Załącznik Nr 8 do SWZ
Znak sprawy: IZiG.271.7.2024

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA
„Systemu Bezpieczeństwa Aktywnego wraz z instalacją i konfiguracją"
do projektu grantowego „Cyberbezpieczny Samorząd" pt. „Kompleksowe wzmacnianie bezpieczeństwa informacji w Gminie Sulęcin ze szczególnym uwzględnieniem systemów w Urzędzie Miejskim w Sulęcinie"

Cześć 1. ZAKRES SPRZĘTOWO-PROGRAMOWY:

Rozdział I. SYSTEM OCHRONY BRZEGOWEJ SIECI

1. **Wymagania Ogólne**: System ochrony brzegowej sieci realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu ochrony brzegowej sieci mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. Dla wszystkich funkcji systemu ochrony brzegowej sieci musi być dostarczony dokument potwierdzony przez producenta lub autoryzowanego dystrybutora o gotowości świadczenia usług wsparcia w języku polskim oraz bezpłatnej obsługi procesu wymiany uszkodzonego urządzenia. System ochrony brzegowej sieci realizując funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. System ochrony brzegowej sieci umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej czterech administratorów do poszczególnych instancji systemu. System wspiera protokoły IPv4 oraz IPv6 w zakresie:
   - Firewall.
   - Ochrony w warstwie aplikacji.
   - Protokołów routingu dynamicznego.
2. **Kompatybilność:** System ochrony brzegowej sieci musi być kompatybilny z dostarczonymi systemami tj.
   2.1. SYSTEMEM OCHRONY POCZTY opisanym w rozdziale II.
   2.2. SYSTEMEM ANTYWIRUSOWYM opisanym w rozdziale III.
3. **Ilość urządzeń:** 10 szt.
4. **Parametry fizyczne systemu brzegowej sieci:**
   4.1. System musi być wyposażony w interfejsy:
      4.1.1. min. 4 szt. porty Gigabit Ethernet RJ-45 dla sieci LAN
      4.1.2. min 1 szt. porty Gigabit Ethernet RJ-45 dla sieci WAN
   4.2. wysokość nie więcej niż 1U
   4.3. Zasilanie z sieci 230V/50Hz.
   4.4. Nie dopuszcza się rozwiązań wirtualnych

5. **Redundancja, monitoring i wykrywanie awarii.**
   5.1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
   5.2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
   5.3. Monitoring stanu realizowanych połączeń VPN.
   5.4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.
6. **Interfejsy, Dysk, Zasilanie:**
   6.1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą 5 szt. portów Gigabit Ethernet z interfejsem RJ-45.
   6.2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
   6.3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
   6.4. System jest wyposażony w zasilanie AC.
7. **Parametry wydajnościowe:**
   7.1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę.
   7.2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B.
   7.3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps.
   7.4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 4 Gbps.
   7.5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1 Gbps.
   7.6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 500 Mbps.
   7.7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.
8. **Funkcje Systemu Bezpieczeństwa:** W ramach systemu ochrony brzegowej sieci są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:
   8.1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
   8.2. Kontrola Aplikacji.
   8.3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
   8.4. Ochrona przed malware.
   8.5. Ochrona przed atakami - Intrusion Prevention System.
   8.6. Kontrola stron WWW.
   8.7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
   8.8. Zarządzanie pasmem (QoS, Traffic shaping).
   8.9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
   8.10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.

8.11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.

8.12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.

8.13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

9. Polityki, Firewall:

9.1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.

9.2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:

9.2.1. Translację jeden do jeden oraz jeden do wielu.

9.2.2. Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

9.3. W ramach systemu ochrony brzegowej sieci istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

9.4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.

9.5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.

9.6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.

9.7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu:

9.7.1. Amazon Web Services (AWS).

9.7.2. Microsoft Azure.

9.7.3. Cisco ACI.

9.7.4. Google Cloud Platform (GCP).

9.7.5. OpenStack.

9.7.6. VMware NSX.

9.7.7. Kubernetes.

10. Połączenia VPN

10.1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:

10.1.1. Wsparcie dla IKE v1 oraz v2.

10.1.2. Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).

10.1.3. Obsługa protokołu Diffie-Hellman grup 19, 20.

10.1.4. Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.

10.1.5. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.

