

WYROBY MEDYCZNE

po nowemu

biuletyn kancelarii IPSO LEGAL

1/2023

CYBER

SECURITY

SPIS TREŚCI

03	WSTĘP
04	OGÓLNE WYMOGI DOTYCZĄCE CYBERBEZPIECZEŃSTWA
05	POZOSTAŁE WYMOGI CYBERBEZPIECZEŃSTWA
07	AKTUALNY STAN WIEDZY. CZYLI JAKI?
08	CYBERBEZPIECZEŃSTWO WYROBÓW MEDYCZNYCH - ZAPIS SZKOLENIA
09	OCENA I ZARZĄDZENIE RYZYKIEM
11	STANDARDY CYBERBEZPIECZEŃSTWA WYROBÓW MEDYCZNYCH - PRZEGLĄD DOBRYCH PRAKTYK
14	NADZÓR PO WPROWADZENIU DO OBROTU
16	INCYDENTY NARUSZENIA CYBERBEZPIECZEŃSTWA

KANCELARIA JEST PARTNEREM:



Klaster
LifeScience
Kraków

OD REDAKCJI



Czwarty numer biuletynu "Wyroby medyczne po nowemu" to prawdziwa gratka dla wszystkich zainteresowanych bezpieczeństwem danych pacjentów i pracą systemów medycznych.

Dlaczego? Ponieważ na temat przewodni tego numeru wybraliśmy cyberbezpieczeństwo wyrobów medycznych - kwestię, która w dzisiejszych czasach staje się coraz bardziej istotna i wymagająca naszej uwagi.

Ataki na systemy medyczne i urządzenia medyczne są realnym zagrożeniem dla pacjentów, a skutki mogą być poważne i groźne dla ich zdrowia i życia.

Z tego powodu wprowadzenie odpowiednich regulacji cyberbezpieczeństwa jest niezwykle ważne.

Dzięki temu możemy minimalizować ryzyko wystąpienia takich zagrożeń i zapewnić bezpieczeństwo pacjentom oraz personelowi medycznemu.

W numerze znajdziecie wiele wartościowych informacji na temat cyberbezpieczeństwa w medycynie, w tym o wprowadzonych w 2017 roku regulacjach dotyczących wyrobów medycznych, które zawierają programowalne systemy elektroniczne i oprogramowanie będące samym w sobie wyrobem medycznym.

Wszystko to wymaga od producentów, dostawców i innych podmiotów zaangażowanych w tworzenie bezpiecznych wyrobów medycznych szczególnej uwagi.

Dlatego też, zachęcam do przeczytania najnowszego numeru biuletynu "Wyroby medyczne po nowemu", w którym holistycznie podchodzimy do analizy tej kwestii. Nie boję się stwierdzenia, że jest to pierwsze w Polsce tak kompleksowe przedstawienie tego zagadnienia.

Niezmiennie zachęcam też do korzystania z tworzonego przez nas MDR Help Point'u gdzie znajdują się aktualne analizy, ciekawostki oraz zapisy szkoleń z nowych regulacji w branży wyrobów medycznych.

Miłej lektury!

Błażej Wągiel

OGÓLNE WYMOGI DOTYCZĄCE CYBERBEZPIECZEŃSTWA

Ogólne wymogi dotyczące cyberbezpieczeństwa są określone w pkt. 17 załącznika I do MDR i pkt. 16 Załącznika I rozporządzenia IVDR.

Odnoszą się one zarówno do aspektów przed wprowadzeniem wyrobów medycznych do obrotu, jak i po wprowadzeniu ich do obrotu.

I tak, zgodnie z tymi przepisami:

- wyroby, które zawierają elektroniczne systemy programowalne, w tym oprogramowanie, lub oprogramowanie, które samo w sobie jest wyrobem, projektuje się tak, aby zapewnić powtarzalność wyników, niezawodność i działanie zgodne z ich przewidzianym użytkowaniem. Na wypadek stanu pojedynczego uszkodzenia podejmuje się odpowiednie środki w celu wyeliminowania lub ograniczenia w możliwie największym stopniu ryzyka lub zakłócenia działania będących jego następstwem.
- w przypadku wyrobów zawierających oprogramowanie lub w przypadku oprogramowania, które samo w sobie jest wyrobem, takie oprogramowanie ma być rozwijane i wytwarzane zgodnie z aktualnym stanem wiedzy oraz z uwzględnieniem zasad cyklu życia oprogramowania, zarządzania ryzykiem, w tym bezpieczeństwa informacji, weryfikacji i walidacji.

- oprogramowanie, które jest przeznaczone do stosowania w połączeniu z mobilnymi platformami obliczeniowymi, jest projektowane i produkowane z uwzględnieniem szczególnych właściwości takiej mobilnej platformy (np. rozmiaru i współczynnika kontrastu ekranu) oraz czynników zewnętrznych związanych z jej stosowaniem (środowisko zróżnicowane pod względem oświetlenia lub hałasu).
- producent określa minimalne wymogi dotyczące sprzętu, właściwości sieci informatycznej oraz środków bezpieczeństwa informatycznego, w tym ochrony przed nieupoważnionym dostępem, niezbędne do zgodnego z przeznaczeniem działania tego oprogramowania.



POZOSTAŁE WYMOGI CYBERBEZPIECZEŃSTWA

W dzisiejszych czasach producenci wyrobów medycznych muszą przestrzegać coraz bardziej restrykcyjnych przepisów związanych z cyberbezpieczeństwem.

