European Union Agency
for Cybersecurity
Vasilissis Sofias Str 1
151 24 Maroussi | Attiki | Greece
Tel: +30 28 14 40 9711
E-mail: info@enisa.europa.eu
www.enisa.europa.eu

WYTYCZNE W ZAKRESIE ZAMÓWIEŃ DOTYCZĄCE CYBERBEZPIECZEŃSTWA W SZPITALACH

Sprawozdanie ma służyć jako „przewodnik” dla pracowników służby zdrowia. Wiele przedstawionych praktyk i zaleceń będzie też użytecznych dla innych organizacji służby zdrowia, ponieważ procesy zamówieniowe bywają bardzo podobne. Sprawozdanie przyda się osobom zajmującym stanowiska techniczne w szpitalach, tj. kierownictwu naczelnego szczebla: dyrektorom ds. informatycznych (CIO), dyrektorom ds. bezpieczeństwa informacji (CISO), dyrektorom technicznym (CTO), zespołom informatycznym, a także specjalistom ds. zamówień w organizacjach służby zdrowia. W niniejszym krótkim dokumencie omówiono główne zagadnienia poruszone w sprawozdaniu – szczegółowe informacje znajdują się w publikacji ENISA Dobre praktyki dotyczące bezpieczeństwa usług medycznych z lutego 2020 r.

PROCES UDZIELANIA ZAMÓWIEŃ

Ponieważ ekosystem szpitala składa się z kilku różnych komponentów informatycznych, cyberbezpieczeństwo należy analizować oddzielnie dla każdego z nich. Bezpieczeństwo cyberprzestrzeni należy uwzględniać na wszystkich etapach procesu udzielania zamówień. W tej części przedstawiamy wspólne etapy procesu udzielania zamówień na produkty i usługi, w tym wyroby medyczne, systemy informacyjne i infrastrukturę.

Wykres 1: Pełny cykl procesu udzielania zamówień w szpitalach

- Faza planowania: Na początku szpital analizuje swoje potrzeby i gromadzi wymagania zgłaszane przez różne wewnętrzne oddziały. Przykładowo, w przypadku pozyskiwania nowej usługi w chmurze dyrektor techniczny powinien zidentyfikować potrzeby i zrozumieć, jakie funkcje może wypełniać ta usługa.

- Faza pozyskiwania: Następnie zgłoszone wymagania uwzględnia się w specyfikacjach technicznych oraz – we współpracy z biurem zamówień – rozpoczyna się proces pozyskiwania (np. przez publikację przetargu). Szpital otrzymuje opisane oferty, a komisja (w której zasiadają dyrektor techniczny/dyrektor ds. bezpieczeństwa informacji bądź członek zespołu informatycznego) ocenia oferty i wybiera najbardziej odpowiednie produkty. Przeprowadza się negocjacje z kontrahentem i udziela się zamówienia.

- Faza zarządzania: Na koniec zamówienie (w tym zarządzanie nim i monitorowanie go) zostaje przypisane jednostce zajmującej się danym obszarem w szpitalu. Wyznaczony specjalista odpowiada za zakończenie przetargu i przyjmowanie opinii użytkowników dotyczących rzeczywistej skuteczności sprzętu/systemu/usługi.

RODZAJE ZAMÓWIEŃ W SZPITALACH

Tabela 1: Rodzaje zamówień (systematyka aktywów)

