K-ZP.261.114.2023 Załącznik nr 2 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest dostarczenie i wdrożenie Platformy wsparcia bezpieczeństwa danych. Przedmiot zamówienia obejmuje wszelkie licencje, bazy danych, usługi, inne składniki – również niewymienione bezpośrednio – które są konieczne, aby wdrożony system bezpieczeństwa działał zgodnie z wymaganiami niniejszego postępowania. System bezpieczeństwa musi zawierać bazę wiedzy eksperckiej, która pozwoli ocenić poprawność zabezpieczeń, identyfikując efektywność zastosowanych mechanizmów sieciowych i lokalnych w stosunku do potencjalnych wektorów ataków. System musi być zbudowany w trybie wysokiej dostępności posiadając przynajmniej dwie aktywne instancje, zapewniając tym zwiększenie wydajności i przepustowości. System powinien zapewnić przepustowość na minimalnym poziomie 5,5Gbps w trybie maksymalnej ochrony.(zapora sieciowa, ips, kontrola aplikacji, ochrona przed złośliwym oprogramowaniem). System musi zapewniać ciągłość pracy w przypadku awarii jednej z instancji. Interfejs systemu bezpieczeństwa musi umożliwiać wyświetlanie i modyfikowanie szczegółowych informacji o każdym elemencie zaimplementowanego składnika infrastruktury teleinformatycznej oraz posiadać mechanizm definiowania dozwolonej komunikacji sieciowej. Dla zdarzeń zawierających adres IP interfejs musi umożliwiać wyświetlanie informacji o zasobach powiązanych z adresem.

Zaimplementowany system odpowiedzialny za bezpieczeństwo teleinformatyczne musi zawierać szczegółową dokumentację pozwalają administrować systemem. System w razie wykrycia incydentów o wysokim ryzyku materializacji zagrożenia natury technicznej (m.in. przełamanie zabezpieczeń, infekcja złośliwym oprogramowaniem) umożliwi automatyczne powiadamianie o incydencie wskazanych pracowników. System musi umożliwiać uwzględnianie danych zgromadzonych w elektronicznej dokumentacji infrastruktury teleinformatycznej w mechanizmach korelacji zdarzeń; wykryte zdarzenia będą priorytetyzowane w odniesieniu do ważności zasobów dla organizacji, które dotyczą np. wspomagania procesów. System musi umożliwiać korelację zdarzeń z anomaliami wykrywanymi w przepływach sieciowych oraz podatnościami pozyskanymi ze skanerów aplikacyjnych i bazy CVE. System musi umożliwiać określenie okna czasowego oraz warunków dla zdarzeń, które mają zostać poddane regułom korelacyjnym, bądź regułom wykonania. System musi umożliwiać wykorzystanie baz reputacyjnych w regułach bezpieczeństwa teleinformatycznego. System musi być wyposażony w graficzny interfejs prezentujący w formie wykresów dane statystyczne związane z procesem obsługi. System musi posiadać zestaw predefiniowanych scenariuszy obsługi. System musi pozwalać na tworzenie własnych scenariuszy obsługi. System musi pozwalać na przekazywanie aktywnych linków pomiędzy innymi zintegrowanymi systemami. System musi umożliwiać identyfikowanie kontekstu odbiegającego od normalnego zachowania użytkownika, korzystając z danych zewnętrznych Threat Intelligence, Active Directory. System musi umożliwiać archiwizację danych na zewnętrzne repozytoria. System musi umożliwiać współpracę z bazami danych MS SQL, My SQL, Oracle.