Mają oni obowiązek zapewnić kompleksowe zabezpieczenie danych pacjentów i wdrożyć procedury oceny zgodności wyrobów medycznych z wymaganiami prawnymi.

Dlatego producenci muszą w całym cyklu życia produktu uwzględnić kwestie takie jak m.in. nadzór po wprowadzeniu produktów do obrotu, raportowanie wyników nadzoru oraz analiza poważnych incydentów i działań korygujących.

Wobec tego producenci nie mogą poprzestać na zgodności z załącznikiem I rozporządzeń, ale też muszą zwrócić uwagę na:

- prywatność i ochronę danych pacjentów w kontekście uczestnictwa w badaniach klinicznych lub badaniach działania, o czym mówi art. 62 pkt. 4 lit. h) MDR oraz art. 58 ust. 5 lit. h IVDR,
- procedury oceny zgodności produktów medycznych z wymaganiami prawnymi, o czym mówi art. 52 MDR oraz art. 48 IVDR,
- System nadzoru po wprowadzeniu produktów medycznych do obrotu, stosowany przez producenta, o czym mówi art. 83 MDR oraz art. 78 IVDR,
- plan nadzoru po wprowadzeniu produktów medycznych do obrotu, o czym mówi art. 84 MDR oraz art. 79 IVDR,
- raportowanie wyników nadzoru po wprowadzeniu produktów medycznych do obrotu, o czym mówi art. 85 MDR oraz art. 80 IVDR,
- okresowe raporty o bezpieczeństwie produktów medycznych, o czym mówi art. 86 MDR oraz art. 81 IVDR,
- zgłaszanie poważnych incydentów i działań korygujących związanych z bezpieczeństwem produktów medycznych, o czym mówi art. 87 MDR oraz art. 82 IVDR,
- raportowanie tendencji dotyczących bezpieczeństwa produktów medycznych, o czym mówi art. 88 MDR oraz art. 83 IVDR,
- analizę poważnych incydentów i działań korygujących związanych z bezpieczeństwem produktów medycznych, o czym mówi art. 89 MDR oraz art. 84 IVDR,
- dokumentację techniczną, o czym mówi Załącznik II do MDR i IVDR,
- dokumentację techniczną dotyczącą nadzoru po wprowadzeniu wyrobów medycznych do obrotu, o czym mówi Załącznik III do MDR i IVDR,
- ocenę kliniczną/działania oraz działania następcze po wprowadzeniu wyrobów medycznych do obrotu, o czym mówi rozdział VI i Załącznik XIV do MDR i IVDR.



REGULACJE, NA KTÓRE POWINIENIEŚ ZWRÓCIĆ UWAGĘ

Wymogi bezpośrednio związane z cyberbezpieczeństwem wyrobów medycznych wykraczają poza zakres przepisów rozporządzeń. Przykładem są wymogi dotyczące prywatności i poufności danych powstałych w wyniku stosowania wyrobów medycznych.

Należy zwrócić uwagę, że cyberbezpieczeństwo wyrobów medycznych to nie tylko kwestia techniczna.

Ochrona prywatności i poufności danych pacjentów to również kwestia etyczna. Producentów wyrobów medycznych zobowiązuje przede wszystkim troska o bezpieczeństwo i dobro pacjentów.

ZWRÓĆ UWAGĘ NA:

> **Dyrektywę (UE) 2016/1148 (NIS 1)**, która przewiduje środki prawne mające na celu zwiększenie ogólnego poziomu cyberbezpieczeństwa w UE, i nakłada na dostawców usług cyfrowych obowiązki zabezpieczenia systemów informatycznych przed atakiem polegające na zapewnieniu odpowiedniego poziomu bezpieczeństwa teleinformatycznego, przeprowadzanie regularnych audytów czy wdrożenie odpowiednich procedur postępowania w przypadku incydentów bezpieczeństwa. Implementowana ustawą o krajowym systemie cyberbezpieczeństwa. Traci moc od dnia 18 października 2024 r.

> **Dyrektywa (UE) 2022/2555 (NIS 2)** w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148, która rozszerza obowiązek zapewnienia cyberbezpieczeństwa m.in. na dostawców usług chmurowych oraz wprowadza nowe obowiązki z zakresu zarządzania cyberbezpieczeństwem poprzez obligatoryjne wdrażanie i stosowanie systemów zarządzania ryzykiem takich jak polityki analizy ryzyka i bezpieczeństwa systemów informatycznych, polityki zarządzania incydentami czy zapewnienia bezpieczeństwa łańcucha dostaw. Implementacja tej dyrektywy do polskiego porządku prawnego powinna nastąpić najpóźniej do 17 października 2024 roku.

> **RODO**, które reguluje przetwarzanie danych osobowych, niezależnie od tego, jak są one przechowywane (w systemie informatycznym, w chmurze, na dysku fizycznym czy papierze).

AKTUALNY STAN WIEDZY. CZYLI JAKI?

Jest jeszcze jedna rzecz, która spędza sen z powiek producentów wyrobów medycznych. Załącznik I rozporządzeń nakłada na producentów obowiązek uwzględnienia **aktualnego stanu wiedzy** podczas projektowania, opracowywania i modernizacji produktów w całym cyklu życia produktu.

Producent powinien wykazać, że jego decyzje oparte są na aktualnym stanie wiedzy, czyli na obowiązujących normach, wytycznych, wiedzy i publicznie dostępnych informacjach naukowych i technicznych.

