#### OPIS PRZEDMIOTU ZAMÓWIENIA

1. Wsparcie w zakresie utrzymania infrastruktury sieciowej FRSE.

2. Opis usług wchodzących w zakres utrzymania infrastruktury sieciowej FRSE:

a) W przypadku stwierdzenia problemów w sieci Zamawiający będzie miał możliwość kontaktu z inżynierem dyżurnym Wykonawcy w trybie 24 godziny / 7 dni w tygodniu. Czas reakcji (potwierdzenie przyjęcia zgłoszenia) będzie nie dłuższy niż 4 godz. od chwili wysłania zgłoszenia przez Zamawiającego. Zgłoszenia będą przesyłane przez odpowiednio ustalone z Zamawiającym kanały komunikacji (telefon, e-mail, WeChat, Whatsapp). Czas reakcji może być dłuższy jeśli strony postanowią inaczej.

b) Wykonawca będzie wykonywał optymalizację konfiguracji urządzeń sieciowych Zamawiającego zmierzającą do minimalizacji skutków potencjalnych niebezpieczeństw/problemów/awarii. Zoptymalizowanie konfiguracji będzie miało na celu zwiększenie niezawodności sieci komputerowej pod kątem pojawienia się nieoczekiwanych awarii.

c) Wykonawca przeprowadzi cykliczne kontrole polityk bezpieczeństwa realizowanych przez firewall’e. Kontrola będzie miała na celu minimalizację pojawienia się ruchu niepożądanego pomiędzy segmentami sieci komputerowej Zamawiającego.

d) Wykonawca będzie wykonywał cykliczną kontrolę mechanizmów UTM (Antywirusa, Ochrony przed atakami – IPS, Filtra URL, Content Filteringu, deszyfracji SSL, Mail Filteringu, Data Filteringu, Application Behavior Control). Kontrola będzie realizowana na firewall’ach i będzie miała na celu możliwie jak najdokładniejsze zabezpieczenie ruchu Zamawiającego.

e) Wykonawca przeprowadzi cykliczną kontrolę konfiguracji urządzeń sieciowych pod kątem badania ustawień mechanizmów ochrony na przełącznikach sieciowych – DAI (dynamic arp inspection), DHCP Snooping, MFF (mac forced forwarding). Kontrola będzie miała na celu zabezpieczenie przed rozprzestrzenianiem się zagrożeń w ramach tego samego segmentu sieci komputerowej Zamawiającego.

f) W przypadku stwierdzenia problemów w sieci Zamawiającego, Wykonawca dokona zdarzeniowej kontroli urządzeń wytypowanych jako problematyczne. Kontrola będzie miała na celu zweryfikowanie poprawnego działania zastosowanych mechanizmów bezpieczeństwa oraz wykrycie przyczyny zaistniałego problemu. Wykonawca przedstawi raport z wykrytego problemu.

g) Wykonawca przeprowadzi aktualizację urządzeń sieciowych Zamawiającego do wersji oprogramowania rekomendowanej przez producenta urządzeń. Aktualizacją oprogramowania będą objęte tylko te urządzenia, które w danym momencie będą znajdowały się na gwarancji producenta. Aktualizacja będzie wykonywana raz na kwartał o ile odpowiednie oprogramowanie będzie udostępnione przez producenta i przetestowane przez Wykonawcę. Aktualizacja oprogramowania może także być wykonana przez Wykonawcę, nie później niż w kolejnym dniu roboczym, po zaistnieniu i zgłoszeniu sytuacji, w której na skutek wykrytej luki w oprogramowaniu lub problemu z działaniem funkcjonalności producent rozwiązania zarekomenduje aktualizację oprogramowania.

h) Wykonawca będzie proaktywnie monitorował urządzenia Zamawiającego. Proaktywny monitoring będzie miał na celu wykrywanie potencjalnych nieprawidłowości w zabezpieczeniach komponentów sieciowych Zamawiającego. W przypadku możliwości pojawienia się nieprawidłowości Wykonawca wskaże Zamawiającemu potencjalnie niebezpieczne obszary w sieci komputerowej oraz przedstawi propozycję ich zabezpieczenia.

i) Wykonawca będzie wykonywał kontrolę i proaktywny monitoring dostępu do sieci Zamawiającego przez pracowników będących poza biurem i chcących się połączyć, przez sieć Internet, z wewnętrznymi zasobami Zamawiającego.

j) Na polecenie Zamawiającego, w przypadku, gdy dostawca usługi dostępu do Internetu nie jest w stanie wywiązać się z jakościowych parametrów opisanych w warunkach umowy pomiędzy Zamawiającym a Dostawcą Internetu (ISP), wykonawca będzie w stanie wesprzeć i koordynować komunikację z dostawcą usługi dostępu do Internetu w celu rozwiązania problemu.

k) Wykonawca będzie wspierał i doradzał Zamawiającemu w zakresie projektowania, „know-how” i najlepszych praktyk sieciowych. Wsparcie Wykonawcy będzie ukierunkowane na rozwój i wdrażanie nowych funkcjonalności, aplikacji oraz mechanizmów związanych z bezpieczeństwem sieci komputerowej.

l) Wykonawca będzie wykonywał monitoring komponentów sieciowych w trybie 24 godziny / 7 dni w tygodniu, przy wykorzystaniu protokołów monitoringu takich jak SNMP i ICMP, oraz przedstawi raporty z wykrycia zagrożeń, bądź nieprawidłowości.

m) Inżynier Wykonawcy podejmie działania w przypadku gdy monitorowane urządzenia Zamawiającego wyślą informację w postaci wiadomości SNMP Trap, wyzwalaną na okoliczność wystąpienia incydentu bezpieczeństwa. Wysyłane incydenty bezpieczeństwa będą związane z następującymi mechanizmami bezpieczeństwa IPS, AV, URL Filtering.

n) W przypadku awarii urządzeń sieciowych Zamawiającego (Access Point , przełącznik sieciowy, UTM etc) do czasu wymiany przez producenta sprzętu na nowy, Wykonawca zobowiązuje się do wypożyczenia skonfigurowanego ww. sprzętu nieodpłatnie.

o) Wykonawca jest zobowiązany dysponować co najmniej dwiema osobami zdolnymi do wykonania zamówienia, które będą uczestniczyć w realizacji Zamówienia, posiadającymi certyfikat z poziomu HCIE Routing&Switching - dla urządzeń sieciowych. Zamawiający zastrzega sobie prawo do weryfikacji posiadania i autentyczności wspomnianych certyfikatów oraz aktywnego uczestnictwa osób posiadających wspomniane certyfikaty w zakresie realizacji usług wchodzących w zakres niniejszego zapytania.

1. Miejsce realizacji zamówienia: Warszawa West Station, Al. Jerozolimskie 142A,.
2. Czas realizacji zamówienia: od dnia zawarcia umowy do 31 grudnia 2022 r.
3. Osoba do kontaktu: Wojciech Boryna [wboryna@fres.org.pl](mailto:wboryna@fres.org.pl) +48 573 441 883

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |