliwych danych przetwarzanych przez nasze urządzenia.

W kontekście **wspólnej odpowiedzialności** Mindray przyznaje, że cyberbezpieczeństwo w opiece zdrowotnej to wspólny wysiłek. Aktywnie współpracujemy z zakładami opieki zdrowotnej, organami regulacyjnymi i innymi interesariuszami, aby stworzyć bezpieczne środowisko opieki nad pacjentem. Ta współpraca jest niezbędna do wskazywania potencjalnych zagrożeń, reagowania na zdarzenia i wzmacniania poziomu bezpieczeństwa na globalnym rynku służby zdrowia. Poprzez promowanie otwartej komunikacji i współpracy dążymy do stworzenia skutecznej obrony przed cyberzagrożeniami.

Filary **modelu cyberbezpieczeństwa produktów Mindray** — zarządzanie i ocena ryzyka, bezpieczne projektowanie i rozwój, środki ochronne i kontrolne, konserwacja i zarządzanie cyklem życia, zarządzanie zdarzeniami i ochrona danych — odzwierciedlają holistyczną strategię, która uwzględnia wieloaspektowy charakter cyberbezpieczeństwa. Każdy filar stanowi krytyczny element naszej wszechstronnej struktury bezpieczeństwa, zapewniając, że nasze urządzenia są nie tylko zgodne z obecnymi standardami, ale także odporne na przyszłe zagrożenia.

Rozumiemy, że zaufanie pokładane w nas i naszych urządzeniach to zobowiązanie, któremu musimy sprostać z niezachwianym oddaniem. W obliczu złożoności ery cyfrowej firma Mindray będzie nadal opierała swoją działalność na uczciwości, innowacyjności i naszym zaangażowaniu na rzecz ochrony systemu opieki zdrowotnej.

Nawigowanie po cyfryzacji opieki zdrowotnej: droga do bezpiecznych innowacji

Na przestrzeni kilku ostatnich dekad branża urządzeń medycznych i opieki zdrowotnej przeszła znaczącą transformację napędzaną przez szybki postęp technologiczny i cyfryzację. Innowacje, takie jak telemedycyna, przenośne urządzenia do monitorowania stanu zdrowia i zdalne narzędzia diagnostyczne zrewolucjonizowały opiekę nad pacjentami, która stała się bardziej wydajna, dokładna i dostępna. Pacjenci mogą dziś korzystać ze spersonalizowanych planów leczenia, monitorowania stanu zdrowia w czasie rzeczywistym i z jak najmniej inwazyjnych procedur, co znacznie poprawia skuteczność leczenia i ogólną jakość życia.

Coraz szersze wykorzystanie zintegrowanych technologii cyfrowych w branży prowadzi do wzrostu zagrożeń cyberbezpieczeństwa. Integracja urządzeń medycznych z sieciami szpitalnymi i platformami opartymi na chmurze stworzyła nowe luki w zabezpieczeniach. Pokazuje to, jak bardzo potrzeba skutecznych środków bezpieczeństwa, które mają zapewnić niezawodności urządzeń i ochronę wrażliwych danych pacjentów.

W ostatnich latach w sektorze opieki zdrowotnej doszło do wielu poważnych naruszeń cyberbezpieczeństwa, podobnych do ataków z użyciem oprogramowania WannaCry. Na przykład, atak ransomware na centrum medyczne Springhill[1] sparaliżował systemy szpitalne, przyczyniając się do śmierci noworodka w wyniku awarii krytycznych systemów monitorowania podczas porodu. Atak ransomware na University of Vermont Health Network[2] z 2020 roku spowodował znaczące zakłócenia w działaniu placówki, opóźniając opiekę nad pacjentami i zmuszając szpitale do powrotu do papierowej dokumentacji. Ataki typu medjack[3], których celem były urządzenia medyczne, takie jak pompy infuzyjne i aparaty do rezonansu magnetycznego, wykorzystywały przestarzałe oprogramowanie i nieodpowiednie środki bezpieczeństwa w celu wniknięcia w szersze sieci szpitalne i przejęcia nad nimi kontroli. Oprogramowanie ransomware NotPetya[4] poważnie wpłynęło na działanie służby zdrowia na całym świecie poprzez wykorzystanie exploitu EternalBlue[5], zaszyfrowanie krytycznych danych i zakłócanie usług. Wszystkie te zdarzenia podkreślają, jak poważny wpływ mogą mieć cyberataki na systemy opieki zdrowotnej, naruszając poufność danych pacjentów i zakłócając świadczenie podstawowych usług medycznych.

W świetle tych wyzwań Mindray zamierza podążać ścieżką innowacji, osiągając przy tym równowagę między wykorzystaniem postępu technologicznego i wyposażeniem naszych urządzeń medycznych w solidne zabezpieczenia. Poprzez przyjęcie rygorystycznych standardów, zgodność z międzynarodowymi wymogami oraz promowanie przejrzystości i wspólnej odpowiedzialności. Mindray stara się zapewnić, że wprowadzane innowacje są bezpieczne i godne zaufania oraz umożliwiają lepszą opiekę nad pacjentem bez poświęcania bezpieczeństwa.

[1] https://www.healthcareitnews.com/news/hospital-ransomware-attack -led-infants-death-lawsuit-alleges
[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

Stanowisko firmy Mindray w sprawie cyberbezpieczeństwa

Uznając rosnące ryzyko zagrożeń cyberbezpieczeństwa, Mindray zobowiązuje się do ciągłego doskonalenia naszych procesów i systemów w celu zintegrowania cyberbezpieczeństwa i ochrony prywatności w każdym aspekcie.

- Przywództwo z wizją
- Bezpieczeństwo dzięki przejrzystości i zaufaniu
- Solidne fundamenty bezpieczeństwa korporacyjnego
- Zgodność i przestrzeganie standardów
- Ochrona w partnerstwie: wspólna odpowiedzialność

Stanowisko firmy Mindray w sprawie cyberbezpieczeństwa

Przywództwo z wizją

Firma Mindray jest wiodącym producentem urządzeń medycznych i rozwiązań, który postawił sobie za cel zaoferowanie wszystkim ludziom lepszej opieki medycznej. Od momentu założenia w 1991 r. firma Mindray koncentrowała się na trzech głównych liniach produktowych: monitorowanie pacjenta i podtrzymywanie życia (PMLS), obrazowanie medyczne (MIS) i diagnostyka in vitro (IVD).

Główna siedziba firmy jest zlokalizowana w Shenzhen w Chinach. Firma ma 42 międzynarodowe spółki zależne i oddziały w 32 krajach, zatrudniając około 7500 pracowników na całym świecie, którzy wspierają różne zakłady opieki zdrowotnej. O zaangażowaniu firmy w innowacje świadczy 12 globalnych centrów badawczo-rozwojowych oraz inwestycje w badania i rozwój na poziomie 10% rocznych przychodów.

Bezpieczeństwo dzięki przejrzystości i zaufaniu

W Mindray nasze zasady i wartości dotyczące bezpieczeństwa produktów mają źródło w niezachwianym zaangażowaniu w ochronę bezpieczeństwa pacjentów, wzmacnianie integralności naszych urządzeń medycznych i ochronę danych wrażliwych. Kierując się międzynarodowymi standardami i najlepszymi praktykami, postawiliśmy sobie za cel przejrzystość, odpowiedzialność i nieustanne doskonalenie. Koncentrujemy się na stworzeniu bezpieczniejszego i bardziej niezawodnego otoczenia opieki zdrowotnej, w którym łączą się najnowocześniejsze technologie i bezkompromisowe bezpieczeństwo, aby zapewnić ochronę i wzmacniać tych, którym służymy.

Mindray w skrócie

Europa
600+ szpitali klinicznych w Europie

USA
20 najlepszych szpitali w USA
9 z 10 najlepszych szpitali kardiologicznych w USA

Chiny
99% szpitali 1. poziomu w Chinach

Obsługa **190+** krajów i regionów

Ponad **18 000** pracowników z 30 krajów

Ponad **50** międzynarodowych oddziałów na całym świecie

4,82 mld USD przychodów w 2023 r.

4400+ inżynierów ds. badań i rozwoju na całym świecie

12 centrów badawczo-rozwojowych na całym świecie

Monitorowanie pacjenta i podtrzymywanie życia

Diagnostyka in vitro

System obrazowania medycznego

„Zaufanie buduje się nie przez pokazywanie tego, co robimy, ale jak to robimy. Przejrzyste podejście Mindray do cyberbezpieczeństwa zapewnia naszym klientom pełny dostęp do informacji o stosowanych przez nas praktykach bezpieczeństwa. Dzięki przejrzystości i otwartości naszych praktyk cyberbezpieczeństwa klienci zyskują pewność, której potrzebują".

Cheng Minghe
Wiceprzewodniczący, członek rady ds. zgodności z przepisami Mindray

„Staramy się, aby bezpieczeństwo było zintegrowane ze strukturą każdego produkowanego przez nas urządzenia, co zapewnia ich niezawodność i odporność na ataki w najważniejszych obszarach opieki zdrowotnej. Cyberbezpieczeństwo to nie dodatek. To podstawowa zasada, według której projektujemy, rozwijamy i produkujemy każde urządzenie medyczne".

