**EZ/93/2023/ESŁ**

**Szczegółowy opis przedmiotu zamówienia (SOPZ)**

**1. Szacowanie ryzyka,** w tym:

a) opracowanie pełnego szacowania ryzyka procesów zachodzących w Szpitalu w zakresie wynikającym z decyzji o wyznaczeniu WSzZ w Kielcach na Operatora Usługi Kluczowej, z uwzględnieniem w szczególności:

- analizy aktywów, ich wartości, potencjalnych zagrożeń, prawdopodobieństwa wystąpienia tych zagrożeń w szczególności w zakresie wystąpienia incydentu, podatności aktywu na zagrożenie, wpływ zagrożenia na bezpieczeństwo aktywu oraz stosowanie zabezpieczeń w kontekście możliwości zaburzenia lub przerwania ciągłości usługi kluczowej,

- opracowanie planu postępowania z ryzykiem,

- opracowanie wyników szacowania ryzyka, ze wskazaniem obszarów najbardziej zagrożonych, które z punktu widzenia usługi kluczowej wymagają poprawy w pierwszej kolejności,

b) prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu w zakresie usług kluczowych, z uwzględnieniem w szczególności:

- zarządzanie ryzykiem poprzez m.in. ponowne szacowanie ryzyka z uwzględnieniem zmian i aktualizacji poziomu zabezpieczeń, nie rzadziej niż raz w roku lub po każdej zmianie, która może mieć istotny wpływ na usługi kluczowe,

- prowadzenia działań mających na celu minimalizację ryzyka.

Szacowanie ryzyka musi zostać przeprowadzone zgodnie z normami ISO 27001 i ISO 31000.

**2. Monitorowanie w trybie ciągłym systemów teleinformatycznych oraz sieci Zamawiającego oraz reagowanie na pojawiające się zdarzenia (SOC).**

Usługa świadczona za pomocą narzędzi Wykonawcy, przez jego zespół i na jego infrastrukturze w zakresie cyberbezpieczeństwa, zgodnie z wymaganiami Rozporządzenia Ministra Cyfryzacji z dnia 4 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo (Dz.U. z 2019 r. poz. 2479).

Wymagania dla usługi Security Operations Center (SOC)

2.1. Wymagania podstawowe:

2.1.1. Wdrożenie i świadczenie usługi SOC poprzedzone jest audytem teleinformatycznym infrastruktury klienta, dzięki czemu możliwe jest dokonanie inwentaryzacji, wskazanie kluczowych serwerów oraz optymalizacja prac wdrożeniowych SOC.

2.1.2. Usługa świadczona przez Wykonawcę w czasie rzeczywistym w trybie 24 godziny/ 7 dni w tygodniu/ 365 dni w roku.

a) czas reakcji: …………….. ***(od 15 minut do 60 minut - kryterium oceny ofert******),*** rozumiane jako rozpoczęcie działań związanych z obsługą zidentyfikowanego incydentu poważnego;

b) dostępność usługi na poziomie co najmniej 99,6%

2.1.3. Usługa SOC, ma być odporna na przerwy w połączeniu sieciowym infrastruktury Zamawiającego z Wykonawcą, zapewniać ciągłość monitorowania oraz dostęp lokalny dla Zamawiającego do zdarzeń z monitorowanych systemów,

2.1.4. Usługa zapewnia:

a) Centrum Kontaktowe,

b) monitorowanie infrastruktury teleinformatycznej i reakcja na incydent bezpieczeństwa,

c) zarządzanie podatnościami,

d) dostarczenie systemu SIEM w modelu usługowym: ……………………...…………………. typ, model oprogramowania SIEM ***(zgodny ze wskazanym w formularzu ofertowym)***,

e) utrzymanie i doskonalenie systemu SIEM,

f) wsparcie w zakresie architektury bezpieczeństwa,

g) wsparcie w zakresie zarządzania zgodnością działalności z normami, zaleceniami i stosowanymi praktykami

2.2. Centrum Kontaktowe (2.1.4.a) zakłada:

a) dostępność Centrum Kontaktowego w trybie 24 godziny/ 7dni w tygodniu/ 365 dni w roku,

b) przekazanie przez Wykonawcę Zamawiającemu danych kontaktowych, w tym co najmniej: adres e-mail oraz nr telefonu,

c) możliwość zgłaszania zdarzeń zidentyfikowanych przez użytkowników systemów teleinformatycznych Zamawiającego, konsultacje techniczne w ramach zidentyfikowanych zagrożeń,