Rodzaj zamówień	Opis rodzaju zamówień
Systemy informacji klinicznych	Zamówienia dotyczące różnego rodzaju oprogramowania związanego z opieką zdrowotną.
Wyroby medyczne	Wszelkiego rodzaju sprzęt komputerowy przeznaczony do leczenia, kontroli lub diagnozowania chorób.
Sprzęt sieciowy	Linie sieciowe (koncentryczne, światłowodowe), bramy, routery, przełączniki, zapory, VPN-y, IPS-y, IDS-y itp.
Systemy teleopieki	Obiekty lub urządzenia do świadczenia opieki poza środowiskiem szpitalnym, zwłaszcza tzw. „szpitalnych usług opieki domowej”.
Mobilne urządzenia obsługi klienta	Wszystkie części oprogramowania wspomagającego opiekę zdrowotną lub gromadzącego dane medyczne, które nie są bezpośrednio podłączone do sieci szpitalnej; na przykład aplikacje do świadczenia telemedycyny.
Systemy identyfikacji	Systemy jednoznacznej identyfikacji pacjentów bądź personelu medycznego (skanery biometryczne, czytniki kart itp.) oraz gwarantowanej identyfikacji lub autoryzacji na potrzeby dostępu do systemów informatycznych.
Systemy zarządzania budynkami	Wszelkiego rodzaju konstrukcje, w których mogą się znajdować obiekty medyczne.
Przemysłowe systemy sterowania	Systemy sterowania wszystkimi fizycznymi elementami ośrodków, na przykład systemy regulacji zasilania, systemy zamykania drzwi, systemy ochrony przemysłowej (o obwodzie zamkniętym).
Usługi specjalistyczne	Wszelkiego rodzaju usługi, w tym zlecane na zewnątrz, świadczone przez specjalistów lub przedsiębiorstwa: usługi medyczne, transportowe, księgowe, techniczne, informatyczne, prawne, konserwacyjne, porządkowe, gastronomiczne itp.
Usługi w chmurze	Komputerowe systemy informacyjne (CIS) lub inne systemy informacyjne zlokalizowane poza budynkiem medycznym lub obiektem centrum danych będącym pod pełną kontrolą działu informatycznego ośrodka medycznego.

SYSTEMATYKA ZAGROŻEŃ

Różne rodzaje zamówień wiążą się z różnymi zagrożeniami dla teleinformatycznego środowiska szpitala. W tej części przedstawiono systematykę zagrożeń, aby czytelnicy – wraz ze swoimi działami informatyki, bezpieczeństwa lub ryzyka – mogli rozpoznać, które zagrożenia są najistotniejsze dla ich organizacji. Takie czynności powinny należeć do zadań informatycznych prowadzonych w szpitalu, niezależnie od jego możliwości zamówieniowych.

Tabela 2: Rodzaje zagrożeń (systematyka zagrożeń)

Zagrożenie	Przykłady
Zjawiska naturalne	Pożary, powodzie lub trzęsienia ziemi
Zakłócenie łańcucha dostaw	Zakłócenie po stronie dostawcy usług w chmurze, zakłócenie po stronie dostawcy sieci, awaria zasilania, zakłócenie/brak odpowiedzialności po stronie producenta wyrobów medycznych
Błędy ludzkie	Błąd w konfiguracji systemu medycznego, brak rejestrów audytu, kontrola nieuprawnionego dostępu/brak procesów, niezgodność z zasadami (w przypadku użycia prywatnych urządzeń (BYOD)), błąd personelu medycznego/pacjenta
Działania w złym zamiarze	Złośliwe oprogramowanie (wirusy, oprogramowanie typu ransomware, zdarzenia w przypadkach BYOD), złośliwe wydobywanie (kryptowalut i danych z urządzeń medycznych), inżynieria społeczna (fałszywe wiadomości i linki (phishing), oszustwa „na przynętę" (baiting), klonowanie urządzeń), kradzież (danych, urządzeń), manipulowanie urządzeniami medycznymi, przechwytywanie danych kart płatniczych (skimming), odmowa usługi, ataki sieciowe, ataki na aplikacje sieciowe, zagrożenie wewnętrzne, fizyczne manipulowanie/uszkodzenie, kradzież tożsamości, cyberszpiegostwo, mechaniczne zakłócanie pracy komponentów
Awarie systemów	Awaria oprogramowania, nieaktualne oprogramowanie układowe, awaria urządzenia, awaria komponentów sieci, niedostateczna konserwacja

DOBRE PRAKTYKI DOTYCZĄCE CYBERBEZPIECZEŃSTWA W ZAMÓWIENIACH

Poniższy wykaz dobrych praktyk nie jest wyczerpujący; stanowi jednak solidną pomoc dla pracowników służby zdrowia zajmujących się informatyką i odpowiedzialnych za zakup sprzętu w szpitalach. Ten zestaw dobrych praktyk jest zbiorczym zestawieniem wszystkich informacji zebranych od pracowników służby zdrowia, z którymi przeprowadzono rozmowy. Czytelnik może dostosować wykaz do priorytetów swojej organizacji.

Dobra praktyka 1. Zaangażowanie działu informatycznego na różnych etapach udzielania zamówień, aby uwzględniać wiedzę fachową z zakresu cyberbezpieczeństwa.