10.1.6. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.

10.1.7. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.

10.1.8. Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.

10.1.9. Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.

10.1.10. Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.

10.1.11. Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.

10.1.12. Mechanizm „Split tunneling" dla połączeń Client-to-Site.

10.2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:

10.2.1. Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.

10.2.2. Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.

10.2.3. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń SSL VPN oraz IPSec VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

11. **Routing i obsługa łączy Internetowych WAN.** W zakresie routingu rozwiązanie zapewnia obsługę:

11.1. Routingu statycznego.

11.2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).

11.3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.

11.4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.

11.5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.

11.6. BFD (Bidirectional Forwarding Detection).

11.7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

12. **Funkcje SD-WAN.**

12.1. System ochrony brzegowej sieci umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.

12.2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

13. Zarządzanie pasmem

13.1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.

13.2. System daje możliwość określania pasma dla poszczególnych aplikacji.

13.3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.

13.4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

14. Ochrona przed malware:

14.1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).

14.2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.

14.3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.

14.4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.

14.5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).

14.6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

14.7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.

14.8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.

14.9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

14.10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

15. Ochrona przed atakami:

15.1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.

15.2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.

15.3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

15.4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.

15.5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.

15.6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).

15.7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.

15.8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

15.9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

16. Kontrola aplikacji:

16.1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.

16.2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

16.3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.

16.4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.

16.5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.

16.6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).

16.7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

17. Kontrola WWW:

17.1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.

17.2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.

17.3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.

17.4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.

17.5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).

17.6. Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.

17.7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.

17.8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.

17.9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

18. Uwierzytelnianie użytkowników w ramach sesji:

18.1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:

18.1.1. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.

18.1.2. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.

18.1.3. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

18.2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.

18.3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.

18.4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

19. Zarządzanie:

19.1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.

19.2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.

19.3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego.

19.4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.

19.5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.

19.6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

19.7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

19.8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).

19.9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

20. Logowanie:

20.1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.

20.2. W przypadku, kiedy usługa logowania i raportowania realizowana jest w chmurze, wymagane są stosowne licencje upoważniające do składowania logów przez okres co najmniej jednego roku.

20.3. W przypadku, kiedy usługa logowania, raportowania, korelacji zdarzeń realizowana jest w chmurze, wykonawca musi dostarczyć stosowne licencje upoważniające do składowania logów przez okres co najmniej jednego roku.

20.4. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.

20.5. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.

20.6. Możliwość włączenia logowania per reguła w polityce firewall.

20.7. System zapewnia możliwość logowania do serwera SYSLOG.

20.8. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

21. Testy wydajnościowe oraz funkcjonalne: Wszystkie funkcje i parametry wydajnościowe systemu ochrony brzegowej sieci mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.

22. Serwisy i licencje. Jeżeli do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje to należy dołączyć dokument potwierdzający to prawo **na okres 24 miesięcy wraz dostawą przedmiotu umowy.** Zakres funkcjonalny serwisów:

22.1. Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen.

22.2. Logowanie i raportowanie w oparciu o usługę realizowaną w chmurze, z czasem retencji logów minimum 1 rok.

23. Opisy do wymagań ogólnych – dokumenty będą wymagane przed podpisaniem umowy zgodnie z zapisami we wzorze umowy w §3 ust.3 pkt 2 i 3

