Bezpieczeństwo urządzeń medycznych – wspólna odpowiedzialność

W firmie Dräger rozwijamy technologie mające służyć ochronie życia. Technologie te podlegają ciągłym zmianom przy jednoczesnym szybkim postępie cyfryzacji opieki zdrowotnej. Pomagamy kształtować te zmiany, aby technologia przekładała się pozytywnie na opiekę nad pacjentami i sytuację finansową szpitali.

1. WPROWADZENIE

W firmie Dräger rozwijamy technologie mające służyć ochronie życia. Technologie te podlegają ciągłym zmianom przy jednoczesnym szybkim postępie cyfryzacji opieki zdrowotnej. Pomagamy kształtować te zmiany, aby technologia przekładała się pozytywnie na opiekę nad pacjentami i sytuację finansową szpitali. Już dziś, a w jeszcze większym stopniu w przyszłości, urządzenia oraz systemy medyczne są i będą łączone w sieci, aby wzajemnie współpracować i umożliwiać nowe zastosowania kliniczne, które obejmują technologie wspomagające procesy decyzyjne, możliwości zdalnego sterowania i automatyzację procesów. Wszystko to musi się jednak odbywać w bezpiecznym środowisku sieciowym, aby zagwarantować prawidłowe funkcjonowanie urządzeń i ochronę danych. Szpitale podejmują ogromne wysiłki w celu zabezpieczenia swoich sieci, a producenci powinni przyczyniać się do tworzenia tego bezpiecznego środowiska poprzez dostarczanie produktów, które są odporne na cyberataki i które mogą być bezpiecznie zintegrowane z sieciami szpitalnymi.
W miarę jak zagrożenia cyberbezpieczeństwa oraz ryzyka dla wewnętrznego i zewnętrznego otoczenia opieki zdrowotnej stale rosną, konieczne jest wprowadzenie sprawdzonych środków kontroli bezpieczeństwa w celu zapewnienia odpowiedniej ochrony pacjentów i ich danych.

Najlepszym sposobem na osiągnięcie tego celu jest wprowadzenie zabezpieczeń już na wczesnym etapie cyklu życia produktu przy zastosowaniu wielopłaszczyznowego podejścia w odniesieniu do standardów i najlepszych praktyk w zakresie cyberbezpieczeństwa. W firmie Dräger to wieloaspektowe podejście jest ściśle zintegrowane z procesami rozwoju produktów oraz z kontrolą techniczną. Nasze urządzenia i systemy medyczne są opracowywane zgodnie z aktualnymi najlepszymi praktykami w zakresie cyberbezpieczeństwa, przedstawionymi w niniejszym dokumencie. Dotyczy to wszystkich aktualnie rozwijanych produktów, jednak niekoniecznie całości asortymentu aktualnie dostępnego w sprzedaży. W przypadku tych produktów należy zwrócić się o formularz MDS2 do lokalnego przedstawiciela handlowego.

W tym opracowaniu przedstawiamy ogólny zarys tego, w jaki sposób wdrażamy zabezpieczenia w procesie rozwoju naszych urządzeń medycznych. Jeśli chcesz poznać więcej szczegółów technicznych na temat tego, jak w firmie Dräger zabezpieczamy wyroby medyczne, zachęcamy do zapoznania się z naszym stanowiskiem technicznym.