System musi umożliwiać kontrolę dostępu do oferowanych przez niego funkcjonalności w oparciu o zdefiniowane role. System musi dokonywać automatycznej integracji z usługą katalogową Microsoft Active Directory celem pobrania informacji o poświadczeniach i zasobach zarejestrowanych w domenie. System musi być dostępny z poziomu dedykowanego klienta aplikacji oraz za pomocą dowolnej przeglądarki internetowej. Szczegółowy zakres i wytyczne procesu wdrożenia systemu:

obszar analizy, zakładający przegląd organizacji wraz z podłączeniem i skonfigurowaniem mechanizmów szacowania ryzyka pod kątem kluczowych zasobów IT i procesów organizacji - obszar analizy ma na celu identyfikację potencjalnych zagrożeń oraz możliwych konsekwencji na jakie narażona jest organizacja – zakres musi zawierać kolejno: pracę z konsultantem, wytyczne dla Zamawiającego celem przygotowania środowiska do instalacji systemu, instalację systemu, zestawienie połączenia zdalnego, aktywację licencji, wstępną konfigurację, import ustawień z organizacji Zamawiającego w tym adresacji znaczących stref bezpieczeństwa wymaganych przez mechanizmy wykrywania (sieci serwerów, DMZ, LAN), przekierowanie logów z obecnych systemów Zamawiającego do nowego systemu, uruchomienie reguł wykrywania i reguł wykonywania zdarzeń, pasywną analizę transmisji sieciowej (ruch z/do serwerów, baz danych, poczty, kontrolerów), analizę podatności, zidentyfikowanie zagrożeń, rekomendacja zabezpieczeń, transfer wiedzy; obszar detekcji, zakładający podłączenie i konfigurację narzędzi odpowiedzialnych za wykrywanie zdarzeń i incydentów bezpieczeństwa w ramach zainstalowanych modułów - obszar detekcji ma na celu uruchomienie i dostrojenie mechanizmów wykrywania zagrożeń - zakres prac powinien uwzględniać kolejno: podłączenie (przekierowanie do systemu) źródeł zdarzeń i ich dalszą konfigurację, podłączenie zapór sieciowych, mechanizmów dedykowanych do wykrywania incydentów bezpieczeństwa, centralnego systemu reagowania na incydenty, w przypadku niestandardowych źródeł, muszą zostać przygotowane odpowiednie parsery, pozwalające na detekcję zgodną z wbudowanymi w system regułami korelacji, adaptację reguł profilowych pozwalających na dostosowanie zdarzeń do wskazanych zasobów, obserwacja i doprecyzowanie postępu w tym wykluczenie/dodanie nowych reguł zdarzeń użytkowników/hostów, dostrojenie systemu w tym reguł priorytetyzacji zdarzeń i incydentów mające na celu dopasowanie czułości systemu do możliwości operacyjnych organizacji; obszar reakcji, zakładający podłączenie i konfigurację mechanizmów wspomagających proces automatyzacji reakcji na wykryte zdarzenia - obszar reakcji ma na celu uruchomienie i dostrojenie mechanizmów automatyzacji w działaniach reagowania na wykryte zagrożenia bezpieczeństwa - zakres prac powinien uwzględniać kolejno: pracę z konsultantem (wprowadzenie do scenariuszy wbudowanych w systemie, analizę wymaganych zmian), konfigurację zespołów obsługi celem właściwej adresacji podatności oraz zdarzeń wymagających obsługi, konfigurację mechanizmów powiadamiania. System bezpieczeństwa musi posiadać uruchomioną usługę piaskownicy, która daje możliwość wstrzymania dostarczenia treści do czasu uzyskania weryfikacji. Systemy odpowiedzialne za bezpieczeństwo teleinformatyczne muszą realizować: - Dynamiczne filtrowanie pakietów poprzez aktywny monitoring połączeń sieciowych, a następnie blokowanie niechcianych pakietów lub przepuszczanie dozwolonych. Ta funkcjonalność musi działać w protokole UDP, filtracja musi odbywać się poprzez regułę wykrywania pakietów komunikacyjnych przez określony czas i badania zarówno pakietów przychodzących, jak i wychodzących. System śledzi