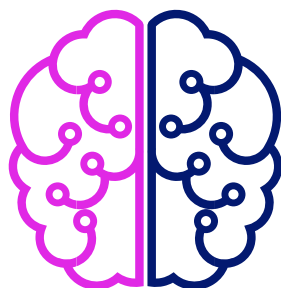
Przy tym należy zadbać o adekwatne uwzględnienie ryzyka bezpieczeństwa.

Aktualny stan wiedzy nie jest zdefiniowany w rozporządzeniach. Jak go zatem interpretować?

Z pomocą przychodzą jednak wytyczne **MDCG 2022-2**, które definiują go jako:

Stopień rozwoju aktualnych możliwości technicznych i/lub przyjętej praktyki klinicznej w odniesieniu do produktów, procesów i zarządzania pacjentem. Stan techniki powinien być oparty na odpowiednich skonsolidowanych wynikach nauki, technologii i doświadczenia.

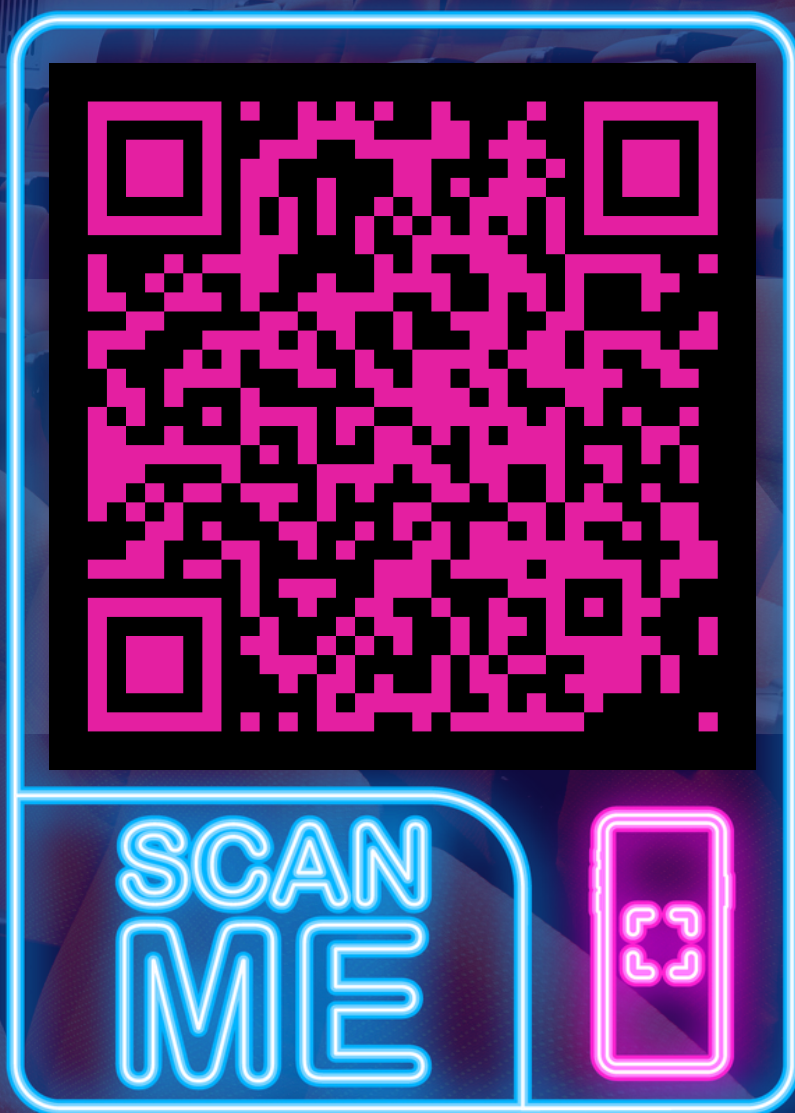
Warto zaznaczyć, że stan aktualny nie musi oznaczać najbardziej zaawansowanego technologicznie rozwiązania i jest czasem określany jako "ogólnie uznany stan techniki".



**LINK DO PEŁNEJ TREŚCI
WYTYCZNYCH MDCG**



Cyberbezpieczeństwo wyróbów medycznych – zapis szkolenia



NAGRANIE DOSTĘPNE TEŻ POD ADRESEM:

[IPSOLEGAL.PL/MDR-HELP-POINT](https://ipsolegal.pl/mdr-help-point)

OCENA I ZARZĄDZANIE RYZYKIEM CYBERNETYCZNYM

OBOWIĄZKI PRODUCENTA

W kontekście cyberbezpieczeństwa wyrobów medycznych istotną rolę odgrywa Załącznik I do rozporządzeń, który jednoznacznie określa jakie wymagania powinien wziąć pod uwagę producent. Chodzi tu w szczególności o wymagania dotyczące:

- sprzętu, właściwości sieci informatycznej oraz środków bezpieczeństwa informatycznego, w tym ochrony przed nieupoważnionym dostępem, niezbędnych do zgodnego z przeznaczeniem działania tego oprogramowania (17.4 MDR/16.4 IVDR).
- projektowania i produkowania wyrobów w taki sposób, by w jak największym stopniu chronić przed nieupoważnionym dostępem, który mógłby zakłócać przewidziane funkcjonowanie wyrobu (18.8 MDR).
- określenia w instrukcji używania informacji na temat przewidzianego zastosowania wyrobu (23.4(b) MDR / 20.4.1.(c) IVDR).