2. CYBERBEZPIECZEŃSTWO – WSPÓLNA ODPOWIEDZIALNOŚĆ

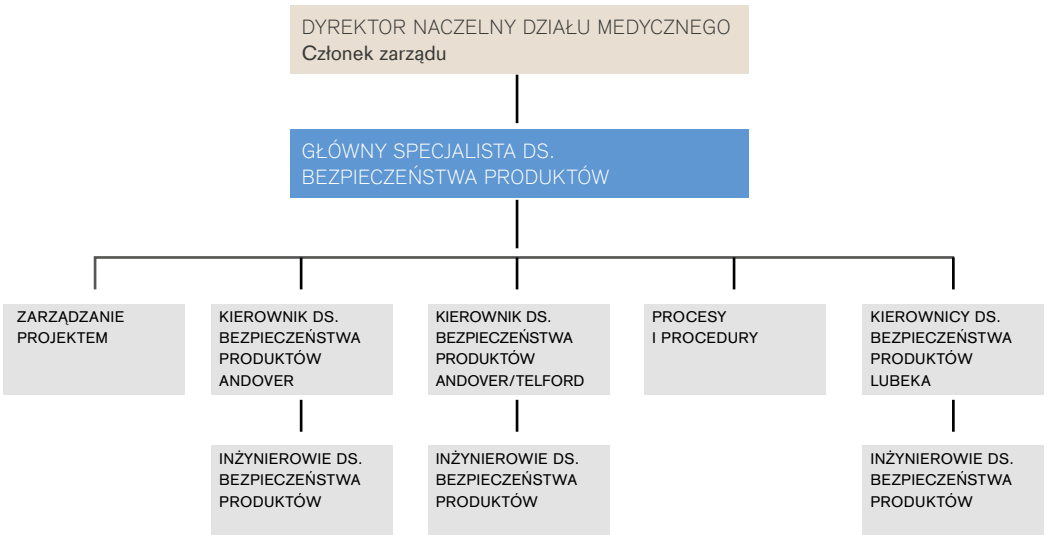
Nie ma czegoś takiego jak złoty środek w dziedzinie cyberbezpieczeństwa. Cyberbezpieczeństwo wymaga kompleksowego podejścia, logicznych i fizycznych środków kontroli w celu ochrony urządzeń medycznych, eliminacji zagrożeń powodujących straty dla pacjentów jak i strat finansowych dla jednostek opieki. Nie jest to przedsięwzięcie krótkoterminowe czy też działanie jednorazowe, lecz ciągły, wielowarstwowy proces minimalizowania ryzyka w odniesieniu do urządzeń medycznych, aby chronić pacjentów przed zagrożeniami.

W miarę jak systemy opieki zdrowotnej stają się w coraz większym stopniu oparte na technologii cyfrowej, bezpieczeństwo sieci szpitalnych nabiera coraz większego znaczenia ze względu na konieczność ograniczenia ryzyka związanego z atakami hakerskimi. W firmie Dräger wiemy, że szpitale stosują najlepsze praktyki w zakresie cyberbezpieczeństwa, aby chronić zarówno swoje sieci jak i zasoby. Naszym obowiązkiem jako dostawcy urządzeń sieciowych i systemów medycznych jest zagwarantowanie bezpiecznej integracji naszych produktów z siecią szpitalną.

Zasady bezpieczeństwa. Naszą wielopłaszczyznową strategię bezpieczeństwa najlepiej opisuje koncepcja „Defense-in-Depth" (Dogłębna Obrona). Nie mamy jednego rozwiązania ani procesu do zapewnienia cyberbezpieczeństwa – stosujemy raczej strategię opartą na warstwach w celu tworzenia zabezpieczeń w naszych urządzeniach i systemach. Strategia ta opiera się na tych samych najlepszych praktykach z zakresu cyberbezpieczeństwa, które coraz więcej szpitali stosuje w swoich strategiach bezpieczeństwa, dzięki czemu nasze urządzenia i systemy można bezproblemowo zintegrować z sieciami i koncepcjami bezpieczeństwa.

Wspólna odpowiedzialność. W celu uzyskania jak najskuteczniejszej ochrony przed cyberatakami najlepiej byłoby, gdyby zabezpieczenia w postaci najlepszych praktyk zostały wdrożone po obu stronach: w szpitalu do zarządzania bezpieczeństwem sieci, a w firmie Dräger do rozwoju bezpiecznych urządzeń sieciowych i systemów medycznych. W ten sposób cyberbezpieczeństwo staje się wspólną odpowiedzialnością. Szpital jest odpowiedzialny za integrację urządzeń medycznych w bezpiecznym środowisku sieciowym w oparciu o własne zasady bezpieczeństwa. Naszym obowiązkiem jako dostawcy urządzeń i systemów medycznych jest ochrona wewnętrznych elementów urządzenia medycznego aż do jego najgłębszej warstwy, aby zapewnić szpitalom możliwość monitorowania aktywności i zmian wprowadzanych w naszych urządzeniach medycznych oraz inicjowanych przez te urządzenia. Dodatkowo musimy zapewnić szpitalom wszelkie informacje i wsparcie niezbędne do bezpiecznego wdrożenia w środowisku sieciowym.

ORGANIZACJA DS. BEZPIECZEŃSTWA PRODUKTÓW W FIRMIE DRÄGER



Nasza organizacja zajmująca się bezpieczeństwem produktów stosuje warstwowe podejście do ochrony, aby zapewnić bezpieczne projektowanie i kontrolę naszych produktów.