Fazy udzielania zamówień: wszystkie

Odnośne rodzaje zamówień: wszystkie

Odnośne zagrożenia: wszystkie

Dobra praktyka 2. Wdrażanie procesu identyfikacji podatności i zarządzania nimi w celu zapewnienia, aby uwzględniano podatności na zagrożenia przed zakupem nowych produktów lub usług bądź aby podatności istniejących produktów/usług na zagrożenia monitorowano w całym cyklu ich eksploatacji.

Fazy udzielania zamówień: wszystkie

Odnośne rodzaje zamówień: systemy informacji klinicznych, wyroby medyczne, sprzęt sieciowy, system teleopieki, mobilne urządzenia obsługi klienta, systemy identyfikacji, przemysłowe systemy sterowania, usługi w chmurze

Odnośne zagrożenia: wszystkie

Dobra praktyka 3. Opracowanie polityki aktualizacji sprzętu i oprogramowania w celu dopilnowania, aby stosowane były najnowsze poprawki systemu operacyjnego i oprogramowania oraz aby oprogramowanie antywirusowe było aktualizowane.

Fazy udzielania zamówień: wszystkie

Odnośne rodzaje zamówień: wyroby medyczne, systemy informacji klinicznych, sprzęt sieciowy, system teleopieki, mobilne urządzenia obsługi klienta, systemy identyfikacji, przemysłowe systemy sterowania, usługi w chmurze

Odnośne zagrożenia: działania w złym zamiarze, zakłócenie łańcucha dostaw, awarie systemów

Dobra praktyka 4. Wzmocnienie kontroli bezpieczeństwa łączności bezprzewodowej w celu zapewnienia, aby dostęp do szpitalnych sieci Wi-Fi był ograniczony i ściśle kontrolowany.

Fazy udzielania zamówień: wszystkie

Odnośne rodzaje zamówień: wyroby medyczne, zdalne urządzenia obsługi klienta, systemy identyfikacji, usługi w chmurze

Odnośne zagrożenia: działania w złym zamiarze, błędy ludzkie

Dobra praktyka 5. Tworzenie strategii testowania w celu zapewnienia, aby nowo nabyte lub na nowo skonfigurowane produkty przechodziły test penetracyjny oraz aby podejmowano działania zaradcze zgodnie z operacyjnymi parametrami rzeczywistego środowiska.

Fazy udzielania zamówień: wszystkie

Odnośne rodzaje zamówień: systemy informacji klinicznych, wyroby medyczne, sprzęt sieciowy, system teleopieki, mobilne urządzenia obsługi klienta, systemy identyfikacji, system zarządzania budynkiem, przemysłowe systemy sterowania, usługi w chmurze

Odnośne zagrożenia: działania w złym zamiarze, awarie systemów, błędy ludzkie

Dobra praktyka 6. Tworzenie planów ciągłości działania w celu zapewnienia, aby awaria któregoś systemu nie zakłóciła funkcjonowania podstawowych usług realizowanych przez szpital oraz aby rola dostawcy była wyraźnie określona.

Fazy udzielania zamówień: wszystkie

Odnośne rodzaje zamówień: wyroby medyczne, systemy informacji klinicznych, sprzęt sieciowy, system teleopieki, mobilne urządzenia obsługi klienta, systemy identyfikacji, przemysłowe systemy sterowania, usługi w chmurze

Odnośne zagrożenia: działania w złym zamiarze, zakłócenie łańcucha dostaw, awarie systemów

Dobra praktyka 7. Uwzględnianie kwestii interoperacyjności w celu zapobiegania problemom w zakresie bezpieczeństwa już istniejących komponentów (dotychczasowych systemów informatycznych).

Fazy udzielania zamówień: wszystkie

Odnośne rodzaje zamówień: systemy informacji klinicznych, wyroby medyczne, system teleopieki, mobilne urządzenia obsługi klienta, systemy identyfikacji, przemysłowe systemy sterowania, usługi w chmurze

Odnośne zagrożenia: awarie systemów, błędy ludzkie, działania w złym zamiarze

Dobra praktyka 8. Stworzenie możliwości testowania wszystkich komponentów w celu zagwarantowania ich zakładanych funkcji: sprawdzanie łatwości użycia, sprawdzanie poprawności wyników pod obciążeniem oraz sprawdzanie pod kątem wad zabezpieczeń (zasad dopuszczających słabe hasła, ataków typu SQL).