23.1. Wymaga się, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U.2023.1582 teks jednolity).

23.2. Wymaga się, aby został uzyskany dokument - oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym.

Rozdział II. SYSTEM OCHRONY POCZTY

1. **Wymagania ogólne:** System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware'ową bez limitu licencyjnego na ilość chronionych kont użytkowników. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o komercyjne bazy zabezpieczeń. Dostarczone rozwiązanie musi mieć możliwość pracy w każdym trybów:
   1.1. Tryb Gateway.
   1.2. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej).
2. **Kompatybilność**: System ochrony poczty musi być kompatybilny z dostarczonymi systemami tj.
   2.1. SYSTEMEM OCHRONY BRZEGOWEJ SIECI opisanym w rozdziale I.
   2.2. SYSTEMEM ANTYWIRUSOWYM opisanym w rozdziale III.
3. **Ilość urządzeń/rozwiązań:** 1 szt. / 1 komplet.
4. **Parametry fizyczne systemu ochrony poczty:**
   4.1. System musi być wyposażony w interfejsy min. 4 szt. porty Gigabit Ethernet RJ-45.
   4.2. System musi być wyposażony w lokalną przestrzeń dyskową o pojemności minimum 1TB.
   4.3. System musi posiadać wbudowany port konsoli szeregowej.
   4.4. Zasilanie z sieci 230V/50Hz.
   4.5. Obudowa do instalacji w szafie rack 19 cali, wysokość nie więcej niż 1U
   4.6. Nie dopuszcza się rozwiązań wirtualnych
5. **Ogólne funkcje systemu ochrony poczty.** Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje:
   5.1. Wsparcie dla co najmniej 20 domen pocztowych.
   5.2. System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 28 tys. wiadomości/godzinę.
   5.3. Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all).
   5.4. Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP.
   5.5. Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości).
   5.6. Możliwość ograniczenia ilości poczty wychodzącej do chronionych domen w oparciu o nie mniej niż: ilość jednoczesnych sesji, maksymalną liczbę wiadomości w ramach sesji, maksymalną liczbę odbiorców w zadanym czasie.
   5.7. Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej.
   5.8. Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów.
   5.9. Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP.
   5.10. Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika.

5.11. Możliwość poddania ponownemu skanowaniu (antywirus, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora.
5.12. Dostęp do kwarantanny użytkownika możliwy poprzez WebMail.
5.13. Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki.
5.14. Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI.
5.15. Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu.
5.16. Białe i czarne listy adresów mailowych dla poszczególnych użytkowników.
5.17. Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika.

6. **Kontrola antywirusowa i ochrona przed malware:** W tym zakresie dostarczony system ochrony poczty musi zapewniać:
6.1. Skanowanie antywirusowe wiadomości SMTP.
6.2. Kwarantannę dla zainfekowanych plików.
6.3. Skanowanie załączników skompresowanych.
6.4. Definiowanie komunikatów powiadomień w języku polskim.
6.5. Blokowanie załączników w oparciu o typ pliku.
6.6. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antywirusowej.
6.7. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu.
6.8. Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.
6.9. Ochronę typu wirus outbrake.

7. **Kontrola antyspamowa:** System musi zapewniać poniższe funkcje i metody filtrowania spamu:
7.1. Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta.
7.2. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania.
7.3. Szczegółowa kontrola nagłówka wiadomości.
7.4. Analiza Heurystyczna.
7.5. Współpraca z zewnętrznymi serwerami RBL, SURBL.
7.6. Filtrowanie w oparciu o filtry Bayes'a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen.
7.7. Możliwością dostrajania filtrów Bayes'a przez poszczególnych użytkowników.
7.8. Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF.
7.9. Kontrola w oparciu o Greylisting oraz SPF.
7.10. Filtrowanie treści wiadomości i załączników.
7.11. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości.
7.12. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antyspamowej.

7.13. Ochrona typu outbrake.
7.14. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).
7.15. Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.

8. **Ochrona przed atakami na usługę poczty:** System musi zapewniać poniższe funkcje i metody filtrowania:
   8.1. Ochrona przed atakami na adres odbiorcy (m.in. email bombing).
   8.2. Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.
   8.3. Definiowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu.
   8.4. Kontrola Reverse DNS (ochrona przed Anty-Spoofing).
   8.5. Weryfikacja poprawności adresu e-mail nadawcy.
9. **Funkcje logowania i raportowania.** W tym zakresie dostarczony system ochrony poczty musi zapewniać:
   9.1. Logowanie do zewnętrznego serwera SYSLOG.
   9.2. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku.
   9.3. Logowanie informacji na temat spamu oraz niedozwolonych załączników.
   9.4. Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych.
   9.5. Możliwość analizy przebiegu sesji SMTP.
   9.6. Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych.
   9.7. Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu.
   9.8. Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.
10. **Funkcje pracy w trybie wysokiej dostępności (HA).** System ochrony poczty musi zapewniać poniższe funkcje:
    10.1. Konfigurację HA w każdym z trybów: gateway, transparent.
    10.2. Tryb synchronizacji konfiguracji dla scenariuszy, gdy każde z urządzeń występuje pod innym adresem IP.
    10.3. Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu.
    10.4. Monitorowanie stanu pracy klastra.
11. **Aktualizacje sygnatur, dostęp do bazy spamu**. W tym zakresie dostarczony system ochrony poczty musi zapewniać:
    11.1. Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym.
    11.2. Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.
12. **Zarządzanie.** System ochrony poczty musi zapewniać poniższe funkcje:
    12.1. System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH.
    12.2. Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy.
    12.3. Powinna istnieć możliwość zdefiniowania co najmniej 3 lokalnych kont administracyjnych.
13. **Certyfikaty.** Dostarczony system powinien posiadać co najmniej dwie z poniższych certyfikacji.
    13.1. VBSpam
    13.2. VB100 rated
    13.3. Common Criteria NDPP