Wszystkie te wymagania są niezbędne do uruchomienia oprogramowania zgodnie z przeznaczeniem.



ZACHOWAJ RÓWNOWAGĘ

W sekcji 1 Załącznika I do rozporządzeń w sprawie wyrobów medycznych wymaga się, aby dopuszczalne ryzyko związane z ich działaniem umożliwiała wysoki poziom ochrony zdrowia i bezpieczeństwa użytkowników.

Można to osiągnąć jedynie poprzez ustanowienie odpowiedniej równowagi między korzyściami a ryzykiem podczas wszystkich możliwych trybów działania wyrobu medycznego.

W kwestii bezpieczeństwa istnieją zagrożenia związane ze zbyt słabymi lub zbyt silnymi zabezpieczeniami. Słabe zabezpieczenia, takie jak słaba kontrola dostępu, mogą umożliwić złośliwą modyfikację działania np. wszczepionego urządzenia kardiologicznego.

Natomiast stosowanie zbyt restrykcyjnych środków bezpieczeństwa, które zapewniają wysoki poziom ochrony, może mieć negatywny wpływ na bezpieczeństwo, zwłaszcza jeśli funkcje bezpieczeństwa nie są odpowiednio zaprojektowane.

Może to doprowadzić do sytuacji, w której personel medyczny może mieć utrudniony dostęp do wszczepionego urządzenia kardiologicznego.

Wymagania w zakresie bezpieczeństwa cybernetycznego należy rozpatrywać zgodnie z charakterem wyrobu, w tym typem wyrobu i zamierzonym zastosowaniem technologii komunikacyjnych.

ZARZĄDZANIE RYZYKIEM

Zarządzanie ryzykiem polega na identyfikacji i pomiarze ryzyka wynikającego z zamierzonego i nieprzewidzianego użycia wyrobu medycznego, a także na jego minimalizowaniu (zob. załącznik I, sekcja 16.1 (IVDR) lub 17.1 (MDR)).

Proces ten składa się z pięciu etapów: analizy ryzyka bezpieczeństwa, oceny ryzyka bezpieczeństwa, kontroli ryzyka bezpieczeństwa, oceny ryzyka szczątkowego (rezydualnego) oraz raportowania.

Jeśli ryzyko związane z bezpieczeństwem lub środkiem kontroli bezpieczeństwa może wpłynąć na bezpieczeństwo i skuteczność wyrobu medycznego, należy je uwzględnić w ocenie ryzyka związanego z bezpieczeństwem. W analogiczny sposób, każda kontrola ryzyka bezpieczeństwa lub rozważania, które mogą wpłynąć na bezpieczeństwo, powinny zostać włączone do analizy ryzyka bezpieczeństwa.

Analiza ryzyka produktu pod kątem bezpieczeństwa powinna uwzględniać wpływ słabych punktów bezpieczeństwa na podstawowe funkcje produktu.

Ze względu na złożoność procesu tworzenia oprogramowania, konfiguracji oprogramowania i współzależności między komponentami oprogramowania, większość produktów ma luki w zabezpieczeniach cybernetycznych.

Przykład: wygaszanie ekranu może chronić dane osobowe. Jednak, gdy wyrób medyczny jest używany do celów interwencyjnych lub do wyświetlania parametrów życiowych, wygaszanie ekranu może stanowić zagrożenie dla bezpieczeństwa i nie powinno być wdrażane.

Nie wiadomo, czy luka zostanie odkryta i wykorzystana, dopóki się to nie stanie. Ogólna zasada mówi jednak, że każda luka, która może zostać wykorzystana w danej implementacji oprogramowania, powinna być traktowana jako czynnik, który może prowadzić do niewłaściwego użycia.

MINIMALIZACJA RYZYKA

Producenci wyrobów medycznych powinni zapewnić, że ich produkty są projektowane i produkowane w taki sposób, aby minimalizować ryzyko wynikające z przewidywalnych warunków środowiskowych. W tym celu mogą monitorować podatność oprogramowania i dostarczać aktualizacje, które zapewnią ciągłość bezpieczeństwa urządzenia.

Podczas procesu zarządzania ryzykiem producent powinien przewidzieć lub ocenić potencjalne zagrożenia, które mogą prowadzić do niewłaściwego użycia.

Przykład: użycie niezabezpieczonego nośnika USB do wprowadzenia danych do systemu informatycznego może być uznane za niewłaściwe użycie, podczas gdy wprowadzenie zdjęć rentgenowskich za pomocą płyty CD może być uzasadnione. Decyzja ta zależeć będzie od konkretnych warunków i środowiska użytkowania.

CYBERBEZPIECZEŃSTWO WYROBÓW MEDYCZNYCH - DOBRE PRAKTYKI

Ryzyko cybernetyczne związane z sieciami teleinformatycznymi w sektorze medycznym jest coraz większe, a producenci oprogramowania powinni zdawać sobie z tego sprawę. Zadania nie ułatwia też stan i podejście do kwestii bezpieczeństwa sieci w niektórych szpitalach.

Dodatkowo różni dostawcy usług medycznych mogą mieć różne podejście do zarządzania ryzykiem swoich sieci teleinformatycznych.

Dlatego ważne jest, aby producenci oprogramowania uwzględniali te różnice i umożliwiali im skuteczne zarządzanie ryzykiem.

Ważne jest również, aby producenci oprogramowania stosowali najlepsze praktyki w zakresie bezpieczeństwa, takie jak szyfrowanie danych, stosowanie zabezpieczeń sieciowych i regularne aktualizacje oprogramowania, aby zapobiegać atakom cybernetycznym i zagrożeniom.