Fazy udzielania zamówień: wszystkie

Odnośne rodzaje zamówień: systemy informacji klinicznych, wyroby medyczne, zdalne urządzenia obsługi klienta, systemy identyfikacji, usługi w chmurze, przemysłowe systemy sterowania, system teleopieki, system zarządzania budynkiem, mobilne urządzenia obsługi klienta

Odnośne zagrożenia: działania w złym zamiarze, błędy ludzkie, awarie systemów, zakłócenie łańcucha dostaw

Dobra praktyka 9. Umożliwienie audytów i logowania w celu śledzenia sprawców ataków oraz skali utraty/kradzieży informacji w przypadku naruszenia systemu.

Fazy udzielania zamówień: wszystkie

Odnośne rodzaje zamówień: wyroby medyczne, system teleopieki, mobilne urządzenia obsługi klienta, systemy identyfikacji, przemysłowe systemy sterowania

Odnośne zagrożenia: działania w złym zamiarze, zakłócenie łańcucha dostaw, awarie systemów

Dobra praktyka 10. Szyfrowanie wrażliwych danych osobowych na czas ich przechowywania i przesyłania poprzez określenie zasad dotyczących systemów, usług lub urządzeń przetwarzających szczególne kategorie danych osobowych określone w art. 9 RODO.

Fazy udzielania zamówień: wszystkie

Odnośne rodzaje zamówień: wyroby medyczne, systemy informacji klinicznych, sprzęt sieciowy, system teleopieki, mobilne urządzenia obsługi klienta, systemy identyfikacji, przemysłowe systemy sterowania, usługi w chmurze

Odnośne zagrożenia: działania w złym zamiarze, zakłócenie łańcucha dostaw, awarie systemów

Dobra praktyka 11. Prowadzenie oceny ryzyka w ramach procesu udzielania zamówień.

Fazy udzielania zamówień: planowanie

Odnośne rodzaje zamówień: wszystkie

Odnośne zagrożenia: wszystkie

Dobra praktyka 12. Planowanie z wyprzedzeniem wymogów dotyczących sieci, sprzętu i licencji, aby ustalić, czy konieczne są dodatkowe aktualizacje lub zakupy przed instalacją nowego systemu.

Fazy udzielania zamówień: planowanie

Odnośne rodzaje zamówień: systemy informacji klinicznych, sprzęt sieciowy, systemy identyfikacji, przemysłowe systemy sterowania

Odnośne zagrożenia: zakłócenie łańcucha dostaw, awarie systemów, zjawiska naturalne, błędy ludzkie

Dobra praktyka 13. Rozpoznawanie zagrożeń związanych z produktami i usługami objętymi zamówieniami oraz dopilnowanie, aby zagrożenia były stale rozpoznawane w całym cyklu udzielania zamówień.

Fazy udzielania zamówień: planowanie, zarządzanie

Odnośne rodzaje zamówień: wszystkie

Odnośne zagrożenia: wszystkie

Dobra praktyka 14. Oddzielanie swojej sieci w celu zapewnienia, aby można było wydzielić lub przefiltrować ruch w sieci, a przez to ograniczyć lub zamknąć dostęp między strefami sieci.

Fazy udzielania zamówień: planowanie, pozyskiwanie

Odnośne rodzaje zamówień: wyroby medyczne, systemy informacji klinicznych, sprzęt sieciowy, system teleopieki, mobilne urządzenia obsługi klienta, systemy identyfikacji, przemysłowe systemy sterowania, usługi w chmurze

Odnośne zagrożenia: działania w złym zamiarze, zakłócenie łańcucha dostaw, awarie systemów

Dobra praktyka 15. Określenie wymogów dotyczących sieci w celu zapewnienia interoperacyjności i uniknięcia problemów po stworzeniu topologii sieci i komponentów.

Fazy udzielania zamówień: planowanie

Odnośne rodzaje zamówień: systemy informacji klinicznych, sprzęt sieciowy, systemy identyfikacji, przemysłowe systemy sterowania, usługi w chmurze, systemy teleopieki, mobilne urządzenia obsługi klienta

Odnośne zagrożenia: zakłócenie łańcucha dostaw, awarie systemów, zjawiska naturalne

Dobra praktyka 16. Ustanowienie bazowych wymogów dotyczących bezpieczeństwa i przełożenie ich na kryteria kwalifikowalności stosowane przy wyborze dostawców.