2.3. Monitorowanie i reakcja na incydent bezpieczeństwa (2.1.4.b) obejmuje co najmniej:

a) monitorowanie systemów teleinformatycznych oraz sieci Zamawiającego;

b) agregację, korelację oraz analizowanie zdarzeń, które zachodzą w systemach oraz sieci Zamawiającego;

c) podstawową obsługę incydentów bezpieczeństwa;

d) zaawansowaną obsługę incydentu w zakresie bezpieczeństwa teleinformatycznego, organizacyjnego i prawnego przez wykwalifikowany zespół wsparcia Wykonawcy;

e) utrzymanie oraz rozbudowanie procedur reakcji na incydent;

f) wsparcie Zamawiającego przy wdrożeniu rekomendacji po wystąpieniu incydentu;

2.4. Zarządzanie podatnościami (2.1.4.c) obejmuje co najmniej:

a) monitoring zewnętrzny publicznej klasy adresowej w zakresie zmian udostępnionych usług;

b) cykliczne skanowanie podatności zasobów, zbieranie informacji o zagrożeniach i podatnościach na incydenty systemu informacyjnego wykorzystywanego przez Zamawiającego do świadczenia usług kluczowych;

c) opracowanie rekomendacji dla zidentyfikowanych podatności;

d) dostarczenie rekomendacji dla zidentyfikowanych podatności dot. potencjalnego dostępu do systemu teleinformatycznego Wykonawcy;

2.5. Dostarczenie systemu SIEM w modelu usługowym, (2.1.4.d) obejmuje co najmniej:

a) zapewnienie niezbędnych licencji (jeżeli są wymagane) do działania systemu SIEM,

b) konfiguracje, wdrożenie, uruchomienie i zapewnienie ciągłości działania systemu SIEM,

c) wdrożenie systemu SIEM nie może zaburzyć działania usług kluczowych w środowisku Zamawiającego,

d) sporządzenie i aktualizowanie dokumentacji technicznej zawierającej opis funkcjonalny i konfigurację wdrożonego systemu SIEM,

e) instruktaż dla administratorów Zamawiającego w zakresie lokalnej obsługi zdarzeń zarejestrowanych w systemie SIEM,

f) rozpoczęcie świadczenia usługi SOC (w oparciu o system SIEM) przy założeniu monitorowania nie mniej niż 100 punktów, najważniejszych dla usług kluczowych,

g) możliwość rozszerzania, w trakcie trwania umowy (bez ponoszenia dodatkowych kosztów przez Zamawiającego), ilości źródeł danych i monitorowanych punktów w zależności od oszacowanego ryzyka i zaleceń oraz bieżącej analizy zdarzeń.

2.6. Utrzymanie i doskonalenie systemu SIEM (2.1.4.e) obejmuje co najmniej:

a) utrzymanie, optymalizacja działania oraz zarządzanie systemem SIEM;

b) rozwój sprawności detekcji zdarzeń bezpieczeństwa;

c) integrację nowych źródeł danych;

d) budowanie i aktualizację reguł korelacyjnych;

e) utrzymanie dokumentacji technicznej rozwiązania.

2.7. Wsparcie w zakresie architektury bezpieczeństwa (2.1.4.f) zakłada:

a) nadzór nad rozwojem utrzymywanego modelu bezpieczeństwa teleinformatycznego;

b) opracowanie cyklicznych rekomendacji dot. modelu bezpieczeństwa na podstawie informacji i ryzyk pozyskanych w ramach obsługi incydentu bezpieczeństwa.

2.8. Wsparcie w zakresie zarządzania zgodnością zakłada:

a) nadzór nad rozwojem utrzymywanego modelu bezpieczeństwa organizacyjnego i prawnego;

b) transfer informacji operacyjnej na poziom zarządczy w ramach analizy ryzyka;

**3. Zarządzanie incydentami**, w tym:

a) opracowanie procedury obsługi incydentów, które mogą obniżać jakość lub przerwać ciągłość świadczenia usługi kluczowej,

Procedury obsługi incydentów muszą uwzględniać co najmniej:

- kategorie incydentów bezpieczeństwa,

- przyczyny incydentów bezpieczeństwa,

- zgłaszanie incydentów związanych z bezpieczeństwem,

- podejmowanie działań w związku ze zgłaszanymi incydentami związanymi z bezpieczeństwem.

b) obsługa incydentów, reakcja na występujące incydenty, zgłaszanie w imieniu Zamawiającego incydentów poważnych do właściwego CSIRT w rozumieniu art. 11 ustawy KSC:

- zapewnienie bieżącej, realizowanej w trybie ciągłym, obsługi incydentu (w tym klasyfikowanie i raportowanie incydentów poważnych do CSIRT),

- przejęcie przez Wykonawcę obowiązku utrzymywania kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa (w tym z CSIRT NASK), w tym wskazanie osoby do kontaktu z CSiRT.