13.4. FIPS 140-2 Certified.

14. **Gwarancja oraz wsparcie.** System ochrony poczty musi być objęty serwisem gwarancyjnym producenta przez okres 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
15. **Opisy do wymagań ogólnych - dokumenty będą wymagane przed podpisaniem umowy zgodnie z zapisami we wzorze umowy w §3 ust.3 pkt 2 i 3**
    15.1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.).
    15.2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

Rozdział III. SYSTEM OCHRONY ANTYWIRUSOWEJ

1. **Wymagania Ogólne**: System ochrony antywirusowej jest przeznaczony dla Urzędu Miejskiego oraz wybranych komputerów jednostek podległych do ochrony systemów w części administracyjnej tych jednostek.
2. **Kompatybilność**: System ochrony antywirusowej musi być kompatybilny z dostarczonymi systemami tj.
    2.1. SYSTEMEM OCHRONY BRZEGOWEJ SIECI opisanym w rozdziale I.
    2.2. SYSTEMEM OCHRONY POCZTY opisanym w rozdziale II.
    Nie może w żaden sposób kolidować z w/w systemami oraz nie może wymagać dodatkowych rozwiązań firm trzecich zapewniających wymaganą kompatybilność.
3. **Ilość licencji:** 250 szt. bez limitu podziału na systemy Windows czy Android, w tym co najmniej 20% licencji do stosowania na serwerowych systemach operacyjnych Windows lub Linux.
4. **Wymagania funkcjonalne:**
    4.1. Rozwiązanie musi wspierać instalację na systemach Windows Server (od 2012 R2), Linux oraz w postaci maszyny wirtualnej w formacie OVA lub dysku wirtualnego w formacie VHD.
    4.2. Rozwiązanie musi zapewniać instalację z użyciem bazy danych MS SQL i MySQL.
    4.3. Rozwiązanie musi zapewniać pobranie wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta.
    4.4. Rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania w języku polskim z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL.
    4.5. Rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi modułami serwera za pomocą certyfikatów.
    4.6. Rozwiązanie musi zapewniać utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi.

4.7. Rozwiązanie musi zapewniać centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, antyspyware, które działają na stacjach roboczych w sieci.
4.8. Rozwiązanie musi zapewniać weryfikację podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe).
4.9. Rozwiązanie musi zapewniać instalowanie i odinstalowywanie oprogramowania firm trzecich dla systemów Windows oraz odinstalowywanie oprogramowania zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT.
4.10. Rozwiązanie musi zapewniać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
4.11. Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
4.12. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
4.13. Rozwiązanie musi zapewniać korzystanie z minimum 100 szablonów raportów, przygotowanych przez producenta oraz musi zapewniać tworzenie własnych raportów przez administratora.
4.14. Rozwiązanie musi zapewniać wysłanie powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog
4.15. Rozwiązanie musi zapewniać podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.

5. Ochrona stacji roboczych:

5.1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11)
5.2. Rozwiązanie musi wspierać architekturę ARM64.
5.3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
5.4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
5.5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
5.6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
5.7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
5.8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
5.9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
5.10. Rozwiązanie musi integrować się z Intel Threat Detection Technology.

5.11. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).

5.12. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.

5.13. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

5.14. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.

5.15. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.

5.16. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:

5.16.1. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,

5.16.2. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,

5.16.3. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,

5.16.4. tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,

5.16.5. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.

5.17. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.

5.18. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.

5.19. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.

5.20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).

5.21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.

5.22. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.

5.23. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:

5.23.1. tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,

5.23.2. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,

5.23.3. tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,

5.23.4. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.