Li Zaiwen
Starszy wiceprezes, członek rady ds. zgodności z przepisami Mindray

Jesteśmy producentem urządzeń medycznych w branży ochrony zdrowia, więc pojęcie „przejrzystości" jest fundamentem naszych zasad i wartości. Nasza wizja wykracza poza zwykłą zgodność. Odzwierciedla to nasze intensywne starania i zobowiązanie na rzecz umożliwienia naszym użytkownikom podejmowania świadomych decyzji. Agencja FDA[6] opowiada się za jasną i otwartą komunikacją na temat funkcji cyberbezpieczeństwa urządzeń i potencjalnych zagrożeń w celu budowania zaufania wśród świadczeniodawców, organów regulacyjnych i pacjentów. Poprzez różne formy udostępniania informacji, w tym białe księgi, instrukcje obsługi i dokumentację techniczną, Mindray dąży do nieustannego zwiększania swojego zobowiązania na rzecz utrzymania przejrzystości w zakresie wdrożonych środków bezpieczeństwa, ustaleń dotyczących ryzyka oraz metod ochrony pacjentów i przetwarzania wrażliwych danych.

Wdrażając zasady bezpieczeństwa i prywatności w fazie projektowania naszych produktów, dokładamy starań, aby zapewnić cyberbezpieczeństwo i prywatność na poziomie koncepcji naszych urządzeń medycznych. Tylko w ten sposób możemy osiągnąć niezawodność podstawowych usług medycznych i nienaruszalność poufności danych. Nasza dokładna struktura zarządzania ryzykiem nieustannie ocenia i minimalizuje potencjalne zagrożenia bezpieczeństwa, zapewniając naszym urządzeniom nie tylko bezpieczeństwo, ale także odporność i niezawodność. Poprzez ścisłą współpracę z zakładami opieki zdrowotnej, organami regulacyjnymi i partnerami z branży dążymy do stworzenia kultury bezpieczeństwa, która wzmacnia zaufanie i pewność w globalnym ekosystemie ochrony zdrowia.

Bezpieczeństwo i prywatność w fazie projektowania

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

Solidne fundamenty bezpieczeństwa korporacyjnego

W Mindray nasze podejście do cyberbezpieczeństwa wpływa na cały nasz etos organizacyjny, co przekłada się na poszczególne produkty i usługi. Zdajemy sobie sprawę, że wysokie bezpieczeństwo informacji **przedsiębiorstwa** ma ogromne znaczenie dla rozwoju i utrzymania zaufania do nas i naszych urządzeń. Tak solidne podstawy można osiągnąć wyłącznie dzięki doświadczonym i przeszkolonym **pracownikom**, którzy projektują oraz dostarczają bezpieczne i niezawodne usługi oraz **produkty**.

Ta wszechstronna strategia bezpieczeństwa, która cyklicznie wzmacnia praktyki w zakresie bezpieczeństwa naszej firmy, kompetencje pracowników i innowacje produktowe, ilustruje symbiotyczną relację niezbędną do zapewnienia ochrony przed cyberzagrożeniami zarówno naszej działalności, jak i produktom, dając klientom i interesariuszom poczucie pewności.

Ujednolicona kultura bezpieczeństwa: Fundamentem kultury korporacyjnej Mindray jest świadomość bezpieczeństwa i najlepsze praktyki. Promujemy podejście oparte na trosce o bezpieczeństwo wśród wszystkich pracowników, od kadry zarządzającej po laboratorium rozwojowe. Ta kultura czujności kształtowana jest poprzez regularne szkolenia obejmujące nie tylko zasady „bezpieczeństwa i prywatności w fazie projektowania", ale także szerzej pojmowane bezpieczeństwo informacji i ochronę prywatności. Ten rozbudowany system szkoleniowy umożliwia włączenie zaawansowanych funkcji bezpieczeństwa i prywatności do codziennych operacji i projektów produktów, wzmacniając wiarygodność i zgodność naszej firmy oraz urządzeń.

Odporna infrastruktura: Nasza infrastruktura bezpieczeństwa korporacyjnego ma na celu zapewnienie stabilności operacyjnej i poufności danych, które mają kluczowe znaczenie dla ciągłości i niezawodności naszej działalności biznesowej oraz obsługi klienta. Zabezpieczając nasze centra danych, sieci i architektury oprogramowania przed zakłóceniami i naruszeniami, zapewniamy, że systemy wspierające rozwój naszych produktów i usługi konserwacyjne są zawsze dostępne i bezpieczne.

Proaktywne reagowanie na zdarzenia i ciągłe doskonalenie: Dzięki dynamicznym możliwościom reagowania na zdarzenia i ciągłej ocenie bezpieczeństwa w Mindray możemy szybko reagować na potencjalne cyberataki i luki w zabezpieczeniach, zarówno na poziomie przedsiębiorstwa, jak i produktu. Ta proaktywna postawa nie tylko pomaga ograniczać ryzyko, ale także wpływa na ciągłe ulepszanie naszych funkcji zabezpieczających dla przedsiębiorstw i produktów w oparciu o rzeczywiste dane i charakter pojawiających się zagrożeń.

Zaangażowanie interesariuszy i przejrzystość: W Mindray staramy się prowadzić otwarty dialog na temat naszych procesów bezpieczeństwa i rozwoju. Zachowując przejrzystość w zakresie naszych strategii bezpieczeństwa przedsiębiorstwa i produktów, chcemy zyskać jeszcze większe zaufanie klientów, zapewniając ich o naszym dążeniu do zachowania wysokich standardów bezpieczeństwa oraz ochrony pacjentów i ich poufnych informacji.

Firma: obrona strategiczna

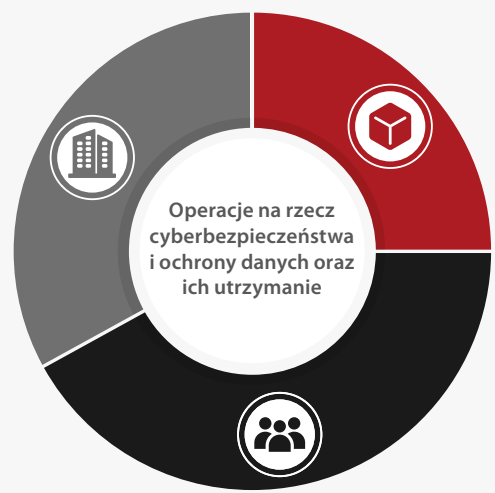
Utrzymywanie niezawodnych zabezpieczeń przedsiębiorstwa przez wdrożenie kompleksowych planów reagowania i niezwykle odpornej infrastruktury. Zapewniają one stabilność operacyjną oraz pozwalają na stałe usprawnianie ochrony systemów wewnętrznych i danych.

Ludzie: doskonalenie osób odpowiedzialnych za bezpieczeństwo

Dzięki szeroko zakrojonym szkoleniom w zakresie praktyk bezpieczeństwa i norm zachowania poufności informacji nasi pracownicy rozwijają naszą kulturę bezpieczeństwa.

Produkt: bezpieczeństwo na poziomie koncepcji

Wyposażenie wszystkich urządzeń medycznych w silne zabezpieczenia już na etapie projektowania oraz budowanie zaufania naszych klientów i dostarczanie im niezawodnych rozwiązań.



Zgodność i przestrzeganie standardów

W Mindray mamy świadomość ogromnego wpływu i znaczenia przestrzegania międzynarodowych norm i certyfikacji na zapewnienie najwyższych poziomów jakości, bezpieczeństwa i cyberbezpieczeństwa produktów. Nasze zobowiązanie do przestrzegania tych standardów wynika nie tylko z chęci zachowania zgodności z przepisami czy zdobycia certyfikatów, ale przede wszystkim wzbudzenia w naszych klientach i użytkownikach poczucia zaufania i bezpieczeństwa. Zapewnia to naszych interesariuszy, że działamy z zachowaniem najwyższej rzetelności, dając im gwarancję, że nasze produkty spełniają surowe normy jakości i bezpieczeństwa. To poczucie zaufania ma kluczowe znaczenie w sektorze opieki zdrowotnej, gdzie niezawodność i bezpieczeństwo urządzeń medycznych ma bezpośredni wpływ na opiekę nad pacjentem i jej wyniki. Te standardy i certyfikaty są zatem świadectwem naszego dążenia do zapewniania bezpieczeństwa naszej firmy i produktów oraz naszych wysiłków na rzecz ciągłego rozwoju i postępu, które popychają nas do ciągłego doskonalenia naszych praktyk.

Firma Mindray przestrzega między innymi następujących obowiązujących norm i wymagań: TIR57, ISO 14971, ISO 31000, IEC/TR 80001-2-2, wymagania i wytyczne FDA stosowane przed wprowadzeniem produktu do obrotu i po nim, MDCG 2019-16, zasady i praktyki IMDRF, europejskie ogólne rozporządzenie o ochronie danych (RODO), amerykańska ustawa o przenośności i odpowiedzialności w ubezpieczeniach zdrowotnych (HIPAA) oraz chińska ustawa o ochronie danych osobowych (PIPL). Standardy te kierują naszymi procesami — od zarządzania ryzykiem i cyberbezpieczeństwa po ogólny rozwój produktu i zarządzanie cyklem życia. Poprzez ich przestrzeganie zapewniamy, że skutecznie zarządzamy ryzykiem operacyjnym, a nasze produkty są projektowane, rozwijane i utrzymywane przy zachowaniu najwyższych poziomów bezpieczeństwa i ochrony.

