Opis przedmiotu szacowania

Przedmiotem szacowania jest przeprowadzenie audytu bezpieczeństwa.

1. Cel audytu

Celem audytu jest wykazanie przez świadczeniodawcę podniesienia poziomu bezpieczeństwa teleinformatycznego po zrealizowaniu czynności, zgodnie z zarządzeniem **NR 68/2022/BBIICD PREZESA NARODOWEGO FUNDUSZU ZDROWIA** oraz w odniesieniu do stanu na dzień przeprowadzenia badania poziomu dojrzałości cyberbezpieczeństwa u Zamawiającego w formie ankiety. Przeprowadzony audyt wykaże podniesienie poziomu bezpieczeństwa teleinformatycznego w odniesieniu do poziomu wynikającego z ankiety lub jego brak. Raport musi zawierać jasne stanowisko audytora w zakresie wykazania, że spożytkowane środki wpłynęły na podniesienie poziomu bezpieczeństwa.

Nazwa obszaru	**Opis działań skutkujących podniesieniem poziomu bezpieczeństwa teleinformatycznego świadczeniodawców**
Skuteczność działania infrastruktury	- Urządzenia i konfiguracja w zakresie ochrony poczty - Urządzenia i konfiguracja w zakresie ochrony sieci - Urządzenia i konfiguracja w zakresie systemów serwerowych - Urządzenia i konfiguracja w zakresie stacji roboczych - Urządzenia i konfiguracja w zakresie systemów bezpieczeństwa
Procesy zarządzania bezpieczeństwem informacji	- Nośniki wymienne - udokumentowany sposób postępowania - Zarządzanie tożsamością / dostęp do systemów w zakresie: -- Przydzielanie dostępu -- Odbieranie dostępu - Pomieszczenie w dyspozycji struktur zespołu odpowiedzialnego za cyberbezpieczeń- stwo w przypadku podmiotów, które otrzymały decyzję uznającą taki podmiot za ope ratora usługi kluczowej, o którym mowa w art. 5 *ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa*
Monitorowanie i reagowanie na incydenty bezpieczeństwa	- Procedury zarządzania incydentami - Raportowanie poziomów pokrycia scenariuszami znanych incydentów - Dokumentacja dotycząca przekazywania informacji do właściwego zespołu CSIRT poziomu krajowego/ sektorowego zespołu cyberbezpieczeństwa - Monitorowanie i wykrycie incydentów bezpieczeństwa - Identyfikacja i dokumentowanie przyczyn wystąpienia incydentów
Zarządzanie ciągłością działania	- Konfiguracja oraz polityki systemów do wykonywania kopii bezpieczeństwa - Raport z przeglądów i testów odtwarzania kopii bezpieczeństwa - Procedury wykonywania i przechowywania kopii zapasowych - Strategia i polityka ciągłości działania, awaryjne oraz odtwarzania po katastrofie (DRP) - Procedury utrzymaniowe
Utrzymanie systemów informacyjnych	- Harmonogramy skanowania podatności - Aktualny status realizacji postępowania z podatnościami - Procedury związane ze z identyfikowaniem (wykryciem) podatności - Współpraca z osobami odpowiedzialnymi za procesy zarządzania incydentami

Zarządzanie bezpieczeństwem i ciągłością działania łańcucha usług	- Polityka bezpieczeństwa w relacjach z dostawcami - Standardy i wymagania nakładane na dostawców w umowach w zakresie cyberbez pieczeństwa - Dostęp zdalny - Metody uwierzytelnienia