Organizacja zajmująca się bezpieczeństwem produktów jest odrębna od organizacji zajmującej się rozwojem produktów i jest zlokalizowana w USA i Europie, co zapewnia jej autonomię i pozwala skupić się na kwestiach bezpieczeństwa, a nie na procesie rozwoju produktów.

Główny specjalista ds. bezpieczeństwa produktów jest odpowiedzialny za wszystkie produkty firmy Dräger i podlega bezpośrednio Zarządowi, który ponosi nadrzędną odpowiedzialność za zapewnienie bezpieczeństwa produktów firmy Dräger podczas ich wdrażania do środowiska organizacji opieki zdrowotnej.

Kierownicy ds. bezpieczeństwa produktów podlegają Głównemu specjaliście ds. bezpieczeństwa produktów i są odpowiedzialni za bezpieczeństwo wszystkich produktów.

Inżynierowie ds. bezpieczeństwa produktów podlegają kierownikom ds. bezpieczeństwa produktów i są odpowiedzialni za wszystkie kontrole i procesy bezpieczeństwa w ramach danego produktu.

Nasze procedury bezpieczeństwa oparte na najlepszych praktykach obejmują następujące funkcje:

IDENTYFIKACJA

Pomaga w rozwijaniu organizacyjnego zrozumienia dla zarządzania ryzykami w obszarze cyberbezpieczeństwa dotyczącymi systemów, ludzi, aktywów, danych i możliwości. Pozwala organizacji skupić się i określić priorytety swoich działań, zgodnie z jej strategią zarządzania ryzykiem oraz potrzebami biznesowymi.

OCHRONA

Określa odpowiednie zabezpieczenia w celu zapewnienia świadczenia usług w zakresie infrastruktury krytycznej. Funkcja ochrony umożliwia ograniczenie lub powstrzymanie skutków potencjalnego zdarzenia związanego z cyberbezpieczeństwem.

WYKRYWANIE

Określa odpowiednie działania mające na celu wykrycie wystąpienia zdarzenia związanego z cyberbezpieczeństwem. Funkcja ta umożliwia szybkie wykrycie zdarzeń związanych z cyberbezpieczeństwem.

REAGOWANIE

Obejmuje odpowiednie czynności w celu podjęcia działań w związku z wykrytym zdarzeniem związanym z cyberbezpieczeństwem. Funkcja ochrony umożliwia powstrzymanie skutków potencjalnego incydentu związanego z cyberbezpieczeństwem.

PRZYWRACANIE

Wspiera szybkie przywrócenie normalnej działalności w celu ograniczenia skutków zdarzenia związanego z cyberbezpieczeństwem.

Bezpieczeństwo od etapu projektowania. Od samego początku uwzględniamy bezpieczeństwo w wymaganiach dotyczących produktów. Dobrze zaprojektowana architektura bezpieczeństwa jest podstawą odporności i bezpiecznego działania naszych produktów. Choć całkowity brak luk w zabezpieczeniach jest niemożliwy do osiągnięcia, wkładamy ogromny wysiłek w proces zabezpieczania naszych urządzeń, aby były one odporne na zagrożenia w środowisku sieciowym.

Aby mieć pewność, że każda decyzja dotycząca projektu uwzględnia bezpieczeństwo, postępujemy zgodnie z wytycznymi, które nazywamy naszymi dziesięcioma zasadami przewodnimi w zakresie cyberbezpieczeństwa. Te przykazania odzwierciedlają dziesięć najważniejszych rzeczy, które należy rozważyć w kontekście integracji cyberbezpieczeństwa z naszymi produktami i systemami. Nasze produkty:

- nie są uzależnione od elementów wycofanych z produkcji, niewspieranych lub podatnych na ataki;
- działają na zasadzie najmniejszych możliwych uprawnień;
- dostarczane są domyślnie w najbezpieczniejszym stanie;
- nie są dostarczane z trwale zakodowanymi danymi uwierzytelniającymi;
- są projektowane od samego początku z uwzględnieniem bezpieczeństwa;
- są odporne na nieoczekiwane dane wejściowe pochodzące z każdego z ich interfejsów;
- są zaprojektowane tak, aby chronić wszystkie dane, będąc zarówno w stanie spoczynku, jak i w stanie pracy oraz przesyłu danych;
- nie mają ukrytych luk typu „backdoor", portów do debugowania ani zbędnego oprogramowania;
- są przystosowane do instalacji łatek zabezpieczających;
- chronią krytyczne funkcje przed nieuprawnionym dostępem.