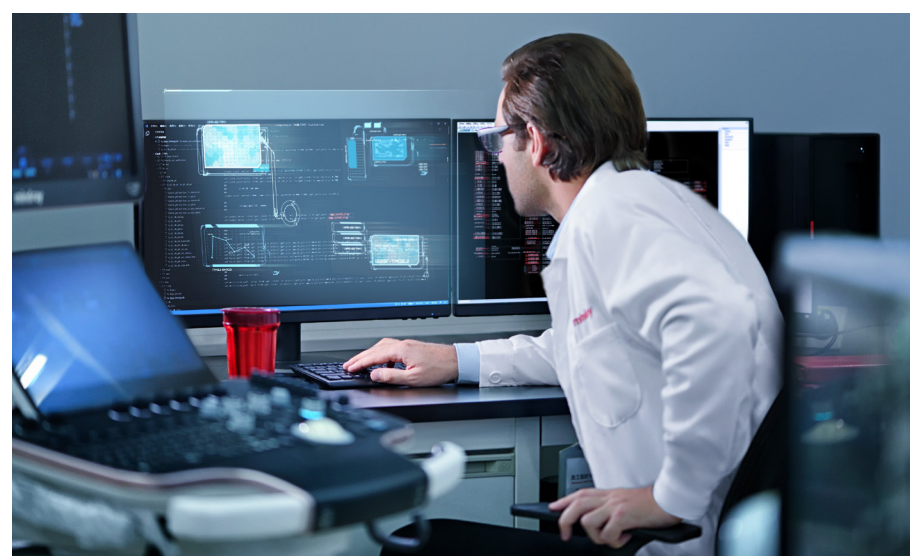
Firma Mindray uzyskała kilka prestiżowych certyfikatów, w tym ISO/IEC 27001:2022 w zakresie zarządzania bezpieczeństwem informacji oraz ISO/IEC 27701:2019 w zakresie zarządzania prywatnością informacji. Obejmują one różne aspekty naszej działalności, takie jak badania i rozwój, sprzedaż, serwis, IT itp., co pokazuje nasze kompleksowe podejście do zgodności i bezpieczeństwa. Wśród innych otrzymanych przez nas certyfikatów warto wymienić m.in. NEN7510 w zakresie bezpieczeństwa informacji w służbie zdrowia czy UL2900-2–1 dotyczący urządzeń podłączanych do sieci.

UL Solutions

Zastosowanie określonych standardów i certyfikatów zależy od konkretnego produktu oraz regionów, w których jest sprzedawany. Na przykład, obowiązujące wymagania FDA są spełniane dla urządzeń zgodnie ze ścieżkami regulacyjnymi i wytycznymi, takimi jak zgłoszenie 510 (k). Poprzez dokładne badania i monitorowanie zapewniamy, że nasze produkty spełniają odpowiednie wymogi regulacyjne w oparciu o ich docelowe rynki i zastosowania.

Poprzez wypełnianie tych standardów oraz zdobywanie i utrzymywanie certyfikacji Mindray pragnie zademonstrować swoje dążenie do doskonałości, zwiększania swojej wiarygodności oraz nieustannego poszukiwania innowacji i ulepszeń. To wszystko zapewnia, że konsekwentnie dostarczamy bezpieczne i niezawodne urządzenia oraz usługi medyczne zakładom opieki zdrowotnej i pacjentom na całym świecie.

Nasze zobowiązanie do przestrzegania tych standardów wynika nie tylko z chęci zachowania zgodności z przepisami czy zdobycia certyfikatów, ale przede wszystkim wzbudzenia w naszych klientach i użytkownikach poczucia zaufania i bezpieczeństwa.



Ochrona w partnerstwie: wspólna odpowiedzialność

W Mindray uważamy, że cyberbezpieczeństwo w branży opieki zdrowotnej i urządzeń medycznych jest wspólnym obowiązkiem. Istota ekosystemu współpracujących ze sobą urządzeń medycznych niejako wymusza na producentach i zakładach opieki zdrowotnej konieczność wypracowania odpowiednich praktyk cyberbezpieczeństwa. Producenci urządzeń są odpowiedzialni za tworzenie bezpiecznych produktów poprzez przestrzeganie przepisów branżowych, integrację solidnych funkcji zabezpieczeń na etapie projektowania i rozwoju, przeprowadzanie rygorystycznych testów oraz terminowe dostarczanie aktualizacji oprogramowania i poprawek w celu wyeliminowania luk w zabezpieczeniach. Muszą także oferować jasne wytyczne dotyczące bezpiecznego korzystania z urządzeń i zapewniać ich konserwację. Z drugiej strony, zakłady opieki zdrowotnej odgrywają kluczową rolę w zarządzaniu bezpieczeństwem po wdrożeniu urządzenia w swoich systemach. Obejmuje to zastosowanie odpowiednich konfiguracji sieci, kontrolowanie fizycznego dostępu do urządzeń i ciągłe monitorowanie pod kątem potencjalnych zagrożeń. Placówki opieki zdrowotnej muszą również zapewnić, że pracownicy są odpowiednio przeszkoleni w zakresie najlepszych praktyk bezpieczeństwa, poszerzają swoją wiedzę na temat funkcji technicznych i przestrzegają protokołów w celu zapewniania ochrony zarówno obsługiwanych urządzeń, jak i wrażliwych danych, które przetwarzają. Dzięki tej współpracy zarówno producenci, jak i zakłady opieki zdrowotnej przyczyniają się do tworzenia bezpiecznego ekosystemu, równoważąc innowacyjność z bezpieczeństwem pacjentów i ochroną danych.

Zasadę tę popiera nie tylko Mindray, ale także liczne instytucje badawcze, środowiska akademickie i inne firmy z branży. Według Międzynarodowego Forum Regulatorów Wyrobów Medycznych (IMDRF)[7] cyberbezpieczeństwo urządzeń medycznych wymaga ścisłej współpracy między producentami urządzeń a zakładami opieki zdrowotnej, co podkreśla znaczenie wspólnej odpowiedzialności w całym cyklu życia urządzenia. Dzięki takiemu podejściu wszystkie strony korzystające z urządzeń medycznych i nimi zarządzające wiedzą, jak zapobiegać zagrożeniom cyberbezpieczeństwa, co zwiększa ich ogólną odporność. Agencja FDA[8] dodatkowo podkreśla, że ochrona przed cyberatakami i reagowanie na nie to wspólna odpowiedzialność wszystkich podmiotów w ekosystemie urządzeń medycznych, w tym placówek opieki zdrowotnej, pacjentów, usługodawców i producentów sprzętu. Ta współpraca pomaga w identyfikowaniu i ograniczaniu ryzyka, a także w skuteczniejszym reagowaniu na zdarzenia i przywracaniu sprawności po ich wystąpieniu.

Promując taką koncepcję wspólnej odpowiedzialności, Mindray dąży do ścisłej współpracy ze wszystkimi zainteresowanymi stronami, w szczególności z zakładami opieki zdrowotnej, w celu zapewnienia im odpowiednich narzędzi do zapobiegania i reagowania na zagrożenia cyberbezpieczeństwa, co w efekcie ma chronić zdrowie i bezpieczeństwo pacjentów.

[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

Model cyberbezpieczeństwa produktów firmy Mindray

Mindray wdraża wewnętrznie opracowane ramy bezpieczeństwa mające zapewnić ochronę naszych urządzeń medycznych, pokazując wszystkim zespołom i oddziałom firmy Mindray, jak wdrażać wytyczne w zakresie cyberbezpieczeństwa.