**4. Opracowanie dokumentacji dla Szpitala dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej** zgodnie z Rozporządzeniem Rady Ministrów z dnia 16 października 2018 r w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (Dz.U. z 2018 r. poz. 2080).

4.1. Dokumentacja dotycząca cyberbezpieczeństwa systemu informacyjnego, zgodnie z w/w Rozporządzeniem, musi zawierać:

4.1.1. Dokumentację normatywną:

1) dokumentacja dotycząca systemu zarządzania bezpieczeństwem informacji wytworzona zgodnie z wymaganiami normy PN-EN ISO/IEC 27001;

2) dokumentacja ochrony infrastruktury, z wykorzystaniem której świadczona jest usługa kluczowa, dotycząca:

a) charakterystyki usługi kluczowej oraz infrastruktury,

b) szacowania ryzyka dla obiektów infrastruktury,

c) oceny aktualnego stanu ochrony infrastruktury (plan postępowania z ryzykiem),

d) opisu zabezpieczeń technicznych obiektów infrastruktury,

e) zasad organizacji i wykonywania ochrony fizycznej infrastruktury,

f) danych o specjalistycznej uzbrojonej formacji ochronnej, o której mowa w art. 2 pkt 7 ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz.U. z 2021 r., poz. 1995 t.j.  ), chroniącej infrastrukturę, jeśli taka formacja występuje;

3) dokumentacja systemu zarządzania ciągłością działania usługi kluczowej wytworzona zgodnie z wymaganiami normy PN-EN ISO 22301;

4) dokumentacja techniczna systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej;

5) dokumentacja wynikająca ze specyfiki świadczonej usługi kluczowej w danym sektorze lub podsektorze.

4.1.2. Dokumentacja operacyjna:

1) dokumentacja dotycząca procedur oraz instrukcji wynikających z dokumentacji normatywnej;

2) opisy sposobów dokumentowania wykonania czynności w ramach ustalonych procedur;

3) dokumentacja poświadczająca każdorazowe wykonanie procedury.

4.2. Wykonawca przekaże Zamawiającemu prawa autorskie do opracowanej dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej.

4.3. Wykonawca w czasie trwania umowy zobowiązany jest aktualizować dokumentację dotyczącą cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, oraz pełnić nadzór nad tą dokumentacją, przy uwzględnieniu konieczności zapewnienia:

a) dostępności dokumentów wyłącznie dla osób upoważnionych zgodnie z realizowanymi przez nie zadaniami;

b) ochronę dokumentów przed niewłaściwym użyciem lub utratą integralności;

c) oznaczanie kolejnych wersji dokumentów umożliwiające określenie zmian dokonanych w tych dokumentach.

**5. Wsparcie Zamawiającego w działaniach edukacyjnych w zakresie cyberbezpieczeństwa** poprzez, m.in. opracowanie materiałów edukacyjnych kierowanych do użytkowników systemów usług kluczowych w celu ich udostępnienia np. na stronach Zamawiającego, opracowanie ostrzeżeń i rekomendacji w zakresie przeciwdziałania nowym cyberzagrożeniom (min. 1 raz na 3m-ce).

Materiały edukacyjne powinny obejmować zakres tematyczny związany z systemami teleinformatycznymi, wykorzystywanymi do usług kluczowych, w tym m.in.:

a) Zagrożenia w cyberprzestrzeni:

− phishing (phishing, spearphishing, walling, smishing, wyszukiwarkowy, vishing)

− ransomware

− wycieki danych

− ataki na IoT

− omówienie incydentów bezpieczeństwa ze świata i z Polski (szczególnie w jednostkach ochrony zdrowia)

b) Zasady Bezpieczeństwa

− bezpieczeństwo haseł

− bezpieczeństwo pracy z pocztą elektroniczną

− bezpieczeństwo urządzeń mobilnych

− bezpieczne korzystanie z urządzeń drukujących

− bezpieczne korzystanie z urządzeń USB

− bezpieczne korzystanie z sieci internet i portali społecznościowych.