5.24. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.

5.25. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.

5.26. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.

5.27. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.

5.28. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.

5.29. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.

5.30. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

6. Ochrona serwerów:

6.1. Rozwiązanie musi wspierać co najmniej systemy Microsoft Windows Server 2012 R2 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7,8 i 9, CentOS 7, Ubuntu Server 18.04 LTS i tym co najmniej: RedHat Enterprise Linux (RHEL) 7,8 i 9, CentOS 7, Ubuntu Server 18.04 LTS i nowsze, Debian 10, Debian 11 i Debian 12, SUSE Linux Enterprise Server (SLEnowsze, Debian 10, Debian 11 i Debian 12, SUSE Linux Enterprise Server (SLES) 15, Oracle S) 15, Oracle Linux 8 oraz Amazon Linux.Linux 8 oraz Amazon Linux.

6.2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.

6.3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.

6.4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.

6.5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

6.6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.

6.7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.

6.8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

7. Dodatkowe wymagania dla ochrony serwerów rodziny Windows:

7.1. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.

7.2. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).

7.3. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.

7.4. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.

7.5. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.

7.6. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.

7.7. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.

7.8. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.

7.9. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

8. Dodatkowe wymagania dla ochrony serwerów z rodziny Linux:

8.1. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.

8.2. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.

8.3. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.

8.4. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.

9. Szyfrowanie:

9.1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 10/11 64-bit.

9.2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).

9.3. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.

9.4. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.

10. Ochrona urządzeń mobilnych opartych o system Android:

10.1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.

10.2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.

10.3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).

10.4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.

10.5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:

10.5.1. usunięcie zawartości urządzenia,

10.5.2. przywrócenie urządzenie do ustawień fabrycznych,

10.5.3. zablokowania urządzenia,

10.5.4. uruchomienie sygnału dźwiękowego,
10.5.5. lokalizację GPS.
10.6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
10.7. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:
10.7.1. nazwę aplikacji,
10.7.2. nazwę pakietu,
10.7.3. kategorię sklepu Google Play,
10.7.4. uprawnienia aplikacji,
10.7.5. pochodzenie aplikacji z nieznanego źródła.

11. Sandbox w chmurze:

11.1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
11.2. Rozwiązanie musi wykorzystywać do działania chmurę producenta.
11.3. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
11.4. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
11.5. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
11.6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
11.7. Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów.
11.8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.
11.9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
11.10. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.
11.11. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo.
11.12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem:
11.12.1. Czysty (lub inne zamienne określenie)
11.12.2. Podejrzany (lub inne zamienne określenie)
11.12.3. Bardzo podejrzany (lub inne zamienne określenie)
11.12.4. Szkodliwy (lub inne zamienne określenie)
11.13. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
11.14. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.
11.15. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.

12. Moduł EDR/XDR:

12.1. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.

12.2. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.

12.3. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.

12.4. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.

12.5. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica".

12.6. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.

12.7. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.

12.8. Serwer musi posiadać ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta.

12.9. Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej.

12.10. Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku.

12.11. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.

12.12. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.

12.13. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.

12.14. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.

12.15. Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich.

12.16. Konsola administracyjna musi mieć możliwość tagowania obiektów.

12.17. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.

Cześć 2. ZAKRES ZADANIOWY:

Rozdział IV. DOSTAWA:

Do czynności Wykonawcy w ramach **dostawy** przedmiotu zamówienia należy:

1. Uzgodnienie z Zamawiającym terminu dostawy sprzętu/rozwiązania i licencji:
2. Rozpakowanie urządzeń oraz elementów dodatkowych, sprawdzenie, czy nie wystąpiły uszkodzenia
3. Zebranie wszystkich opakowań i oddanie ich do dyspozycji Zamawiającego
4. Weryfikacja czasu gwarancji i typu gwarancji na podstawie numerów seryjnych urządzeń
5. Weryfikacja ilości licencji i typy licencji
6. Podpisanie obustronnie **protokołu dostawy**, który jest podstawą do realizacji zadań z rozdziału V. INSTALACJA.