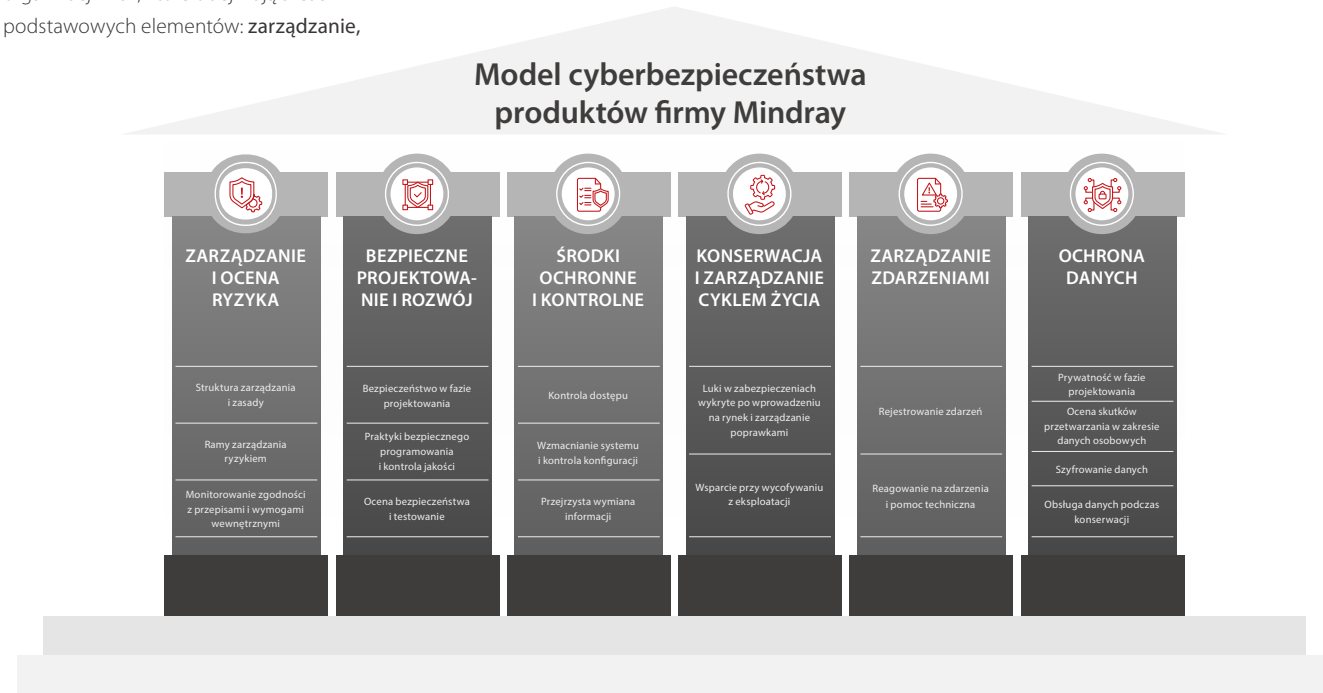
- Zarządzanie i ocena ryzyka
- Bezpieczne projektowanie i rozwój
- Środki ochronne i kontrolne
- Konserwacja i zarządzanie cyklem życia
- Zarządzanie zdarzeniami
- Ochrona danych

Model cyberbezpieczeństwa produktów firmy Mindray

Cyberbezpieczeństwo produktów firmy Mindray jest nierozłącznie związane z modelem cyberbezpieczeństwa produktów firmy Mindray. Są to wewnętrznie opracowane ramy bezpieczeństwa mające zapewnić ochronę naszych urządzeń medycznych, a także pokazywać wszystkim zespołom i oddziałom firmy Mindray, jak wdrażać wytyczne w zakresie cyberbezpieczeństwa. Nasz model opiera się na zasadach Cybersecurity Framework (CSF)[9] organizacji NIST, które obejmują sześć podstawowych elementów: **zarządzanie, identyfikowanie, ochrona, wykrywanie, reagowanie i odzyskiwanie.** Opierając się na tych uznanych podstawach, dostosowaliśmy nasz model do wyzwań i wymagań branży urządzeń medycznych.

Model składa się z sześciu filarów i 17 elementów. Każdy filar spełnia międzynarodowe standardy i wymogi regulacyjne, uwzględniając wszystkie krytyczne aspekty cyberbezpieczeństwa produktu.

Filar **zarządzania i oceny ryzyka** zapewnia ustrukturyzowane podejście do zarządzania zagrożeniami cyberbezpieczeństwa zgodne ze standardami branżowymi i wymogami regulacyjnymi. **Bezpieczne projektowanie i rozwój** uwzgledniają praktyki bezpieczeństwa od samego początku cyklu życia produktu, wykorzystując najlepsze standardy, takie jak bezpieczne kodowanie i rygorystyczne testy. **Środki ochronne i kontrolne** wdrażają zabezpieczenia techniczne, takie jak kontrola dostępu i wzmacnianie systemu, w celu ochrony przed nieautoryzowanym dostępem i zagrożeniami cybernetycznymi. **Konserwacja i zarządzanie cyklem życia** koncentruje się na ciągłym kontrolowaniu bezpieczeństwa urządzeń poprzez skuteczne zarządzanie lukami w zabezpieczeniach i bezpieczne wycofywanie produktów z eksploatacji. Filar **zarządzania zdarzeniami** ustanawia procesy wykrywania, reagowania i analizowania zdarzeń związanych z cyberbezpieczeństwem, podkreślając wspólną odpowiedzialność firmy Mindray i zakładów opieki zdrowotnej. Wreszcie filar **ochrony danych** zapewnia poufność, integralność i dostępność danych pacjentów poprzez uwzględnienie ochrony prywatności w fazie projektowania, ocenę wpływu na prywatność, szyfrowanie i rozbudowane środki kontroli podczas przetwarzania danych.



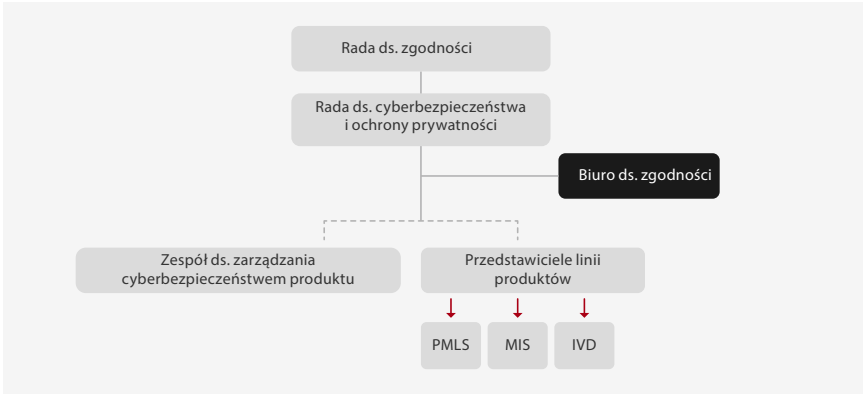
[9] https://www.nist.gov/cyberframework

Zarządzanie i ocena ryzyka

Cyberbezpieczeństwo produktów Mindray opiera się na solidnych podstawach obejmujących ustrukturyzowane zasady zarządzania, ramy zarządzania ryzykiem i metodologię monitorowania zgodności.

Struktura zarządzania i zasady

Usprawniając proces podejmowania strategicznych decyzji i wdrażania zasad, ustanowiliśmy wyraźne zakresy odpowiedzialności i kanały komunikacyjne.



Rada ds. zgodności, złożona z członków kierownictwa najwyższego szczebla firmy Mindray, wskazuje i nadzoruje nasze działania w zakresie cyberbezpieczeństwa. Czuwa nad różnymi obszarami, w tym strategiami i planami dotyczącymi cyberbezpieczeństwa oraz zgodności z przepisami w zakresie ochrony prywatności. Rada przewodzi wszystkim inicjatywom firmy i działaniom na rzecz zgodności, a także podejmuje kluczowe decyzje dotyczące głównego planu rozwoju.

Rada ds. cyberbezpieczeństwa i ochrony prywatności określa zasady oraz cele firmy w zakresie cyberbezpieczeństwa i ochrony prywatności zarówno na poziomie przedsiębiorstwa, jak i produktu. Rada wskazuje i weryfikuje odpowiednie wewnętrzne zasady i programy ramowe, a także zarządza pełnym wdrożeniem w jednostkach biznesowych we wszystkich regionach i sprawuje nad nim nadzór.

Biuro ds. zgodności wspiera codzienne działania rad, na bieżąco informuje zespół o różnych przepisach i regulacjach oraz koordynuje prace nad redagowaniem zasad i programów ramowych. Biuro to wspiera rady w nadzorowaniu i kontrolowaniu prawidłowego wdrażania środków cyberbezpieczeństwa i ochrony prywatności, aktywnie wspierając skuteczne dostosowywanie zasad przez jednostki biznesowe w różnych regionach.

Zespół ds. zarządzania cyberbezpieczeństwem produktu zajmuje się technicznymi aspektami cyberbezpieczeństwa urządzeń, odgrywając kluczową rolę we wspieraniu rady i biura ds. zgodności. Odpowiada on za ustanowienie wewnętrznych wymogów i standardów w zakresie cyberbezpieczeństwa. Główne obowiązki obejmują wskazywanie, promowanie i stosowanie niezbędnych technologii cyberbezpieczeństwa i metod testowania, monitorowanie i ocenę podatności, a także zapewnianie wsparcia technicznego podczas badań w kluczowych obszarach, takich jak reagowanie na luki w zabezpieczeniach i bezpieczne tworzenie oprogramowania.

Przedstawiciele linii produktów, jako jednostka odpowiedzialna za rozwój produktu, są odpowiedzialni za wdrażanie wymogów i standardów określonych przez radę, biuro i zespół ds. zarządzania cyberbezpieczeństwem produktu na każdym etapie cyklu życia produktu, takim jak rozwój, produkcja, konserwacja itp. Zapewniają, że przyjęte cyberzabezpieczenia są zintegrowane z każdym produktem. Przekazują także kierownictwu terminowe uwagi na temat potrzeb i problemów związanych z cyberbezpieczeństwem oraz współpracują nad zwiększaniem ogólnych zdolności grupy w zakresie zarządzania cyberbezpieczeństwem produktów.