2. Przedmiotem zamówienia jest wykonanie usługi polegającej na:

a. wykonaniu audytu bezpieczeństwa, w tym:

a) inwentaryzacji obszarów z przetwarzaniem informacji w systemach informacyjnych wraz z otoczeniem,
b) identyfikacja informacji i jej klasyfikacja,
c) inwentaryzacja zasobów infrastruktury teleinformatycznej, oprogramowania i obszarów bezpiecznych,
d) identyfikacja podatności,
e) identyfikacja dostawców,
f) przegląd i inwentaryzacja procedur,
g) przegląd dokumentacji,
h) zidentyfikowaniu wszelkich niezgodności i wskazanie działań naprawczych,

b. wskazanie możliwości wdrożenia procesu zarządzania incydentami bezpieczeństwa, pozwalający m.in. na zgłaszanie poważnych incydentów do krajowego zespołu CSIRT w czasie nieprzekraczającym 24 godzin od ich wykrycia,
c. wskazanie sprawnego procesu zarządzania podatnościami i gromadzenia wiedzy na temat zagrożeń cyberbezpieczeństwa,
d. opracowanie dokumentacji dotyczącej cyberbezpieczeństwa systemów informatycznych oraz bezpieczeństwa przetwarzania informacji wykorzystywanych do świadczenia usług,
e. opracowanie dokumentacji w rozumieniu ustawy KSC i rozporządzenia w sprawie rodzajów dokumentacji w szczególności:

- dokumentacja o stosowanym systemie zarządzania bezpieczeństwem informacji w tym opracować procedury działania w przypadku naruszenia bezpieczeństwa systemu informacyjnego,
- dokumentacja ochrony fizycznej i środowiskowej infrastruktury służącej do świadczenia usługi kluczowej (w tym szacowania ryzyka),
- dokumentacja zapewnienia ciągłości działania (Business Continuity Management),
- dokumentacja techniczna systemu informacyjnego służącego do świadczenia usługi kluczowej,

f. przeprowadzenie audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usług zgodnego z wymogami ustawy KSC w szczególności zgodnie z zapisem art. 15 ust. 2 pkt 2 lit a ustawy KSC.
a. Weryfikacja przywództwa
b. Weryfikacja polityk bezpieczeństwa
c. Weryfikacja ról, odpowiedzialności i uprawnień
d. Weryfikacja działań odnoszących się do ryzyka i szans
e. Weryfikacja wsparcia dla SZBI, w tym zasoby, kompetencje, uświadamianie, komunikację i dokumentowanie
f. Weryfikacja działań operacyjnych i ciągłości działania
g. Weryfikacja adekwatności zabezpieczeń do zidentyfikowanych zagrożeń,

h. Weryfikacja oceny wyników SZBI w tym monitorowanie, pomiary, analiza, ocena, audyty wewnętrzne i przeglądy zarządzania
i. Weryfikacja ciągłego doskonalenia
j. Weryfikacja zgodności dokumentacji z normami i stanem faktycznym

k. Przygotowanie raportu, który wykaże podniesienie poziomu bezpieczeństwa teleinformatycznego w odniesieniu do poziomu wynikającego z ankiety (która będzie udostępniona po podpisaniu umowy) lub jego brak zgodnie ze stanem na dzień przeprowadzenia badania poziomu dojrzałości cyberbezpieczeństwa u Zamawiającego. Raport musi zawierać jasne stanowisko audytora w zakresie wykazania, że spożytkowane środki wpłynęły na podniesienie poziomu bezpieczeństwa. Raport przygotowany zostanie po wdrożeniu rozwiązań podnoszących poziom cyberbezpieczeństwa dofinansowanych ze środków pochodzących z funduszu przeciwdziałania COVID-19, po wykonaniu audytu. Raport musi być przygotowany i przekazany Zamawiającemu nie później niż do 21.11.2022 r.

Ponadto Zamawiający wymaga dokonania testów penetracyjnych i analizy wdrożonych u Zamawiającego środków bezpieczeństwa obejmujących:

1) Zabezpieczenia wdrożone na urządzeniach końcowych (komputery przenośne, stacje robocze, urządzenia mobilne itp.) w liczbie ok. 1200

2) Zabezpieczenia wdrożone w sieci lokalnej LAN Zamawiającego;

3) Zabezpieczenia wdrożone w systemach informatycznych Zamawiającego ulokowanych w 3 centrach przetwarzania danych obejmujących zarówno serwery fizyczne, jak i wirtualne na których pracują systemy typu: HIS, LIS, RIS, ERP, oraz systemy niezbędne do utrzymania ciągłości działania podmiotu.