DOBRE PRAKTYKI WEDŁUG MDCG

Dlatego dostawcy usług dla sektora ochrony zdrowia powinni przyjąć najlepsze praktyki w zakresie cyberbezpieczeństwa, aby utrzymać odpowiedni jego stan.

MDCG wskazuje, że dobre praktyki obejmują w szczególności:

- Zapewnienie dobrych zabezpieczeń fizycznych, aby uniemożliwić nieuprawniony fizyczny dostęp do urządzeń medycznych lub punktów dostępu do sieci.
- Ustanowienie środków kontroli dostępu (np. oparte na rolach), aby zapewnić, że tylko uwierzytelniony i upoważniony personel ma dostęp do elementów sieci, przechowywanych informacji, usług i aplikacji.
- Kontrolowanie dostępu do sieci, takie jak segmentacja, w celu ograniczenia komunikacji między urządzeniami medycznymi.
- Regularne aktualizowanie oprogramowania, aby zapewnić jego terminową implementację.
- Ochrona przed złośliwym oprogramowaniem, aby uniemożliwić nieautoryzowany dostęp do kodu źródłowego.
- Szkolenia z zakresu cyberbezpieczeństwa, aby pracownicy byli świadomi zagrożeń i wiedzieli, jak im przeciwdziałać.



SECURE BY DESIGN

Krytycznymi aspektami projektowania mechanizmów bezpieczeństwa dla wyrobów medycznych, są bezpieczeństwo, ochrona i skuteczność.

Dlatego producenci muszą uwzględniać te kwestie od wczesnego etapu rozwoju i procesu produkcyjnego, a także w całym cyklu życia wyrobu, co wyrażono wprost w przepisach rozporządzeń:

- **Sekcja 3 załącznika I do MDR** - poprzez wprowadzenie systemu zarządzania ryzykiem w całym cyklu życia wyrobu medycznego,
- **Załącznik I sekcja 4 IVDR/MDR** - poprzez przyjęcie środków sterowania ryzykiem,
- **Załącznik I sekcja 16 (IVDR) lub 17 (MDR),**
- **Załącznik I Sekcje 16.4 (IVDR) lub 17.4 i 18.8 (MDR),**
- **oraz Załącznik I sekcja 22.1 (MDR)**, który wymaga, by wyroby przeznaczone do stosowania przez laików były projektowane i produkowane w taki sposób, by ich działanie było zgodne z ich przewidzianym zastosowaniem, biorąc pod uwagę umiejętności laików i środki jakimi dysponują, a także wpływ dających się racjonalnie przewidzieć różnic w technice laików oraz w środowisku.

Mimo tych wymagań ogólne podejście do zarządzania bezpieczeństwem wyrobów medycznych i oprogramowania nie różni się od zarządzania cyberbezpieczeństwem innych systemów teleinformatycznych.

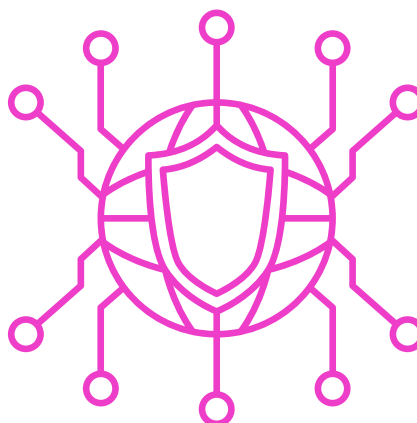
STRATEGIA DEFENSE IN DEPTH

MDCG wskazuje na osiem procesów, które powinny być wprowadzone przez producentów wyrobów medycznych w celu ustanowienia odpowiednich zabezpieczeń systemów informatycznych (*defense in depth*) w całym cyklu życia wyrobu:

Zarządzanie bezpieczeństwem zapewniające, że działania związane z bezpieczeństwem są odpowiednio planowane i wykonywane w całym cyklu życia produktu.

Specyfikacja wymagań bezpieczeństwa identyfikująca zdolności bezpieczeństwa, które są wymagane do odpowiedniej ochrony poufności, integralności i dostępności danych, funkcji i usług wyrobu medycznego a także określony kontekst bezpieczeństwa wyrobu. Zdolności bezpieczeństwa mogą obejmować takie elementy jak uwierzytelnianie, autoryzacja, szyfrowanie czy inne możliwości zabezpieczeń, które wyrób powinien zawierać. Kontekst bezpieczeństwa powinien natomiast obejmować takie elementy jak poziom bezpieczeństwa fizycznego, ochrona interfejsu itd.

Bezpieczeństwo w fazie projektowania - proces ten ma za zadanie zapewnić, że produkt jest zaprojektowany z uwzględnieniem zasad dogłębnej ochrony.



Bezpieczna implementacja - proces ten jest stosowany w celu zapewnienia bezpiecznej implementacji cech wyrobu i odnosi się do wszystkich komponentów sprzętowych i oprogramowania. Tego procesu nie stosuje się do komponentów dostarczanych przez dostawców zewnętrznych, do których stosowany jest proces **Zarządzanie bezpieczeństwem**.

Testowanie weryfikacji i walidacji bezpieczeństwa - proces ten służy do dokumentowania testów bezpieczeństwa wymaganych do zapewnienia, że wszystkie wymagania bezpieczeństwa dla wyrobu zostały spełnione oraz, że bezpieczeństwo wyrobu jest zachowane, gdy jest on używany zgodnie z przeznaczeniem. Proces ten powinien być dostosowany do innych działań związanych z testowaniem wyrobu i może być wykonywany w różnym czasie przez różnych pracowników na różnym etapie cyklu życia wyrobu.