Ramy zarządzania ryzykiem

Solidne ramy zarządzania ryzykiem to fundament strategii cyberbezpieczeństwa firmy Mindray. Umożliwiają nam szybkie identyfikowanie, ocenę i eliminowanie potencjalnych luk w zabezpieczeniach w sposób systemowy w całym cyklu życia produktu.

Nasze ramy zarządzania ryzykiem rozpoczynają się od szczegółowej oceny zagrożeń przy użyciu programu modelowania zagrożeń STRIDE, który rozpoznaje i kategoryzuje potencjalne zagrożenia związane ze spoofingiem, manipulacją, odrzuceniem, ujawnieniem informacji, odmową usługi i podniesieniem uprawnień. Proces ten pozwala nam dogłębnie zrozumieć możliwe formy zagrożeń i ocenić ich potencjalny wpływ na bezpieczeństwo urządzeń.

Nasze wysiłki w zakresie zarządzania ryzykiem obejmują utworzenie szczegółowego planu zarządzania ryzykiem, zestawienie materiałów oprogramowania (SBOM), ocenę ryzyka związanego ze znanymi lukami oraz raporty z testów penetracyjnych i skanowania. Dokumenty te zawierają dokładny przegląd wdrożonych środków bezpieczeństwa i stanowią świadectwo naszego zaangażowania na rzecz bezpieczeństwa produktów. Wyniki tych analiz pozwalają nam lepiej zaprojektować nasze mechanizmy kontroli ryzyka wpisane w określone wymogi bezpieczeństwa produktu, które kierują kolejnymi fazami projektowania i testowania.

Nasza analiza ryzyka związanego z cyberbezpieczeństwem nie jest jednorazowym działaniem, ale ciągłym procesem, który przebiega przez cały cykl życia produktu. Takie podejście pozwala na wczesne wykrywanie i neutralizowanie potencjalnych zagrożeń, redukując tym samym ryzyko naruszeń bezpieczeństwa po wdrożeniu.

Monitorowanie zgodności z przepisami i wymogami wewnętrznymi

Monitorowanie zgodności z przepisami jest ważnym elementem naszej strategii cyberbezpieczeństwa. Pozwala nam na dopasowanie wewnętrznych standardów do wymogów określonych w przepisach i praktyk powszechnie stosowanych w branży. Rada ds. cyberbezpieczeństwa i ochrony prywatności zapewnia, że wymogi regulacyjne są stale oceniane, a wszelkie istotne zmiany w standardach i wymaganiach dotyczących rozwoju produktów są niezwłocznie wprowadzane. Aby wyjść poza minimalne wymogi zgodności, Mindray nieustannie prowadzi badania i porównuje się z najlepszymi w branży. Takie proaktywne podejście sprawia, że zabezpieczenia stosowane przez firmę są skuteczne i aktualne oraz odzwierciedlają najnowsze postępy i trendy w zakresie cyberbezpieczeństwa.

Aby zapewnić, że opracowane standardy bezpieczeństwa są wdrażane zgodnie z przeznaczeniem, Mindray stosuje także „tabelę weryfikacyjną cyberbezpieczeństwa i danych w odniesieniu do badań i rozwoju". Pozwala ona sprawdzić, czy praktyki w zakresie rozwoju i produkcji są zgodne z ustalonymi wytycznymi i wymaganiami. Tabela ta służy jako lista kontrolna na potrzeby audytów wewnętrznych, zapewniając kontrolę jakości.

Bezpieczne projektowanie i rozwój

Bezpieczeństwo w fazie projektowania

Jak pokazaliśmy wcześniej, bezpieczeństwo w fazie projektowania stanowi podstawę ideologii firmy Mindray, która zapewnia wdrażanie zasad i wymogów dotyczących bezpieczeństwa już na etapie projektowania produktu. Ta podstawowa filozofia jest osadzona i odzwierciedlona w naszych rozbudowanych systemach i zasadach, które zapewniają, że specyfikacje dotyczące zabezpieczeń są brane pod uwagę od samego początku i zakorzenione w naszym podejściu do projektowania produktów. Działania związane z cyklem rozwoju zabezpieczeń są ściśle zintegrowane z naszym ogólnym procesem rozwoju produktu, co zapewnia stosowanie najlepszych praktyk w zakresie cyberbezpieczeństwa.

Projektując wszystkie nasze produkty, opieramy się na zasadzie głębokiej obrony, która stanowi fundament podejścia **„bezpieczeństwo w fazie projektowania".** Ta wielopoziomowa strategia obrony gwarantuje, że nawet w przypadku niesprawności jednego zabezpieczenia pozostałe warstwy ochrony nadal będą zabezpieczać urządzenie i przechowywane na nim dane.

Praktyki bezpiecznego programowania i kontrola jakości

Opierając się na zasadach bezpieczeństwa w fazie projektowania, opracowaliśmy **kompleksowe i systemowe standardy bezpiecznego programowania**. W tym celu korzystaliśmy z norm Międzynarodowej Komisji Elektrotechnicznej (IEC), najlepszych praktyk z branży, a także naszego ogromnego doświadczenia w rozwoju oprogramowania. Nasze standardy bezpiecznego kodowania obejmują różne kluczowe aspekty programowania, **w tym walidację danych wejściowych, obsługę błędów i uwierzytelnianie.** Zasady te pozwalają na usunięcie potencjalnych luk w zabezpieczeniach na etapie kodowania, znacznie zmniejszając ryzyko wystąpienia luk w produktach końcowych.

Kontrola procesu i **standardy zapewnienia jakości** są kolejnymi kluczowymi elementami bezpiecznego kodowania. Dzięki naszej **3-etapowej procedurze przeglądu kodu,** która obejmuje ocenę listy kontrolnej z wykorzystaniem ustalonych standardów bazowych, statyczny przegląd kodu z wykorzystaniem zaawansowanych narzędzi oraz ręczną walidację przez człowieka, Mindray zapewnia, że wszyscy inżynierowie oprogramowania przestrzegają standardów bezpiecznego kodowania w całym procesie rozwoju.

Ponadto w Mindray dokładamy wszelkich starań, aby zapewnić naszym programistom otoczenie i warunki sprzyjające ciągłemu doskonaleniu i wymianie wiedzy. Wszyscy programiści przechodzą regularne szkolenia w zakresie technik bezpiecznego kodowania i są na bieżąco z najnowszymi lukami w zabezpieczeniach oraz sposobami ich eliminowania. Dzięki takiemu proaktywnemu podejściu nasi inżynierowie są dobrze przygotowani do radzenia sobie z pojawiającymi się zagrożeniami.

Ocena bezpieczeństwa i testowanie

Firma Mindray wdrożyła też procedury oceny bezpieczeństwa i testowania, aby umożliwić identyfikację potencjalnych luk w zabezpieczeniach i ich wyeliminowanie, a także testowanie i weryfikowanie wdrażanych zabezpieczeń.

- **Wyszukiwanie luk w zabezpieczeniach:**
  Używamy zaawansowanych narzędzi, aby regularnie skanować nasze produkty i systemy pod kątem potencjalnych luk w zabezpieczeniach, proaktywnego rozpoznawania zagrożeń i szybkiego stosowania niezbędnych poprawek.
- **Testy penetracyjne:**
  Symulowane złożone cyberataki są przeprowadzane w celu przetestowania odporności urządzeń w warunkach rzeczywistych.
- **Zewnętrzna ocena bezpieczeństwa:**
  Do oceny bezpieczeństwa angażujemy niezależne organizacje zewnętrzne. Stanowi to dodatkowy poziom weryfikacji i gwarancji, a także zapewnia zgodność naszych produktów ze standardami branżowymi i regulacyjnymi.

To kompleksowe podejście podkreśla nasze zaangażowanie na rzecz dostarczania urządzeń medycznych, które są bezpieczne, niezawodne i zgodne z przepisami, a tym samym zapewnia użytkownikom poczucie spokoju w stale zmieniającym się świecie cyberbezpieczeństwa.

Środki ochronne i kontrolne

W myśl zasady wspólnej odpowiedzialności wyposażenie urządzeń medycznych w niezbędne funkcje i możliwości ochronne jest podstawowym obowiązkiem firmy Mindray jako producenta urządzeń.

Kontrola dostępu

Kontrola dostępu, w tym mechanizmy takie jak **uwierzytelnianie, autoryzacja i rozliczanie**, jest krytycznym elementem bezpieczeństwa urządzeń medycznych, który zapewnia, że tylko upoważnione osoby mają dostęp do poufnych informacji i funkcji systemu. Urządzenia medyczne Mindray są wyposażone w mechanizm **kontroli dostępu opartej na rolach (RBAC)**, który nadaje poszczególnym użytkownikom uprawnienia na podstawie ich roli w organizacji. Dzięki temu organizacje mogą przyznawać użytkownikom minimalny dostęp w zależności od ich potrzeb operacyjnych, zmniejszając w ten sposób ryzyko nieautoryzowanego dostępu do plików lub dowolnych zmian konfiguracji.