Rozdział V. INSTALACJA:

Do czynności Wykonawcy w ramach **instalacji** przedmiotu zamówienia należy:

1. Uzgodnienie z Zamawiającym terminu instalacji sprzętu/rozwiązania i oprogramowania
2. Uruchomienie wszystkich urządzeń i rozwiązań
3. Instalację oprogramowania wchodzącego w skład systemu ochrony antywirusowej na wskazanych przez Zamawiającego systemach operacyjnych stacji roboczych i serwerów. Ilość 250 licencji jest z pewnym zapasem w stosunku do ilości systemów operacyjnych.
4. Wykonanie testów poprawności działania
5. Podpisanie obustronnie **protokołu instalacji**, który jest podstawą do realizacji zadań z rozdziału VI. KONFIGURACJA

Rozdział VI KONFIGURACJA:

Do czynności Wykonawcy w ramach **konfiguracji** przedmiotu zamówienia należy:

1. Uzgodnienie z Zamawiającym terminu konfiguracji systemów dostarczonych w ramach przedmiotu zamówienia
2. **Konfiguracja systemu ochrony brzegowej sieci:**
   - 2.1. W ramach postępowania ma zostać dostarczone 10 szt. urządzeń. Dla dziewięciu z nich ma być dostarczona usługa **dedykowana do oferowanego rozwiązania** umożliwiająca przeniesienie konfiguracji z obecnie użytkowanych urządzeń FortiGate model 30E na oferowane urządzenia. Pozostałe, dziesiąte urządzenie będzie uruchamiane jako nowe, co oznacza implementację konfiguracji funkcjonalnie tożsamej jak w pozostałych urządzeniach. Wymaga się, aby przeniesienie konfiguracji z obecnie użytkowanych urządzeń FortiGate na nowe dostarczone w ramach postepowania w momencie wymiany tych urządzeń nie spowodowało przerwy w pracy większej niż dwie godziny.
   - 2.2. Konfiguracja urządzeń winna zawierać tożsame ustawienia jakie posiadają aktualnie wykorzystywane rozwiązania tj. urządzenia FortiGate model 30E, a ochrona brzegowa sieci powinna zostać co najmniej na tym samym poziomie.
   - 2.3. Wykonanie testów poprawności działania każdego z urządzeń
3. **Konfiguracja systemu ochrony poczty:**
   - 3.1. Konfigurację rozwiązania należy wykonać dla trybu Gateway wraz ze wsparciem administratorów Zamawiającego przy konfiguracji usług pocztowych hostowanych w NetArt Group (nazwa.pl)

3.2. Wykonanie testów poprawności działania rozwiązania.

4. **Konfiguracja systemu ochrony antywirusowej:**
   4.1. Konfiguracja oprogramowania dostarczonego w ramach systemu ochrony antywirusowej winna zawierać niezbędne dodatkowe polityki bezpieczeństwa, tożsame do aktualnych w celu zapewnienia ochrony co najmniej na tym samym poziomie.
   4.2. Wykaz i opis polityk, może zostać dostarczony dopiero po podpisaniu umowy z Wykonawcą.
5. Podpisanie obustronnie **protokołu konfiguracji**, który jest podstawą do realizacji zadań z rozdziału VII. SZKOLENIE.

Rozdział VII SZKOLENIE: Dla każdego z systemów opisanych w rozdziałach I, II i III tj. dla:

1. Systemu ochrony brzegowej sieci
2. Systemu ochrony poczty
3. Systemu antywirusowego

Należy wykonać szkolenia certyfikowane dla dwóch administratorów w ilości 6 godzin dla każdego systemu w zakresie niezbędnym do samodzielnego administrowania oferowanymi systemami. Forma szkolenia (stacjonarna lub online) do uzgodnienia z Zamawiającym. Po zakończeniu szkolenia wymagane są imienne certyfikaty dla każdego administratora z każdego odbytego szkolenia. Podpisanie obustronnie **protokołu szkoleń**.

Cześć 3. ROZLICZENIE

Podstawą do wystawienia faktury jest podpisanie obustronnie **protokołu końcowego** realizacji przedmiotu zamówienia, gdzie poszczególne protokoły wymienione w opisie zadań z rozdziałów V, VI i VII w cześć 2. „ZAKRES ZADANIOWY" będą stanowić załączniki do protokołu końcowego

Signature Not Verified
Dokument podpisany przez
DARIUSZ EJCHART
Data: 2024.03.19 07:05:34 CET