pakiety wychodzące, które żądają określonego rodzaju pakietów przychodzących i zezwala na przechodzenie pakietów przychodzących, o ile stanowią one dokładną odpowiedź. System monitoruje wszystkie sesje i weryfikuje wszystkie pakiety. Na przykład system przechwytuje informacje o stanie i kontekście pakietu i porównuje je z dominującymi danymi sesji. Jeśli identyczny wpis już istnieje, pakiet może przejść przez system. Jeśli dopasowanie nie zostanie znalezione, pakiet musi przejść pewne kontrole zasad. W tym czasie, jeśli pakiet spełnia wymagania polityki, system zakłada, że jest to połączenie zastępcze i przechowuje dane sesji w odpowiednich tabelach. Następnie pozwala pakietowi przejść. Jeśli pakiet nie spełnia warunków polityki, jest odrzucany; - Funkcję serwera DNS oraz filtrowanie zapytań DNS lokalnie oraz w ruchu

przechodzącym przez system; - Inspekcję SSL/TLS dla http/2, smtp, ftp, pop3; - Dwuskładnikowe uwierzytelnianie sprzętowe polegające na generowaniu unikalnych kodów cyfrowych na dedykowanym urządzeniu odrębnym od centrali systemu oraz urządzenia typu telefon, autoryzujących połączenia VPN; - Mechanizm DLP, ochrona przed wyciekiem informacji; - Oznaczanie metodą określania priorytetów dla ruchu różnego typu pakietów w sieci w zależności od kodu zapisanego w polu pakietu IP, który umożliwia przypisywanie różnemu typowi ruchu w sieci różnych poziomów jakości usług; - Kontrolę pasma QoS oraz kształtowanie ruchu poprzez zarządzanie przepustowością i opóźnianie wybranych datagramów celem dostosowania do pożądanego profilu ruchu; - Ochronę poczty, z wykorzystaniem smtp oraz pop3, przed niechcianymi informacjami; - Weryfikowanie zawartości stron internetowych; - Ochronę przed malware; - Zarządzanie pasmem dla wybranych rodzajów stron internetowych; - Ochronę przed atakami w czasie rzeczywistym, poprzez analizę polegającą na defragmentacji, łączeniu pakietów w strumienie danych, analizie nagłówków pakietów oraz analizie protokołów aplikacyjnych lub polegającą na polegająca na wyszukiwaniu w pakietach ciągów danych charakterystycznych dla znanych ataków sieciowych; - Uruchamianie szyfrowanych wirtualnych sieci prywatnych, w których ochrona posiada kilka faz negocjowanych, przy czym jako pierwsze negocjowane są: algorytmy szyfrowania (DES, 3DES, AES 128 i 256 bit w trybie GCM), funkcje haszowania (MD5, SHA), rodzaj autentykacji (PSK, RSA), grupa 19, 20 Diffiego-Hellmana, czas ważności, następnie negocjowane są materiały do tworzenia kluczy i algorytmy do szyfrowania danych przesyłanych przez tunel; obsługa tych sieci prywatnych musi być zgodna ze standardami RFC2409 oraz RFC4306; - Monitorowanie tuneli vpn i stałe utrzymywanie ich aktywności; - Określenie pasma dla wybranego użytkownika bez względu na adres IP; - Uruchamianie połączeń miejsce-miejsce oraz klient-miejsce; definiowane protokoły statycznego i dynamicznego przekierowywania adresów pomiędzy sieciami dla tuneli; monitorowanie tunelu szyfrowanego, a w przypadku niedostępności automatyczne uruchomienie zapasowego połączenia; - Definiowanie statycznego przekierowywania adresów pomiędzy sieciami połączeń szerokopasmowych; - Analizę tras równoważnych dla przekierowywania adresów pomiędzy sieciami na zasadzie Equal cost multi-path; - Protokół używany do wykrywania błędów między dwoma urządzeniami sieciowymi połączonymi łączem, poprzez zapewnienie niskich narzutów na wykrywanie usterek nawet na nośnikach fizycznych, które nie obsługują wykrywania awarii jakiegokolwiek rodzaju, takich jak Ethernet, obwody wirtualne, tunele i MPLS Label Switched Paths, sesje w tym protokole muszą działać w trybie asynchronicznym (oba punkty końcowe okresowo wysyłają