Urządzenia Mindray, choć różnią się w zależności od modelu, posiadają kilka dodatkowych zabezpieczeń w celu zwiększenia bezpieczeństwa dostępu. Obejmują one między innymi te funkcje:

Mechanizm blokowania	Po określonej liczbie kolejnych nieudanych prób logowania urządzenie jest blokowane. Zapobiega to nieautoryzowanemu dostępowi w wyniku ataków siłowych.
Automatyczne wylogowywanie	Aby zapobiec nieautoryzowanemu dostępowi, gdy urządzenie jest pozostawione bez nadzoru, sesje są kończone po okresie bezczynności.
Zarządzanie hasłami	Urządzenia Mindray umożliwiają dostosowywanie zasad dotyczących haseł. Zalecamy także, aby użytkownicy regularnie zmieniali hasła.
Scentralizowane i bezpieczne uwierzytelnianie	Mindray wykorzystuje zaawansowane, bezpieczne systemy do przechowywania poświadczeń i przeprowadzania uwierzytelniania. Stosują one technologię szyfrowania, aby chronić poświadczenia i zarządzać uprawnieniami, zapewniając bezpieczne uwierzytelnianie i zmniejszając ryzyko kradzieży lub niewłaściwego użycia poświadczeń.
Kontrola ważnych zmian w konfiguracji	Ważne zmiany, takie jak aktualizacja systemu operacyjnego, podlegają rygorystycznej kontroli dostępu, umożliwiając przeprowadzanie aktualizacji tylko upoważnionym pracownikom.

Wzmacnianie systemu i kontrola konfiguracji

Zwiększanie odporności systemu na włamania to nasze kolejne działanie mające na celu zmniejszenie powierzchni ataku i w rezultacie zabezpieczenie naszych urządzeń.
Kluczowe elementy praktyk Mindray w zakresie zwiększania odporności systemu, które mogą różnić się w zależności od modelu, obejmują:

Wytyczne dotyczące zwiększania odporności systemu operacyjnego	Dla różnych funkcji systemu operacyjnego określono szczegółowy zestaw metod konfiguracji i wymagań. Zapewniają one bezpieczną konfigurację systemu operacyjnego w ujednolicony sposób we wszystkich zespołach programistycznych poprzez skuteczne wdrożenie wymagań w ustrukturyzowany sposób.
Białe listy aplikacji i procesów	Na urządzeniach można uruchamiać tylko zatwierdzone aplikacje i procesy. Zapobiega to włączaniu nieautoryzowanego oprogramowania lub wykonywaniu działań mogących zagrozić bezpieczeństwu systemu.
Programy antywirusowe i zabezpieczające przed złośliwym oprogramowaniem	Urządzenia Mindray są przystosowane do płynnej współpracy ze standardowymi programami antywirusowymi i zabezpieczającymi przed złośliwym oprogramowaniem, co zapewnia im ciągłą ochronę przed takimi zagrożeniami.
Zapora	Oparte na systemie Microsoft Windows urządzenia Mindray używają wbudowanej zapory, aby ograniczyć dostęp z zewnątrz i kontrolować aplikacje działające na urządzeniu.
Wyłączanie niepotrzebnych źródeł zagrożenia	W zależności od potrzeb biznesowych i okoliczności niepotrzebne usługi, porty i funkcje, takie jak zdalne logowanie i automatyczne uruchamianie nośników USB, są wyłączone. Ma to na celu zminimalizowanie ryzyka potencjalnych ataków.
Tryb kiosku	Urządzenia z trybem kiosku znacznie zmniejszają zasięg ataku, ograniczając dostęp użytkownika tylko do niezbędnych funkcji, zapobiegając nieautoryzowanym działaniom i minimalizując dostęp do poufnych informacji o pacjentach.
Kontrola aktualizacji systemu operacyjnego i oprogramowania.	Uaktualnienie systemu operacyjnego i oprogramowania urządzenia można przeprowadzić wyłącznie za pomocą kontrolowanych pakietów zweryfikowanych i wydanych przez firmę Mindray. Tylko autoryzowany personel może przeprowadzać uaktualnienia, a automatyczne aktualizacje systemu operacyjnego są wyłączone, aby zapobiec nieautoryzowanym zmianom.

Przejrzysta wymiana informacji

Mindray dokłada wszelkich starań, aby zachować przejrzystość zabezpieczeń stosowanych w naszych urządzeniach.
Nasze najważniejsze działania mające na celu poprawę przejrzystości to między innymi:

Dokumentacja dotycząca cyberbezpieczeństwa

Zapewniamy obszerną dokumentację dotyczącą cyberbezpieczeństwa dla każdej linii produktów, która szczegółowo opisuje środki ochrony, mechanizmy kontroli i praktyki, a także pomaga interesariuszom zrozumieć nasze działania na rzecz cyberbezpieczeństwa. Aby uzyskać dokumentację dotyczącą konkretnego produktu, należy skontaktować się z firmą Mindray.

Instrukcje obsługi produktów

Nasze instrukcje obsługi zawierają szczegółowe opisy i zalecenia dotyczące funkcji cyberbezpieczeństwa naszych produktów, pomagając użytkownikom zrozumieć istniejące mechanizmy bezpieczeństwa i sposoby ich skutecznego wykorzystania.

Oświadczenie producenta dotyczące bezpieczeństwa urządzeń medycznych (MDS2)

Mindray udostępnia oświadczenie MDS2 na żądanie, aby pomóc zakładom opieki zdrowotnej w ocenie zagrożeń cyberbezpieczeństwa i środków zaradczych związanych z naszymi urządzeniami. Niniejszy dokument przedstawia możliwości naszych urządzeń medycznych w zakresie bezpieczeństwa, oferując przejrzystość w kwestii zgodności naszych produktów z niezbędnymi wymogami bezpieczeństwa i normami operacyjnymi.

Zestawienie materiałów oprogramowania (SBOM)

W przypadku odpowiednich urządzeń na żądanie oferujemy również zestawienie SBOM. SBOM zawiera szczegółową listę komponentów oprogramowania wykorzystywanych w naszych urządzeniach medycznych, umożliwiając interesariuszom identyfikację wszelkich bibliotek lub zależności stron trzecich, które mogą stwarzać ryzyko. Ta przejrzystość ma kluczowe znaczenie dla zrozumienia potencjalnych luk w zabezpieczeniach i utrzymania integralności architektury oprogramowania urządzenia.

Pomoc w planach wdrożenia

Pomagamy zakładom opieki zdrowotnej w planach wdrożenia, zapewniając, że funkcje bezpieczeństwa naszych urządzeń są prawidłowo zintegrowane z wdrożonym środowiskiem i skutecznie zarządzane. Wsparcie to obejmuje wskazówki dotyczące instalacji, konfiguracji i bieżącej konserwacji.

Konserwacja i zarządzanie cyklem życia

Konserwacja po wprowadzeniu produktu na rynek podkreśla odpowiedzialność firmy Mindray w zakresie ochrony pacjentów, ich danych i opieki zdrowotnej — od wdrożenia oprogramowania do wycofania go z eksploatacji.

Luki w zabezpieczeniach wykryte po wprowadzeniu na rynek i zarządzanie poprawkami

Produkty firmy Mindray wykorzystują systemy operacyjne innych firm, takie jak Microsoft Windows i Linux. Aby zapewnić bezpieczeństwo tych systemów operacyjnych, opracowaliśmy **kompleksową strategię zarządzania poprawkami,** która umożliwia nam stałe monitorowanie potencjalnych luk w zabezpieczeniach, ocenę ich wpływu na nasze urządzenia i wdrażanie poprawek w celu wyeliminowania tych problemów.

W przypadku produktów działających w systemie Microsoft Windows ocena wpływu nowo wydanych poprawek zabezpieczeń i poprawek doraźnych (hotfix) zwykle rozpoczyna się w ciągu 48 godzin od otrzymania przez Mindray informacji o ich wydaniu. Oceniamy wpływ poprawek, aby określić, czy należy niezwłocznie je zainstalować, czy można to zrobić w ramach zaplanowanych aktualizacji. W przypadku krytycznych poprawek wymagających natychmiastowej uwagi zapewniamy **szczegółowe instrukcje instalowania przyspieszonych aktualizacji**. Zapewnia to, że groźne luki w zabezpieczeniach są eliminowane szybko i bezpiecznie. W innych przypadkach poprawki są wydawane w ciągu kilku tygodni i przekazywane użytkownikom urządzeń, dzięki czemu są oni informowani na bieżąco, a nasze urządzenia pozostają chronione. W przypadku naszych produktów opartych na systemie Linux przeprowadzamy analizę co sześć miesięcy. Zważywszy że platformy Linux w urządzeniach medycznych są zwykle dostosowane do konkretnych zastosowań, poprawki są zazwyczaj wydawane w formie pełnej aktualizacji oprogramowania. Jeśli zagrożenia nie można wyeliminować poprzez instalację samych poprawek systemu operacyjnego, może zostać wydana aktualizacja oprogramowania systemowego.