Zapewniamy, że nasze produkty i systemy są zaprojektowane w taki sposób, aby zapewnić pożądany poziom bezpieczeństwa. Tworzymy modele zagrożeń, czyli analizę systemu z punktu widzenia atakującego, stosując się do najlepszych praktyk. Określamy możliwe motywy i wykorzystujemy model STRIDE[1] służący do mapowania kategorii zagrożeń na atrybuty bezpieczeństwa, aby zidentyfikować możliwe luki i problemy związane z bezpieczeństwem. W ten sposób zagrożenia mogą być oceniane i minimalizowane na wczesnym etapie projektowania systemów.

[1] Nazwa modelu STRIDE to akronim, gdzie kolejne litery oznaczają kolejne grupy zagrożeń: Spoofing (podszywanie się), Tampering (manipulowanie danymi), Repudiation (zatarcie śladów), Information disclosure (ujawnienie informacji), Denial of Service (zablokowanie lub ograniczenie dostępu) i Elevation of Privilege (podniesienie uprawnień).

Utrzymanie produktów i monitorowanie podatności na zagrożenia. Rozumiemy, jak ważne jest monitorowanie informacji dostępnych publicznie pod kątem luk w zabezpieczeniach. Nasz zespół ds. bezpieczeństwa produktów nieustannie monitoruje różne źródła informacji w poszukiwaniu opublikowanych luk bezpieczeństwa w komponentach innych firm i określa ich potencjalny wpływ na produkty firmy Dräger. Nasze źródła to między innymi National Vulnerability Database (NVD), lista CVE firmy MITRE, VulnDB oraz kilka kanałów RSS, list dyskusyjnych i stron internetowych odnoszących się do poszczególnych producentów. Ponadto firma Dräger jest członkiem Niemieckiego Stowarzyszenia na rzecz Cyberbezpieczeństwa („Allianz für Cybersicherheit"), które dostarcza aktualnych informacji o bieżących zagrożeniach i podatnościach.

Prowadzimy stronę poświęconą bezpieczeństwu produktów pod adresem

HTTPS://draeger.com/security

– znajdują się tam dane kontaktowe oraz informacje dotyczące procedur, które należy stosować w celu testowania i zgłaszania luk w zabezpieczeniach lub problemów związanych z bezpieczeństwem. Strona ta zawiera również informacje dotyczące procedur, które są stosowane każdorazowo po wystąpieniu incydentu oraz publiczne ostrzeżenia dotyczące bezpieczeństwa produktów.

KILKA SŁÓW NA KONIEC OD NASZEGO GŁÓWNEGO SPECJALISTY DS. BEZPIECZEŃSTWA PRODUKTÓW

Firma Dräger doskonale zdaje sobie sprawę ze swojej odpowiedzialności wobec pacjentów i szpitali. Dlatego wraz z moim zespołem ds. bezpieczeństwa produktów intensywnie pracujemy nad tym, aby mające miejsce cyberataki na szpitale nie oddziaływały na opiekę nad pacjentami ani na integralność danych pacjentów przechowywanych w naszych urządzeniach i systemach medycznych. Jako Twój Specjalista w Intensywnej Terapii posiadamy wiedzę oraz doświadczenie, aby pomóc Tobie i Twojemu szpitalowi utrzymać bezpieczną pracę naszych urządzeń medycznych w sieciach szpitalnych.

Naszą misją jest wdrażanie najlepszych praktyk w zakresie cyberbezpieczeństwa w proponowanych przez nas rozwiązaniach w celu zapewnienia najwyższego w branży poziomu ochrony i bezpieczeństwa. Jednocześnie dążymy do uczynienia przyszłych systemów opieki zdrowotnej bardziej bezpiecznymi. Nasze osobiste wartości, takie jak uczciwość, wiarygodność, profesjonalizm i wzajemny szacunek, odgrywają tu kluczową rolę. To właśnie tymi wartościami kieruję się zarówno ja i mój zespół.

Jeff Moore, Główny specjalista ds. bezpieczeństwa produktów

Więcej informacji na naszej stronie https://www.draeger.com/cybersecurity

WYDAWCA

NIEMCY
Drägerwerk AG & Co. KGaA
Moislinger Allee 53–55
23542 Lubeka

www.draeger.com

DMC-101134 | 21.11-1