do siebie pakiety, jeśli pewna liczba tych pakietów nie zostanie odebrana, sesja kończy się) oraz w trybie na żądanie (pakiety nie są wymieniane po ustanowieniu sesji; zakłada się, że punkty końcowe mają inny sposób weryfikacji łączności między sobą); - Filtrowanie tras w protokołach dynamicznego przekierowywania adresów pomiędzy sieciami; - Monitoring adresu IP z danego interfejsu systemu, jeśli adresu nie ma, to system automatycznie usuwa go z tablicy przekierowywania adresów pomiędzy sieciami; - Type of Service w nagłówkach IP; - Reguły bazowego przekierowywania adresów pomiędzy sieciami polegające na wyborze trasy w zależności od adresu źródłowego; - Trasowanie dynamiczne z wykorzystaniem PIM, BGP, OSPF w wersji 3, RIP w wersji 2, RIPng; - Określanie maksymalnej i gwarantowanej ilości pasma oraz wskazanie priorytetu ruchu; - Określanie pasma dla konkretnej aplikacji; - Określenie ochrony malware dla wybranego zakresu ruchu oraz dla urządzeń mobilnych typu telefon; - Blokowanie i oznaczanie zasobów, które są zaszyfrowane, uszkodzone lub wykraczają poza zdefiniowaną ochronę przed szkodliwym oprogramowaniem; - sprawdzanie archiwów zagnieżdżonych z określeniem zakresu zagnieżdżeń, które będą

dekompresowane celem sprawdzenia, dotyczy zasobów zip, rar; - Mechanizm ochrony przed szkodliwym oprogramowanie musi działać na protokołach: http/s, ftp, pop3, imap, smtp, cifs, dwukierunkowy ftp również na portach niestandardowych; - Usuwanie wrażliwej treści plików docx, xlsx, pdf; - Dla połączeń szyfrowanych kapsułkowanie pakietów na protokół o niewielkim narzucie danych sterujących, nie więcej niż 8 bajtów, a następnie translację NAT; - Metodę podtrzymywania nieaktywnych sesji IKE zgodną z RFC3706; - Technikę dzięki której można zdefiniować które aplikacje i urządzenia mają kierować połączenie przez sieć VPN, a które z jej pominięciem; - Technikę dla szyfrowanych wirtualnych sieci prywatnych gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki z wykorzystaniem html5 oraz z wykorzystaniem dedykowanego oprogramowania, kiedy to można zdefiniować które aplikacje i urządzenia mają kierować połączenie przez sieć VPN, a które z jej pominięciem; - Translację adresów jeden do wielu oraz jeden do jeden oraz translację PAT; - Dla protokołu SIP musi istnieć dedykowana brama proxy aplikacji, która wykonuje translację adresów i portów, alokację zasobów, kontrolę odpowiedzi aplikacji oraz synchronizację danych i sterowanie ruchem, kontrolować inicjowanie sesji aplikacji i chronić serwery aplikacji, uniemożliwiając lub przerywając połączenia, gdy jest to konieczne, w celu zapewnienia bezpieczeństwa; - Korzystanie z zewnętrznych zasobów adresacji IP oraz kategorii stron internetowych przy tworzeniu polityki bezpieczeństwa; - Dla funkcji ochrony sieci szerokopasmowej musi być dostępny harmonogram włączania i wyłączania reguł ochrony; - Pełną zgodność z Amazon, Microsoft, Cisco, Google, OpenStack, Kubernetes, VMWare w zakresie budowania polityki kontroli dostępu; - Logowanie do aplikacji chmurowej lub komercyjnego systemu logowania, w ramach logowania przekazywane są dane o dozwolonym i blokowanym ruchu, aktywności użytkowników, kondycji systemu; logowanie musi obejmować wszystkie moduły sieciowe i bezpieczeństwa i umożliwiać wyłączenie dla danej reguły; - Dostęp do panelu administratora systemu musi być ograniczony wskazaniem określonego adresu IP oraz musi być podział ról administracyjnych, tak, aby dany administrator mógł zarządzać jedynie wybraną częścią systemu bez dostępu do obszarów zastrzeżonych; - Dostęp poprzez API z pełną dokumentacją wykorzystania; - Protokoły zarządzania zgodne z snmp 3; - W celu bezpiecznego