4) Zabezpieczenia wdrożone na styku sieci lokalnej LAN z siecią publiczną Internet;

5) Zastosowanych zabezpieczeń fizycznych, środowiskowych oraz zapewniających ciągłość dostaw i usług, od których zależy realizacja usługi kluczowej Zamawiającego;

3. Sposób realizacji prac

Wszystkie prace związane z realizacją zamówienia wykonywane będą w sposób następujący:

1) Audyt, o którym mowa w pkt.2 ppkt. a), opierać się będzie na wizji lokalnej przeprowadzonej przez wskazane przez Wykonawcę osoby w lokalizacji Zamawiającego. Ponadto analiza oparta będzie o wywiad i oświadczenia wskazanych przez Zamawiającego osób. Opracowanie końcowej dokumentacji, wykonane zostanie w siedzibie Wykonawcy;

2) Audyt będzie prowadzony na poziomie trzech warstw: metodologicznej, organizacyjnej, dokumentacyjnej;

3) Zamawiający wymaga, aby przedmiotowa analiza i ocena cyberbezpieczeństwa realizowana była w oparciu o obowiązującą normę PN ISO/IEC 27001

Audyt bezpieczeństwa, o którym mowa może być przeprowadzony przez:

1) jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2022 r. poz. 5), w zakresie właściwym do podejmowanych ocen bezpieczeństwa systemów informacyjnych;

2) co najmniej dwóch audytorów posiadających:
   a) certyfikaty określone w poniższym wykazie certyfikatów uprawiających do przeprowadzenia audytu (każdy z audytorów powinien posiadać przynajmniej po

jednym z wymienionych certyfikatów) lub

b) co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych, lub
c) co najmniej dwuletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych i legitymujących się dyplomem ukończenia studiów podyplomowych w zakresie audytu bezpieczeństwa systemów informacyjnych, wydanym przez jednostkę organizacyjną, która w dniu wydania dyplomu była uprawniona, zgodnie z odrębnymi przepisami, do nadawania stopnia naukowego doktora nauk ekonomicznych, technicznych lub prawnych.

Wykaz certyfikatów uprawniających do przeprowadzenia audytu:

1) Certified Internal Auditor (CIA);
2) Certified Information System Auditor (CISA);
3) Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami *ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku,* w zakresie certyfikacji osób;
4) Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami *ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku*, w zakresie certyfikacji osób;
5) Certified Information Security Manager (CISM);
6) Certified in Risk and Information Systems Control (CRISC);
7) Certified in the Governance of Enterprise IT (CGEIT);
8) Certified Information Systems Security Professional (CISSP);
9) Systems Security Certified Practitioner (SSCP);
10) Certified Reliability Professional;
11) Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert

4. Oczekiwany produkt finalny.

Zamawiający wymaga, aby produkt finalny stanowiła ocena systemu bezpieczeństwa cybernetycznego Zamawiającego zgodnie z Ustawą, obejmująca:

1) Opracowanie raportu przeprowadzonej analizy zgodnie z metodyką ISO 27001, w tym:

    a. określenie niezgodności,

    b. dla zgodności określenie potencjału do doskonalenia i opracowanie rekomendacji dotyczących wdrożenia wymaganych ustawą zabezpieczeń organizacyjnych i technicznych

2) Wytyczne, rekomendacje oraz opisy techniczne rozwiązań (wraz z szacunkową wyceną) dotyczące sposobu wdrożenia odpowiednich, do oszacowanego ryzyka, środków technicznych i organizacyjnych, w tym utrzymania i bezpiecznej eksploatacji systemu informacyjnego;