Zarządzanie zagadnieniami związanymi z bezpieczeństwem - proces ten jest stosowany do obsługi zagadnień związanych z bezpieczeństwem produktu.

Zarządzanie aktualizacjami zabezpieczeń - proces ten stosowany jest w celu zapewnienia, że aktualizacje zabezpieczeń i poprawki bezpieczeństwa związane z wyrobem są testowane i udostępniane użytkownikom wyrobu w odpowiednim czasie.

Wytyczne dotyczące bezpieczeństwa - proces ten wykorzystywany jest do dostarczenia i utrzymania dokumentacji użytkownika, która opisuje sposób integracji, konfiguracji i utrzymania dogłębnej ochrony zgodnie z kontekstem bezpieczeństwa produktu.



NADZÓR PO WPROWADZENIU DO OBROTU

MONITOROWANIE ZAGROŻEŃ

Wraz z wprowadzeniem wyrobów medycznych na rynek, ich producenci muszą skupić się na monitorowaniu zagrożeń związanych z cyberbezpieczeństwem. Problemy te mogą zmieniać się i rozwijać w czasie, a więc kontrole przeprowadzone przed wprowadzeniem wyrobu do obrotu mogą nie wystarczyć do utrzymania akceptowalnego poziomu bezpieczeństwa.

Zgodnie z wymaganiami art. 83 MDR lub art. 78 IVDR, producent jest zobowiązany do wprowadzenia systemu nadzoru po wprowadzeniu do obrotu i regularnego jego aktualizowania. Nadzór nad cyberbezpieczeństwem wyrobów medycznych powinien być integralną częścią tego systemu.

System nadzoru po wprowadzeniu do obrotu powinien obejmować aktywne i regularne zbieranie doświadczeń użytkowników z wyrobów znajdujących się na rynku (w tym oprogramowania i komponentów sprzętowych stron trzecich), w celu ich przeglądu oraz terminowego wdrożenia niezbędnych działań korygujących, z uwzględnieniem charakteru i ryzyka związanego z danym wyrobem. Producent powinien włączyć do swojego systemu dystrybutorów wyrobu oraz, w stosownych przypadkach, autoryzowanych przedstawicieli i importerów wyrobu, aby uzyskać odpowiednie informacje z rynku.

SKUTECZNY SYSTEM NADZORU NAD CYBERBEZPIECZEŃSTWEM

Zgodnie z zaleceniami MDCG, skuteczny system nadzoru cyberbezpieczeństwa po wprowadzeniu do obrotu wyrobów medycznych powinien uwzględniać cztery kluczowe aspekty:

- **Po pierwsze**, system ten powinien zapewnić działanie wyrobu w przewidzianym środowisku, czyli zapewnić, że wyroby będą działać bezpiecznie i zgodnie z przeznaczeniem w warunkach, w jakich są one użytkowane.
- **Po drugie**, system powinien umożliwiać dzielenie się i rozpowszechnianie informacji dotyczących bezpieczeństwa cybernetycznego oraz wiedzy na temat słabych punktów i zagrożeń związanych z bezpieczeństwem cybernetycznym.
- **Po trzecie**, system powinien obejmować likwidację luk bezpieczeństwa. Oznacza to, że producent powinien regularnie przeglądać dostępne informacje i działać w celu zlikwidowania wszelkich luk w systemie bezpieczeństwa.
- **Wreszcie**, system powinien zapewnić odpowiednią reakcję na incydent. Oznacza to, że producent powinien mieć wdrożony plan działania w przypadku wystąpienia incydentu związanego z cyberbezpieczeństwem, a także wdrażać niezbędne korekty w celu zapobiegania podobnym incydentom w przyszłości.

WSPÓŁODPOWIEDZIALNOŚĆ

Chociaż MDR i IVDR nakładają obowiązki prawne tylko na producentów, to należy zauważyć, że w przypadku dostarczania bezpiecznych usług oprogramowania dla branży medycznej ważne jest uznanie roli i oczekiwań wszystkich zainteresowanych stron: **producentów, dostawców, świadczeniodawców, użytkowników profesjonalnych, pacjentów, integratorów, operatorów systemów oraz organów regulacyjnych.**

Wszystkie te podmioty ponoszą wspólną odpowiedzialność za zapewnienie cyber-bezpieczeństwa dla dobra pacjentów.

Modyfikacja wyrobu medycznego, np. instalacja lub umożliwienie korzystania z oprogramowania osobom trzecim, w tym łatanie oprogramowania, powinno zawsze odbywać się na podstawie wyraźnych, opublikowanych wytycznych producenta.