uwierzytelniania użytkowników system musi prowadzić weryfikacje tożsamości poprzez: statyczne hasła i definicje użytkowników zapisane lokalnie oraz w bazie LDAP, zewnętrzne bazy danych z wykorzystaniem RADIUS, RSA, SSO w integracji z Microsoft AD, RADIUS, API, SYSLOG, dla ruchu http musi być dostępny protokół SAML; - Ochronę stron internetowych wykorzystując definiowane kategorie (po włączeniu dostęp będzie zabroniony) dynamic dns, proxy, phishing, malware; dodatkową możliwość dopisywania kategorii oraz konieczność wykonania akcji potwierdzającej przed otwarciem określonej strony; mechanizm blokowania niechcianych treści w wyszukiwarkach gogle, yahoo; wysyłanie definiowanych komunikatów zwrotnych do użytkownika dla akcji podejmowanych przez filtr stron internetowych; - Określanie dozwolonych protokołów na konkretnym porcie oraz zablokowanie pozostałych protokołów, chcących korzystać z tego portu; - Kontrolę czynności wykonywanych w aplikacjach Facebook, Google, Microsoft; - Blokowanie aplikacji na niestandardowych portach; - Dostęp do bazy sygnatur z kategoriami aplikacji proxy, p2p, których uruchamianie jest szczególnie istotne dla bezpieczeństwa; - Monitorowanie poprzez port SPAN; - Funkcję zapory sieciowej w trybie transparentnym oraz z techniką przesyłania ruchu sieciowego, która wiąże się ze zmianą źródłowych/docelowych adresów protokołu internetowego, numerów portów UDP, pakietów protokołu internetowego podczas ich przepływu, sum kontrolnych (zarówno w pakiecie protokołu internetowego, jak i w segmencie UDP); - Pełną aktywną, pasywną, klastrową

dwuinstancyjność fizyczną oraz logiczną, z synchronizacją sesji pomiędzy instancjami, (zarządzaną łącznie przez ośmiu administratorów) w obszarach: przekierowania ruchu sieciowego/internetowego, szyfrowanych połączeń wirtualnych sieci prywatnych, kontroli i prewencji przeciwko włamaniom, kontroli aplikacji; - Pełne wsparcie dla protokołów internetowych wersji 4 i 6 w obszarach: zapory sieciowej, ochrony warstwy aplikacji, protokołów dynamicznego przekierowywania ruchu sieciowego pomiędzy różnymi sieciami; - Monitoring i wykrywanie uszkodzenia elementów programowych systemów zabezpieczeń oraz łączy sieciowych oraz stanu realizowanych połączeń wirtualnych sieci prywatnych; - Konfigurację kilku fizycznych połączeń jako jedno w celu zwiększenia prędkości, z wykorzystaniem techniki, gdzie awaria jednego fizycznego połączenia zostaje rozpoznana nawet w przypadku kiedy przebiega ono przez konwerter mediów i przez co status połączenia pozostaje aktywny np. w porcie przełącznika oraz wszystkie urządzenia połączone tą techniką muszą potwierdzić prawidłową konfigurację; - Bezpośrednie przyłączenie różnych zewnętrznych urządzeń sieciowych poprzez integralne konektory miedziane w ilości szesnaście oraz optyczne w ilości dwanaście przy czym cztery z nich muszą gwarantować prędkość przesyłania większą niż gigabit na sekundę; - W przypadku instalacji systemu na jakimkolwiek urządzeniu zewnętrznym, musi być możliwość zarządzania z wykorzystaniem dedykowanego portu szeregowego; - Funkcję przywracania działania w przypadku utraty zasilania; - W przypadku instalacji systemu na jakimkolwiek urządzeniu zewnętrznym, urządzenie to musi mieć zasilanie nadmiarowe; - Przy włączonym zapisie logowania oraz włączonych usługach: zapory, kontroli i prewencji przed włamaniem, kontroli aplikacji, ochrony przed szkodliwym oprogramowaniem - przepustowość dla typowego jednoczesnego ruchu sieciowego: 3% youtube oraz twitter, 20% http, 5% ftp, 1% bazy danych Oracle, AOL oraz ssh, 6% Facebook, 11% osobno https, poczta Google oraz Yahoo, 8% Amazon - ma być nie mniej niż pięć gigabitów na sekundę