**6. Wsparcie Zamawiającego i konsultacje w zakresie doboru i wdrażania środków technicznych i organizacyjnych, odpowiednich i proporcjonalnych do szacowanego ryzyka, mających wpływ na bezpieczeństwo teleinformatyczne Szpitala.**

Wykonawca zapewni pomoc w analizie wyników szacowanego ryzyka i doborze adekwatnych i możliwych do zaimplementowania w środowisku teleinformatycznym Zamawiającego, rozwiązań w celu poprawy bezpieczeństwa informatycznego. Wsparcie w tym zakresie powinno uwzględniać optymalizację pod kątem planowanych celów oraz możliwości organizacyjnych i finansowych.

**7. Wspieranie Zamawiającego w zakresie: identyfikowania zagrożeń w odniesieniu do systemów informacyjnych; analizowania oprogramowania szkodliwego i określania jego wpływu na system informacyjny Zamawiającego; zabezpieczania śladów kryminalistycznych na potrzeby postępowań prowadzonych przez organy ścigania.**

Wsparcie w tym zakresie powinno być realizowane co najmniej poprzez:

1. identyfikowanie zagrożeń w odniesieniu do systemów informatycznych, z uwzględnieniem w szczególności:

- zablokowania dostępu do usługi kluczowej,

- włamania do systemu informatycznego,

- utraty danych,

- kradzieży danych,

- ujawnienia danych poufnych,

- zafałszowania informacji,

- kradzieży sprzętu,

- uszkodzenia systemów komputerowych,

1. analizowanie zidentyfikowanego oprogramowania szkodliwego i określanie jego wpływu na system informacyjny, której celem jest w szczególności:

- ujawnienie przeznaczenia tego oprogramowania,

- katalogu metod interakcji z systemem operacyjnym,

- sposobu działania,

- użytych metod komunikacji,

- zmian wprowadzanych w systemie plików,

- zmian wprowadzanych w konfiguracji stacji roboczej,

- metod zapewnienia persystencji (przetrwania w systemie),

- metod odtworzenia stanu stacji roboczej sprzed uruchomienia malware,

- prawdopodobnego autora oprogramowania,

- okoliczności wytworzenia oprogramowania,

- wykorzystanych podatności.

1. zabezpieczenie informacji potrzebnych do analizy powłamaniowej powinny pozwolić na określenie wpływu incydentu poważnego na świadczenie usługi kluczowej, w tym informacji dotyczących:

– rodzajów usług kluczowych, na które incydent miał wpływ,

– liczby użytkowników usługi kluczowej, na których incydent miał wpływ,

– momentu wystąpienia i wykrycia incydentu oraz czasu jego trwania,

– zasięgu geograficznego obszaru, którego dotyczy incydent poważny,

– wpływu incydentu na świadczenie usługi kluczowej przez innych operatorów usług kluczowych i dostawców usług cyfrowych,

– przyczyny zaistnienia incydentu i sposób jego przebiegu oraz skutków jego oddziaływania na systemy informacyjne lub świadczone usługi kluczowe na potrzeby postępowań prowadzonych przez organy ścigania.

**8. Przeprowadzenie dwóch audytów zgodności bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej** z wymaganiami ustawy o krajowym systemie cyberbezpieczeństwa, zgodnie z wymogami art.15 ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (tj. Dz.U. z 2022 r. poz. 1863). W wyniku audytu ma zostać sporządzone pisemne sprawozdanie z przeprowadzonego audytu, które ma być przekazane Zamawiającemu wraz z dokumentacją z przeprowadzonego audytu.

8.1. Audyty mają być przeprowadzone zgodnie ze szczegółowymi wytycznymi, określonymi w przytoczoną powyżej Ustawą oraz obowiązującymi w tym zakresie rozporządzeniami wykonawczymi.

8.2.Terminy przeprowadzenia dwóch audytów bezpieczeństwa systemu informatycznego wykorzystywanego do świadczenia usługi kluczowej wynikają z Ustawy o krajowym systemie cyberbezpieczeństwa oraz decyzji o uznaniu Zamawiającego za operatora usługi kluczowej.

8.3. Każdy z dwóch Audytów powinien być zakończony sprawozdaniem, zgodnym z ustawą o krajowym systemie cyberbezpieczeństwa, sporządzonym wg szablonu opublikowanego w serwisie www.gov.pl.