Przed instalacją pakiety aktualizacji przechodzą **weryfikację sumy kontrolnej**. Zapewnia to integralność i autentyczność pakietu aktualizacji, tym samym zapobiegając nieautoryzowanym modyfikacjom. Ponadto nasz proces aktualizacji jest ściśle kontrolowany, dzięki czemu tylko upoważniony personel może przeprowadzać aktualizacje za pomocą opracowanego przez Mindray narzędzia chronionego hasłem. Automatyczne aktualizacje systemu operacyjnego są wyłączone, aby zapobiec nieautoryzowanym zmianom.

Koniec okresu eksploatacji i wsparcie przy wycofywaniu z eksploatacji

Choć proces ten może różnić się w zależności od rynku, wysyłamy naszym klientom szczegółowe **pisma z informacjami o procedurach postępowania w związku ze zbliżającym się końcem okresu eksploatacji produktów**. Pisma te zawierają kluczowe informacje o zaprzestaniu świadczenia usług konserwacyjnych, dostępności części i terminach wsparcia technicznego, dając klientom wystarczająco dużo czasu na zaplanowanie wymiany lub aktualizacji. Takie przejrzyste podejście sprawia, że klienci są dobrze poinformowani i mogą zachować ciągłość operacyjną podczas odchodzenia od starszych modeli, a także wzmacnia wysiłki Mindray na rzecz doskonałej obsługi klienta.

W przypadku urządzeń, które mają zostać wycofane z eksploatacji, najważniejsze jest bezpieczne i odpowiedzialne przeprowadzenie tego procesu, w ramach którego należy zapewnić, że nikt nie uzyska nieautoryzowanego dostępu do poufnych informacji, a urządzenia nie będą stanowić zagrożenia po ich wycofaniu. Mindray udziela wsparcia i umożliwia zakładom opieki zdrowotnej bezpieczne wycofanie urządzeń z eksploatacji, udostępniając im naszych doświadczonych pracowników lub przekazując dokumentację z zakresu najlepszych praktyk bezpiecznej utylizacji, np. instrukcje trwałego wymazywania danych. Ponadto doradzamy zakładom opieki zdrowotnej w kwestiach zgodności z lokalnymi przepisami i międzynarodowymi wytycznymi, w tym określonymi przez FDA i NIST, dotyczącymi utylizacji urządzeń elektronicznych, zapewniając, że wycofane urządzenia są usuwane w sposób bezpieczny i zgodny z prawem.

ZARZĄDZANIE ZDARZENIAMI

W kontekście branży opieki zdrowotnej i urządzeń medycznych zarządzanie zdarzeniami jest uznawane za wspólną odpowiedzialność. Jedynie współpraca między zakładami opieki zdrowotnej i producentami urządzeń medycznych może zapewnić skuteczność w zapobieganiu cyberatakom i reagowaniu na nie. Poprzez przyjęcie opisanego dalej podejścia dążymy do wspierania współpracy w zakresie cyberbezpieczeństwa. W ten sposób zarówno firma Mindray, jak i zakłady opieki zdrowotnej mają odpowiednie środki do reagowania na potencjalne zagrożenia bezpieczeństwa i minimalizowania ryzyka.

Rejestrowanie zdarzeń

Skuteczne rejestrowanie zdarzeń to kluczowy element, który mogą zaoferować producenci urządzeń medycznych. Urządzenia medyczne Mindray są wyposażone w specjalne dzienniki do rejestrowania operacji związanych z bezpieczeństwem zapewniające szczegółowy zapis działań, który może być kluczowy dla analizy zdarzeń i reagowania na nie. Ściśle współpracujemy z zakładami opieki zdrowotnej w procesie eksportowania i analizowania dzienników bezpieczeństwa oraz zarządzania nimi z uwzględnieniem określonych okoliczności i potrzeb.

Nasze urządzenia są także wyposażone w różne mechanizmy tworzenia kopii zapasowych i odzyskiwania danych. Pozwala to zapewnić, że krytyczne informacje dotyczące bezpieczeństwa są zachowane i można je przywrócić w przypadku awarii systemu lub niepożądanych zdarzeń. Taka odporność systemu zapewnia zachowanie integralności i dostępności dzienników bezpieczeństwa oraz wspomaga ciągłe działania na rzecz ochrony.

Reagowanie na zdarzenia i pomoc techniczna

Firma Mindray utworzyła specjalne zespoły nadzorujące proces reagowania na zdarzenia oraz stale monitorujące i badające występujące zdarzenia, które mogą wpływać negatywnie na nasze urządzenia. Po wykryciu lub zgłoszeniu zdarzenia związanego z bezpieczeństwem zespoły, współpracując z poszczególnymi jednostkami biznesowymi, oceniają ryzyko, opracowują plany reagowania i wdrażają odpowiednie rozwiązania. Opracowaliśmy „Wytyczne reagowania na zdarzenia związane z cyberbezpieczeństwem", aby wprowadzić standardowe i ujednolicone procedury w różnych podmiotach. W razie wystąpienia zagrożenia wymagającego zgłoszenia do odpowiednich organów nadzoru ściśle współpracujemy z odpowiednimi organami, aby szybko i dokładnie przekazywać im wymagane informacje. Przez cały czas trwania procedury utrzymujemy stały kontakt z naszymi klientami. Staramy się wspólnie szybko ocenić sytuację i wdrożyć niezbędne środki, aby zminimalizować negatywne skutki i zapewnić bezpieczeństwo urządzeń.

W ramach dodatkowego wsparcia urządzenia medyczne firmy Mindray są wyposażone w funkcje zapewniające ciągłość działania nawet w przypadku wykrycia zdarzeń związanych z cyberbezpieczeństwem. W zależności od możliwości niektóre urządzenia wykorzystują mechanizmy, takie jak uzupełnianie i synchronizacja danych, aby zapewnić bezpieczeństwo najważniejszych danych pacjentów w przypadku awarii sieci. Część urządzeń jest też wyposażona w mechanizm dzielący sieć na osobne warstwy, który może izolować zagrożenia występujące na urządzeniu od sieci szpitalnej. Dodatkowo zastosowanie środowiska sieciowego z nadmiarowymi sieciami przewodowymi i bezprzewodowymi umożliwia bezproblemową pracę urządzenia, nawet jeżeli jedna z sieci ulegnie awarii.

Pomagając zakładom opieki zdrowotnej w systematycznym reagowaniu na zdarzenia i zapewniając wsparcie techniczne, Mindray stara się umożliwić partnerom skuteczne zarządzanie i minimalizowanie skutków zdarzeń związanych z cyberbezpieczeństwem oraz zwiększenie odporności operacyjnej.

OCHRONA DANYCH

Prywatność w fazie projektowania

Firma Mindray przeprowadziła analizę porównawczą swoich procesów względem norm międzynarodowych i najlepszych praktyk na poziomie przedsiębiorstwa, a następnie na podstawie jej wyników wdrożyła system zarządzania zgodnością z przepisami dotyczącymi bezpieczeństwa informacji i ochrony poufności danych. System ten zarządza całym cyklem życia danych, w tym ich gromadzeniem, przesyłaniem, wykorzystywaniem, udostępnianiem, przechowywaniem i usuwaniem, zgodnie z zasadami legalności, sprawiedliwości, uczciwości, otwartości i przejrzystości. Ma to na celu ochronę **poufności, integralności i dokładności** wszystkich danych osobowych przetwarzanych przez Mindray. Dzięki tak rozbudowanemu systemowi zarządzania firma Mindray uzyskała certyfikaty ISO/IEC 27001 oraz ISO/IEC 27701 i stale udoskonala swoje wymagania dotyczące prywatności.

W oparciu o taką kulturę korporacyjną i świadomość ochrony prywatności, a także zobowiązanie do ochrony i poszanowania prywatności oraz danych klientów i pacjentów, firma Mindray wdrożyła podstawowe zasady „**prywatności w fazie projektowania**" i „**domyślnej ochrony prywatności**" w procesie rozwoju produktów. (Więcej informacji można znaleźć na ilustracji na stronie 6). Te zasady są wdrażane już na etapie koncepcyjnym i planowania rozwoju produktów przez zastosowanie podstawowych wytycznych w zakresie uprawnień, rejestrowania, szyfrowania oraz deidentyfikacji/anonimizacji itd. Włączając ochronę prywatności do projektu od samego początku, zapewniamy, że środki ochrony prywatności nie są jedynie dodatkiem, ale stanowią integralną część architektury produktu. W ten sposób proaktywnie rozwiązujemy obawy związane z prywatnością, zwiększając zaufanie użytkowników i spełniając wymogi regulacyjne.

Mindray dąży do tego, aby ochrona prywatności była podstawową wartością wpisaną w cały proces rozwoju produktów.

Zaangażowanie firmy Mindray w ochronę prywatności w fazie projektowania pozwoliło nam zdobyć zaufanie zakładów opieki zdrowotnej i pacjentów, umożliwiając przetwarzanie wrażliwych danych użytkowników z zachowaniem najwyższych standardów bezpieczeństwa i prywatności.