dla kontroli i ochrony przed włamaniem, ponad trzy gigabity na sekundę dla zapory sieciowej, nie mniej niż trzy gigabity na sekundę dla ochrony przed zagrożeniami teleinformatycznymi; - Przepustowość ponad dwadzieścia sześć gigabitów na sekundę przy ochronie pakietów 1504 oraz 512 bajtowych; - Protokół sterowania transmisją z wydajnością nie mniej niż trzy miliony jednoczesnych sesji na sekundę przy zdolności nawiązywania ponad dwieście siedemdziesiąt pięć tysięcy nowych sesji na sekundę; - Szyfrowane połączenia wirtualnych sieci prywatnych muszą odbywać się z wydajnością nie mniej niż trzynaście gigabitów na sekundę dla pakietów 512 bajtowych; - Wydajność szyfrowanych protokołem SSL połączeń wirtualnych sieci prywatnych nie mniej niż dwa gigabity na sekundę, przy utrzymaniu ponad pięciuset jednoczesnych połączeń w trybie szyfrowania, gdzie oryginalny pakiet protokołu internetowego jest enkapsulowany i dodawany jest do niego nowy nagłówek tego protokołu; - Funkcję kontroli aplikacji z wydajnością trzynaście gigabitów na sekundę, przy zapewnieniu przesyłania ponad szesnastu milionów pakietów na sekundę; - Szyfrowanie połączeń sieci prywatnych z wykorzystaniem algorytmu SHA256 z wydajnością trzynaście gigabitów na sekundę przy pakietach 512 bajtowych; - Ochronę przed zagrożeniami na zasadzie: analizy anomalii w protokołach sieciowych chroniąc przed atakami DoS oraz DDoS; analizy zachowania aplikacji przeglądarkowych chroniąc przed atakami CSS, SQL, roboty, trojany, exploity; kontrolowania długości nagłówka, ilości parametrów adresów internetowych, ciasteczek; blokowania komunikacji C&C; włączania ochrony prewencyjnej tylko dla wybranych zakresów komunikacji sieciowej; - Pełną zgodność z jednym ze standardów: ANSA, CGF, SERV, FCC, BSMI, VCC, ICSA w zakresie obsługi działania: technik ochrony na styku internetu, szyfrowania protokołu internetowego, ochrony antywirusowej, zgodności z protokołem internetowym wersji 6, szyfrowania wirtualnych sieci prywatnych. Zasady wsparcia gwarancyjnego w powyższym

zakresie, udzielonego na przedmiot zamówienia: i) wykonawca zapewni fabryczne wsparcie wszystkich producentów, których składniki zostaną użyte do realizacji przedmiotu zamówienia; ii) wsparcie, o którym mowa powyżej, ma zapewnić bez ponoszenia dodatkowych kosztów aktualizację wszystkich komponentów składających się na realizację przedmiotu zamówienia; iii) wsparcie musi być zagwarantowane pisemnie na etapie składania ofert; iv) jeśli producentem systemu bezpieczeństwa jest wykonawca, to musi on mieć swoje regionalne przedstawicielstwo w Polsce i zadeklarować, że utrzyma je przez okres gwarancji; v) alternatywnie, jeśli producentem systemu bezpieczeństwa jest wykonawca, to musi wyznaczyć pełnomocnika, który będzie ponosił odpowiedzialność przez okres gwarancji, w przypadku niedostępności wykonawcy; vi) jeśli producentem systemu bezpieczeństwa nie jest wykonawca, to wsparcie o którym mowa powyżej, musi być zapewnione Zamawiającemu bezpośrednio od producenta, tzn. bez pośrednictwa wykonawcy, już na etapie dostarczenia przedmiotu zamówienia; vii) w przypadku problemu lub wątpliwości w działaniu dowolnego składnika wdrożonego systemu, producent systemu zobowiązuje się do pisemnej odpowiedzi serwisowej w czasie 2 godzin, zaś w przypadku usterki – w czasie 15 minut, w tym celu producent systemu lub wykonawca (w porozumieniu z producentem) uruchomi dla Zamawiającego dedykowany portal przeglądowy i monitorujący działanie systemu, przy czym to uruchomienie nastąpi przed odebraniem przedmiotu zamówienia; viii) gwarancja producenta musi być świadczona codziennie, całą dobę przez co najmniej siedemdziesiąt pięć miesięcy.