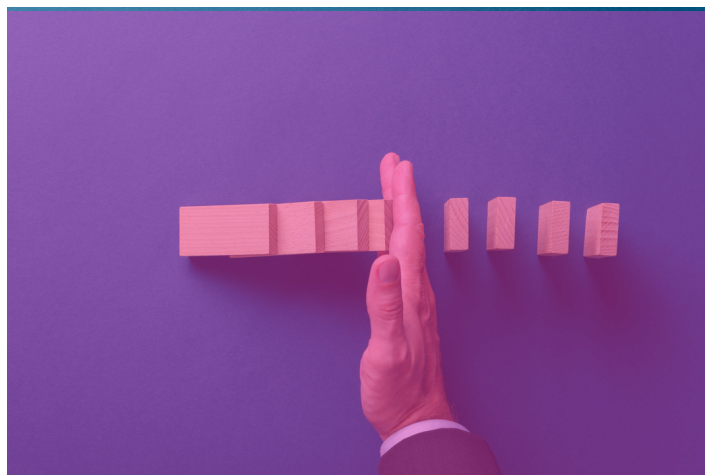
Należy pamiętać, że wszelkie nieuprawnione modyfikacje, takie jak poprawki oprogramowania, oprogramowanie antywirusowe, programy użytkowe, gry, pliki muzyczne i inne, mogą wpłynąć na działanie lub bezpieczeństwo systemu w nieprzewidywalny sposób, otwierając drzwi do łatwego wykorzystania podatności urządzenia medycznego.

Aby zapewnić, że zarządzanie urządzeniami w medycznej sieci informatycznej odbywa się w sposób odpowiedzialny, można podzielić tę odpowiedzialność między poszczególnymi uczestnikami procesu tworzenia wyrobu medycznego.

Dzięki odpowiednio skonstruowanym umowom o podziale odpowiedzialności, każda strona będzie świadoma swoich obowiązków i zapewni to właściwe zarządzanie bezpieczeństwem wyrobu po wprowadzeniu do obrotu.

W przypadku pacjentów i pracowników służby zdrowia należy zachęcać do odpowiedzialnych zachowań w sieci, takich jak zwracanie uwagi na prywatność, podejrzane wiadomości oraz odpowiedzialne przeglądanie stron internetowych.

Natomiast w instrukcjach użytkowania należy również informować o konieczności regularnego aktualizowania oprogramowania, stosowania silnych haseł oraz tworzenia kopii zapasowych.



INCYDENTY NARUSZENIA CYBERBEZPIECZEŃSTWA

INCYDENT I POWAŻNY INCYDENT

Zgodnie z rozporządzeniami MDR i IVDR:

- **incydentem** jest wadliwe działanie lub pogorszenie właściwości lub działania, w tym błąd użytkowy wynikający z cech ergonomicznych, wyrobu udostępnionego na rynku, a także wszelkie nieprawidłowości w informacjach podanych przez producenta oraz wszelkie działania niepożądane oraz szkody będące konsekwencją decyzji lekarskiej, podjęcia lub niepodjęcia działania na podstawie informacji lub wyników dostarczonych przez wyrób.
- Natomiast **poważny incydent** definiowany jest jako każde zdarzenie, które bezpośrednio lub pośrednio doprowadziło, mogło doprowadzić lub może doprowadzić do:
 - zgonu pacjenta, użytkownika lub innej osoby;
 - czasowego lub trwałego poważnego pogorszenie stanu zdrowia pacjenta, użytkownika lub innej osoby;
 - poważnego zagrożenia zdrowia publicznego.

ZACHOWAJ RÓWNOWAGĘ

Producent jest odpowiedzialny za zgłaszanie wszystkich poważnych incydentów i działań korygujących w zakresie bezpieczeństwa zgodnie z art. 87 MDR lub art. 82 IVDR.

Jeśli producent wyrobów medycznych otrzyma informację o poważnym incydencie, jest zobowiązany do natychmiastowego przeprowadzenia postępowania wyjaśniającego.

W ramach tego procesu, dokonuje się oceny ryzyka związanego z incydentem i wprowadzane są niezbędne poprawki, aby zminimalizować ryzyko związane z danym wyrobem.

Aby uzyskać potrzebne informacje z rynku, producent powinien zaangażować dystrybutorów wyrobu oraz, w niektórych przypadkach, autoryzowanego przedstawiciela i importerów.

Dzięki temu możliwe jest zapewnienie, że wymagane działania zostaną podjęte i zakończone w odpowiednim terminie.