Fazy udzielania zamówień: planowanie, pozyskiwanie

Odnośne rodzaje zamówień: wyroby medyczne, systemy informacji klinicznych, sprzęt sieciowy, system teleopieki, mobilne urządzenia obsługi klienta, systemy identyfikacji, przemysłowe systemy sterowania, usługi w chmurze

Odnośne zagrożenia: działania w złym zamiarze, zakłócenie łańcucha dostaw, awarie systemów

Dobra praktyka 17. Stworzenie specjalnego zapytania ofertowego na potrzeby zamówień dotyczących usług w chmurze z uwzględnieniem wymogów w zakresie regulacji i polityki.

Fazy udzielania zamówień: planowanie, pozyskiwanie

Odnośne rodzaje zamówień: usługi w chmurze

Odnośne zagrożenia: działania w złym zamiarze, zakłócenie łańcucha dostaw

Dobra praktyka 18. Priorytetowe traktowanie zamówień dotyczących aktywów, które są certyfikowane pod kątem programów/norm cyberbezpieczeństwa.

Fazy udzielania zamówień: pozyskiwanie

Odnośne rodzaje zamówień: wyroby medyczne, systemy informacji klinicznych, sprzęt sieciowy, system teleopieki, mobilne urządzenia obsługi klienta, systemy identyfikacji, przemysłowe systemy sterowania, usługi w chmurze

Odnośne zagrożenia: działania w złym zamiarze, zakłócenie łańcucha dostaw, awarie systemów

Dobra praktyka 19. Prowadzenie ocen skutków dla ochrony danych przy planowaniu zamówienia na nowy system lub nową usługę.

Fazy udzielania zamówień: pozyskiwanie

Odnośne rodzaje zamówień: systemy informacji klinicznych, wyroby medyczne, sprzęt sieciowy, system teleopieki, mobilne urządzenia obsługi klienta, systemy identyfikacji, usługi specjalistyczne, usługi w chmurze

Odnośne zagrożenia: działania w złym zamiarze, błędy ludzkie

Dobra praktyka 20. Ustawianie bram sieciowych, przez które są podłączone dotychczasowe systemy/urządzenia i które zapewniają kontrolę wejściową w przypadku problemów wewnątrz tych grup.

Fazy udzielania zamówień: pozyskiwanie, zarządzanie

Odnośne rodzaje zamówień: wyroby medyczne, system teleopieki, mobilne urządzenia obsługi klienta, systemy identyfikacji, przemysłowe systemy sterowania

Odnośne zagrożenia: działania w złym zamiarze, zakłócenie łańcucha dostaw, awarie systemów

Dobra praktyka 21. Prowadzenie szkoleń z cyberbezpieczeństwa dotyczących praktyk organizacji w zakresie bezpieczeństwa w celu zapewnienia odpowiedniego przeszkolenia pracowników bądź kontrahentów/konsultantów zewnętrznych pracujących w obiektach organizacji.

Fazy udzielania zamówień: pozyskiwanie, zarządzanie

Odnośne rodzaje zamówień: wszystkie

Odnośne zagrożenia: działania w złym zamiarze, błędy ludzkie

Dobra praktyka 22. Opracowanie planów reagowania na incydenty obejmujących nowo nabyte produkty lub systemy.

Fazy udzielania zamówień: pozyskiwanie, zarządzanie

Odnośne rodzaje zamówień: wyroby medyczne, systemy informacji klinicznych, sprzęt sieciowy, system teleopieki, mobilne urządzenia obsługi klienta, systemy identyfikacji, przemysłowe systemy sterowania, usługi w chmurze

Odnośne zagrożenia: działania w złym zamiarze, zakłócenie łańcucha dostaw, awarie systemów

Dobra praktyka 23. Udział sprzedawcy/producenta w zarządzaniu incydentami i określenie jasnych warunków w zapytaniu ofertowym.

Fazy udzielania zamówień: pozyskiwanie, zarządzanie

Odnośne rodzaje zamówień: wyroby medyczne, systemy informacji klinicznych, sprzęt sieciowy, system teleopieki, mobilne urządzenia obsługi klienta, systemy identyfikacji, przemysłowe systemy sterowania, usługi w chmurze

Odnośne zagrożenia: działania w złym zamiarze, zakłócenie łańcucha dostaw, awarie systemów

Dobra praktyka 24. Zaplanowanie i monitorowanie czynności konserwacyjnych w odniesieniu do wszystkich urządzeń w celu zapewnienia odpowiedniego poziomu funkcjonalności oraz podejmowania decyzji dotyczących ewentualnych aktualizacji/poprawek itp.