Ocena skutków przetwarzania w zakresie danych osobowych

Dla firmy Mindray przestrzeganie przepisów dotyczących ochrony danych i prywatności to nie tylko obowiązek prawny, ale fundament, który pomaga nam ograniczać ryzyko związane z naruszeniami danych i zwiększa zaufanie naszych interesariuszy. Stawiając sobie za cel kompleksowe wskazywanie luk w zgodności oraz zagrożeń dla prywatności i ochrony danych, wprowadziliśmy **„ocenę skutków przetwarzania w zakresie danych osobowych" (PIA)** do procesu rozwoju produktów, aby zapewnić wdrożenie odpowiednich środków kontroli zgodnie z obowiązującymi przepisami. Proces PIA obejmuje dokładną analizę i dokumentację potencjalnych zagrożeń dla prywatności, a następnie wdrożenie odpowiednich strategii mających je wyeliminować. Tak dokładna ocena i wdrożenie środków kontroli umożliwia nie tylko firmie Mindray, ale także naszym klientom zachowanie zgodności z odpowiednimi przepisami prawa i regulacjami, takimi jak **RODO, HIPAA czy PIPL**. Opublikowaliśmy również szczegółowy **dokument dotyczący RODO**[10], w którym opisano, w jaki sposób firma Mindray przestrzega jednego z najbardziej rozbudowanych międzynarodowych standardów ochrony danych. Zawiera on informacje o ładzie korporacyjnym, kontrolach wewnętrznych i mechanizmach przetwarzania danych osobowych stosowanych w firmie Mindray. Przedstawiają one nasze zaangażowanie na rzecz utrzymania wysokich standardów bezpieczeństwa i prywatności danych.

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

Szyfrowanie danych

W myśl zasady „prywatności w fazie projektowania" szyfrowanie danych stanowi podstawę podejścia firmy Mindray do ochrony danych. Służy jako krytyczny mechanizm obronny do ochrony poufnych informacji przed nieautoryzowanym dostępem i naruszeniami. Firma Mindray wykorzystuje kompleksowe metody szyfrowania zapewniające bezpieczeństwo danych przesyłanych przez sieć, jak i przechowywanych w pamięci masowej. Każda linia produktów firmy Mindray wykorzystuje protokoły i metody dobrane do konstrukcji danego urządzenia i potrzeb biznesowych. Zapewnia to właściwą ochronę wszystkich danych.

Przesyłane dane

Podczas transmisji danych stosowane są standardy DICOM i HL7, które obsługują różne protokoły szyfrowania, w tym TLS 1.2 z szyfrowaniem AES-256. W przypadku komunikacji bezprzewodowej urządzenia Mindray obsługują standard WPA/WPA2 Enterprise, który zapewnia skuteczne szyfrowanie danych przesyłanych przez sieci Wi-Fi.

Przechowywane dane

Chociaż staramy się minimalizować rejestrowanie i przechowywanie danych osobowych, w wyjątkowych okolicznościach urządzenia Mindray stosują szyfrowanie przy pomocy bezpiecznych algorytmów, takich jak AES-256, aby zapobiec niewłaściwemu wykorzystaniu przechowywanych danych w przypadku nieautoryzowanego dostępu.

Wyświetlane dane

Informacje umożliwiające identyfikację wyświetlane na monitorze lub w eksportowanych raportach można skonfigurować tak, aby były ukryte. Ta elastyczność daje większą kontrolę nad zarządzaniem dostępem do informacji osobistych.

Eksport danych

W przypadku kopii zapasowych tworzonych na nośnikach USB, do ochrony zarchiwizowanych danych wykorzystywana jest kompresja 7z z silnym szyfrowaniem, która zapewnia, że zbiory danych są bezpiecznie kompresowane i przechowywane. Urządzenia Mindray obsługują również techniki anonimizacji i pseudonimizacji podczas eksportowania lub tworzenia kopii zapasowych wrażliwych materiałów na dyskach twardych.

Dzięki zastosowaniu zaawansowanych technologii szyfrowania i podtrzymywaniu rygorystycznych standardów w zakresie ochrony danych urządzenia Mindray umożliwiają użytkownikom odpowiednią ochronę danych przez cały czas, niezależnie od tego, czy są one przesyłane, przechowywane, wyświetlane czy eksportowane.

Obsługa danych podczas konserwacji

Może się zdarzyć, że w okresach wymaganych prac konserwacyjnych trzeba będzie udzielić naszym pracownikom dostępu do urządzeń lub przesłać je do naszych punktów serwisowych. Na wypadek gdyby dane na urządzeniach nie zostały w pełni usunięte, zanonimizowane lub utajnione, firma Mindray wprowadziła rygorystyczne protokoły i dokładne przepisy wewnętrzne dotyczące obsługi danych podczas konserwacji. Ma to zapewnić, że poufne informacje są odpowiednio chronione lub niszczone, aby zapobiec nieautoryzowanemu dostępowi.

Firma Mindray zapewnia zakładom opieki zdrowotnej kompleksowe wytyczne w zakresie bezpiecznego zarządzania danymi w trakcie konserwacji urządzenia. Kluczowym środkiem jest funkcja bezpiecznego wymazywania danych. Zdecydowanie zaleca się jej używanie w celu zapewnienia, że żadne poufne informacje nie pozostaną na obsługiwanych urządzeniach.

Lokalne zespoły w każdym regionie w pierwszej kolejności oceniają, czy problemy można rozwiązać na ich poziomie. W regionach, w których zwrot urządzeń i dzienników do Chin jest zabroniony, wszystkie problemy są rozwiązywane lokalnie. W przypadkach gdy zwrot urządzeń i dzienników do Chin w celu rozwiązania problemów jest dozwolony i nieunikniony, lokalny zespół sprawdza, czy wrażliwe dane zostały prawidłowo usunięte z zachowaniem zgodności z międzynarodowymi przepisami o ochronie danych i regulacjami dotyczącymi międzynarodowego transferu danych. Alternatywnie można zastosować metody utajniania danych, które przekształcają informacje wrażliwe w sposób uniemożliwiający ich identyfikację lub śledzenie, zachowując jednocześnie ich przydatność do celów diagnostycznych. Może to obejmować maskowanie lub modyfikację danych umożliwiających identyfikację osób oraz potwierdzenie przy użyciu testów anonimizacji, że pozostałych danych nie można powiązać z poszczególnymi pacjentami.

Równocześnie nasz personel stosuje **środki kontroli dostępu**, kierując się zasadą minimalnego uprzywilejowania. Dzięki temu tylko upoważnieni pracownicy mają dostęp do urządzenia oraz znajdujących się na nim danych i jest on ograniczony do obszarów niezbędnych do wypełniania ich obowiązków. Wszyscy pracownicy wewnętrzni lub upoważnieni pracownicy zewnętrzni są zobowiązani do zachowania poufności. Ma to zapewnić, że przetwarzają pozostałe dane z zachowaniem najwyższej dyskrecji i bezpieczeństwa.

W przypadku zdalnej konserwacji Mindray korzysta z bezpiecznych narzędzi pod ścisłym nadzorem zespołu ds. zarządzania ryzykiem i kontrolą. Autoryzacja klienta jest wymagana przed przeprowadzeniem jakichkolwiek zdalnych czynności konserwacyjnych. Ponadto, zgodnie z zasadą minimalnej konieczności, w celu zminimalizowania ryzyka ujawnienia danych uzyskiwany jest dostęp tylko do niezbędnych informacji wymaganych do konserwacji. Procedury kontroli i kończenia sesji mają na celu zapewnić, że sesje zdalnego dostępu są bezpiecznie przeprowadzane i kończone po zrealizowaniu zadań konserwacyjnych.

Mindray zobowiązuje się do utrzymywania najwyższych standardów ochrony danych przez cały cykl życia swoich urządzeń medycznych. Podejście to nie tylko chroni poufne informacje, ale także wzbudza poczucie zaufania wśród użytkowników naszych urządzeń. Oddaje to zaangażowanie firmy Mindray w rozwój technologii medycznych, przy jednoczesnym stawianiu bezpieczeństwa klientów i użytkowników na pierwszym miejscu.

UWAGI KOŃCOWE

Patrząc w przyszłość, firma Mindray zamierza konsekwentnie dążyć do rozwoju technologii medycznych, zachowując przy tym najwyższe standardy cyberbezpieczeństwa. Rozumiemy, że zaufanie pokładane w nas i naszych urządzeniach to zobowiązanie, któremu musimy sprostać z niezachwianym oddaniem. Poprzez ciągłe ulepszanie naszych środków ochrony cyberbezpieczeństwa i zapobieganie nowym zagrożeniom chcemy dostarczać rozwiązania medyczne, które są nie tylko innowacyjne, ale też bezpieczne.

Podsumowując, niniejszy dokument jest świadectwem wszechstronnego i proaktywnego podejścia firmy Mindray do cyberbezpieczeństwa. Podkreśla on nasze zaangażowanie w ochronę danych pacjentów, zapewnianie integralności naszych urządzeń medycznych i promowanie kultury bezpieczeństwa, która jest integralną częścią naszej misji. W obliczu złożoności ery cyfrowej firma Mindray będzie nadal opierała swoją działalność na uczciwości, innowacyjności i zaangażowaniu na rzecz ochrony systemu opieki zdrowotnej.