RAPORTOWANIE TENDENCJI

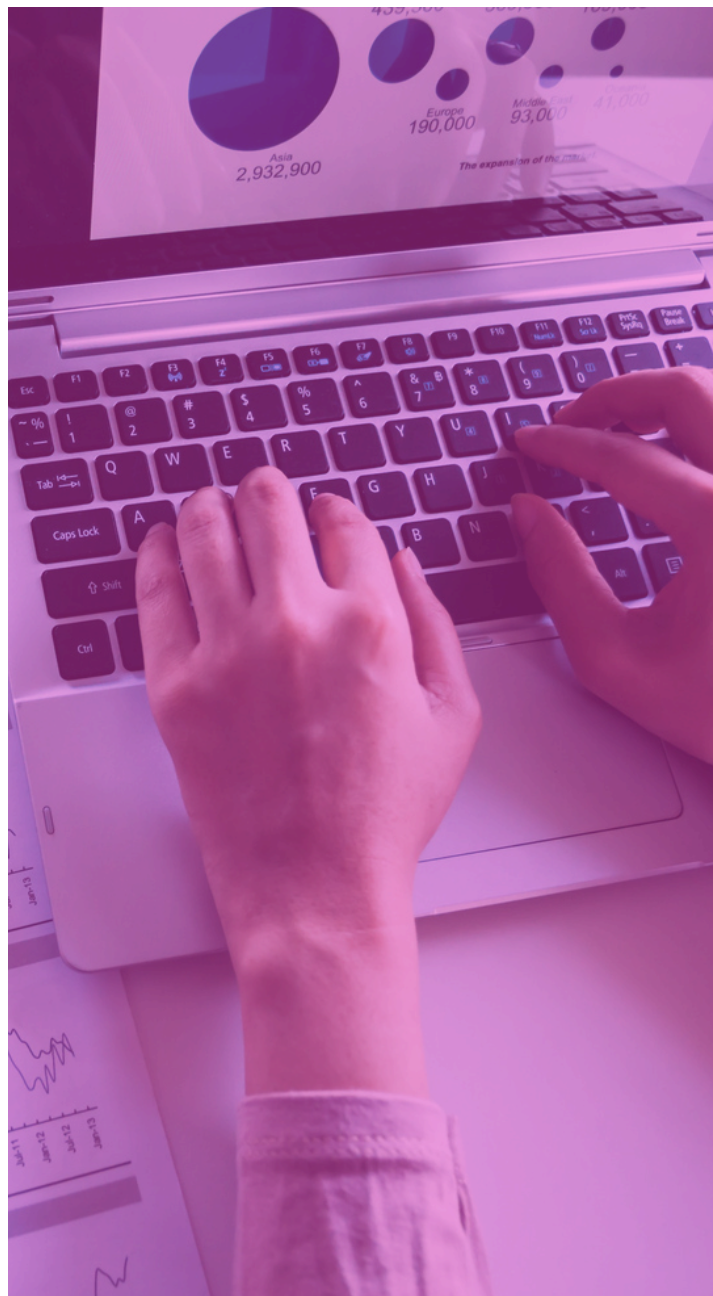
W przypadku wszystkich incydentów, producenci są zobowiązani do przekazywania raportów przez EUDAMED zgodnie z art. 88 MDR i art. 83 IVDR.

Jeśli częstotliwość lub ciężkość incydentów niebędących poważnymi incydentami lub spodziewanych działań niepożądanych wzrasta w sposób istotny, co może wpłynąć na analizę stosunku korzyści do ryzyka oraz stworzyć niebezpieczeństwo dla zdrowia lub bezpieczeństwa pacjentów, użytkowników lub innych osób, producenci muszą przeprowadzić raportowanie tendencji.

CO POWINIEN ZAWIERAĆ RAPORT TENDENCJI?

Według MDCG raport tendencji powinien zawierać informacje na temat:

- metodologii, jaka została zastosowana do ustalenia każdego istotnego statystycznie wzrostu częstotliwości lub ciężkości incydentów,
- sposobu, w jaki producent zarządza incydentami,
- okresu obserwacji, który został uwzględniony w planie nadzoru rynku po wprowadzeniu do obrotu.



Przykłady incydentów według MDCG

URZĄDZENIE	NARUSZENIE
Inkubator dla wcześniaków	Nieuprawniony użytkownik z fizycznym dostępem do urządzenia odgaduje słabe hasło do konta serwisowego i eksportuje dane dotyczące terapii i pacjenta przez złącze USB.
System monitorowania pacjenta	Przechwycenie komunikacji sieciowej pomiędzy lokalnym monitorem pacjenta a centralną stacją monitorowania. W ten sposób przejmujący wchodzi w posiadanie wrażliwych informacji o stanie zdrowia pacjenta.
Rezonans magnetyczny	Próba infekcji w sieci prowadząca do błędu "Blue Screen".

Przykłady poważnych incydentów według MDCG

URZĄDZENIE	NARUSZENIE
Wszczepialny czujnik do monitorowania ciśnienia w tętnicy płucnej u pacjentów z niewydolnością serca	Atakujący modyfikuje lub tworzy dane pacjenta przesyłając do lub z zewnętrznego urządzenia elektronicznego, powodując błędną diagnozę, która wpływa na opiekę nad pacjentem.
Rozrusznik serca	Nieautoryzowana osoba jest w stanie wywołać przeciążenie urządzenia w wyniku dużej ilości komend.
Aparat Rentgenowski	Pliki DICOM zainfekowane wykonywalnym złośliwym oprogramowaniem importowane i eksportowane rozprzestrzeniają się w sieci PACS i urządzeń medycznych.



CO PRAWNICY Z IPSO LEGAL MOGĄ ZROBIĆ DLA CIEBIE.

Błażej Wągiel - radca prawny zarządzający
kancelarią IPSO Legal.

Zapewnia wsparcie klientów, pomagając im poruszać się po materii związanej z prawem medycznym i farmaceutycznym, negocjacjach umów, compliance i strategicznych decyzjach biznesowych przed którymi stają na co dzień.

W ramach naszej praktyki life science wspieramy producentów, dystrybutorów i importerów w:

- analizie i ocenie ryzyka ,
- prowadzeniu badań klinicznych i działania,
- projektach IT w medycynie,
- projektach telemedycznych,
- zapewnianiu zgodności wyrobów medycznych,
- wprowadzeniu do obrotu wyrobów medycznych,
- zapewnieniu zgodności z przepisami dotyczącymi reklamy i promocji wyrobów medycznych
- zgodności z przepisami dotyczącymi prywatności i ochrony danych,
- współpracy z podmiotami trzecimi.

KANCELARIA JEST PARTNEREM:



Klaster
LifeScience
Kraków



MedSilesia
Śląska Sieć Wyrobów Medycznych



Masz wątpliwości w zakresie nowych regulacji dotyczących wYROBÓW medycznych?

Skontaktuj się ze mną



Błażej Wągiel

radca prawny

bwagiel@ipsolegal.pl

+48 509 163 107



WWW.IPSOLEGAL.PL