Fazy udzielania zamówień: pozyskiwanie, zarządzanie

Odnośne rodzaje zamówień: systemy informacji klinicznych, sprzęt sieciowy, wyroby medyczne, systemy zarządzania budynkami, system teleopieki, mobilne urządzenia obsługi klienta, systemy identyfikacji, przemysłowe systemy sterowania, usługi w chmurze

Odnośne zagrożenia: błąd ludzki, awaria systemu, zjawiska naturalne

Dobra praktyka 25. Dostęp zdalny powinien mieć jak najmniejszy zakres i należy nim administrować w taki sposób, aby komunikacja zewnętrzna z dostawcą była ograniczona wyłącznie do urządzenia, nad którym dostawca ma kontrolę.

Fazy udzielania zamówień: pozyskiwanie, zarządzanie

Odnośne rodzaje zamówień: wyroby medyczne, systemy informacji klinicznych, sprzęt sieciowy, system teleopieki, mobilne urządzenia obsługi klienta, systemy identyfikacji, przemysłowe systemy sterowania, usługi w chmurze

Odnośne zagrożenia: działania w złym zamiarze, zakłócenie łańcucha dostaw, awarie systemów, błędy ludzkie

Dobra praktyka 26. Stosowanie wymogu wprowadzania poprawek w odniesieniu do wszystkich komponentów oraz ujęcie odpowiednich informacji w zapytaniu ofertowym.

Fazy udzielania zamówień: pozyskiwanie, zarządzanie

Odnośne rodzaje zamówień: wyroby medyczne, systemy informacji klinicznych, sprzęt sieciowy, system teleopieki, mobilne urządzenia obsługi klienta, systemy identyfikacji, przemysłowe systemy sterowania, usługi w chmurze

Odnośne zagrożenia: działania w złym zamiarze, zakłócenie łańcucha dostaw, awarie systemów

Dobra praktyka 27. Zwiększanie poziomu wiedzy pracowników o cyberbezpieczeństwie, aby mieli oni świadomość zagrożeń związanych z nowo pozyskanymi produktami lub usługami.

Fazy udzielania zamówień: zarządzanie

Odnośne rodzaje zamówień: wszystkie

Odnośne zagrożenia: wszystkie

Dobra praktyka 28. Prowadzenie wykazu mienia i zarządzanie ustawieniami w celu zapewnienia, aby po dodaniu lub usunięciu dowolnego komponentu w środowisku teleinformatycznym wykaz ten był odpowiednio aktualizowany oraz aby istniały bazowe ustawienia bezpieczeństwa komponentów teleinformatycznych i odpowiednio nimi zarządzano.

Fazy udzielania zamówień: zarządzanie

Odnośne rodzaje zamówień: systemy informacji klinicznych, wyroby medyczne, sprzęt sieciowy, system teleopieki, mobilne urządzenia obsługi klienta, systemy identyfikacji

Odnośne zagrożenia: działania w złym zamiarze, błędy ludzkie, awarie systemów

Dobra praktyka 29. Ustanowienie specjalnych mechanizmów kontroli dostępu do obiektów z wyrobami medycznymi: obiekty te powinny być objęte ochroną fizyczną i dostępne jedynie dla wyspecjalizowanych pracowników.

Fazy udzielania zamówień: zarządzanie

Odnośne rodzaje zamówień: wyroby medyczne, system zarządzania budynkiem, systemy identyfikacji

Odnośne zagrożenia: działania w złym zamiarze, błędy ludzkie

Dobra praktyka 30. Częste organizowanie testów penetracyjnych lub prowadzenie ich po wprowadzeniu zmiany w architekturze/systemie oraz ujęcie odpowiednich warunków w zapytaniu ofertowym.

Fazy udzielania zamówień: pozyskiwanie, zarządzanie

Odnośne rodzaje zamówień: wyroby medyczne, systemy informacji klinicznych, sprzęt sieciowy, system teleopieki, mobilne urządzenia obsługi klienta, systemy identyfikacji, przemysłowe systemy sterowania, usługi w chmurze

Odnośne zagrożenia: działania w złym zamiarze, zakłócenie łańcucha dostaw, awarie systemów