System zabezpieczenia komunikacji teleinformatycznej ma realizować: - ochronę antyspamową, antywirusową oraz antyspyware'ową dla pięciuset użytkowników; - Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o komercyjne bazy zabezpieczeń; - pracę w trybach gateway oraz transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej); - wspierać powierzchnię dyskową o pojemności co najmniej 900GB; - Polityki filtrowania tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all); - routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP; - Zarządzanie kolejkami komunikacji (np. reguły opóźniania dostarczenia wiadomości; - 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; - Ochrona i analiza komunikacji przychodzącej jak i wychodzącej; - wielowarstwowe polityki wykrywania spamu oraz wirusów; - Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP; - Kwarantanna komunikacji z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika; - Możliwość poddania ponownemu skanowaniu (antywirus, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora; - Archiwizacja komunikacji przychodzącej i wychodzącej w oparciu o polityki; - przechowywanie komunikacji oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej NFS, iSCSI; - Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu; - Białe i czarne listy adresów mailowych dla poszczególnych użytkowników; - Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika; - Ochrona przed atakami na adres odbiorcy; - Definiowanie maksymalnej ilości wiadomości otrzymywanych w jednostce czasu; - Definiowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu; - Kontrola Reverse DNS; - Logowanie do zewnętrznego serwera SYSLOG; - Logowanie

zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku; - Logowanie informacji na temat spamu oraz niedozwolonych załączników; - Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych; - Możliwość analizy przebiegu sesji SMTP; - Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach; - Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym; - Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę; - System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH; - Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu webowego z opcją wstawienia własnego logo; - możliwość zdefiniowania co najmniej 3 lokalnych kont administracyjnych; - co najmniej dwie z certyfikacji: VBSpam, VB100 rated, Common Criteria NDPP, FIPS 140-2 Certified; - Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta; - Filtrowanie komunikacji w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania; - Szczegółowa kontrola nagłówka wiadomości; - Analiza Heurystyczna; - Współpraca z zewnętrznymi serwerami RBL, SURBL; - Możliwością dostrajania filtrów Bayes'a przez poszczególnych użytkowników; - Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF; - Filtrowanie treści wiadomości i załączników; - Możliwość zdefiniowania ponad pięćdziesiąt polityk kontroli antyspamowej i antywirusowej; - Ochrona typu outbrake dla spamu i wirusów; - Skanowanie załączników skompresowanych; - Definiowanie komunikatów powiadomień w języku polskim; - Blokowanie załączników w oparciu o typ pliku; - 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; - 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; - skanowanie antyspamowe i antywirusowe z wydajnością dwadzieścia pięć tysięcy wiadomości na godzinę; - System musi być dostarczony w modelu „na własność" tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania. Zasady wsparcia gwarancyjnego w powyższym zakresie, udzielonego na przedmiot zamówienia: i) wykonawca zapewni fabryczne wsparcie wszystkich producentów, których składniki zostaną użyte do realizacji przedmiotu zamówienia; ii) wsparcie, o którym mowa powyżej, ma zapewnić bez ponoszenia dodatkowych kosztów aktualizację wszystkich komponentów, również sprzętowych, składających się na realizację przedmiotu zamówienia; iii) wsparcie musi być zagwarantowane pisemnie na etapie składania ofert; iv) jeśli producentem systemu bezpieczeństwa jest wykonawca, to musi on mieć swoje regionalne przedstawicielstwo w Polsce i zadeklarować, że utrzyma je przez okres gwarancji; v) alternatywnie, jeśli producentem systemu bezpieczeństwa jest wykonawca, to musi wyznaczyć pełnomocnika, który będzie ponosił odpowiedzialność przez okres gwarancji, w przypadku niedostępności wykonawcy; vi) jeśli producentem systemu bezpieczeństwa nie jest wykonawca, to wsparcie o którym mowa powyżej, musi być zapewnione Zamawiającemu bezpośrednio przez producenta, tzn. bez pośrednictwa wykonawcy, już na etapie dostarczenia przedmiotu zamówienia; vii) wsparcie producenta musi być świadczone codziennie, całą dobę przez okres sześćdziesiąt miesięcy. System bezpieczeństwa teleinformatycznego i system zabezpieczenia komunikacji teleinformatycznej musi zapewniać dostępność co najmniej dla 500 użytkowników.

Analiza bieżącego poziomu ochrony i reguł zabezpieczeń musi być wykonana w siedzibie zamawiającego. System musi być wdrożony w oparciu o wykorzystywane reguły bezpieczeństwa. Zakres migracji reguł bezpieczeństwa, konfiguracji, itp. zostanie określony podczas realizacji umowy. Wdrożenie systemu bezpieczeństwa nie może zakłócić dostępu do usług w siedzibie Zamawiającego. Z uwagi na istotę i złożoność Platformy wsparcia bezpieczeństwa danych Zamawiający nie dopuszcza rozwiązań chmurowych. Zamawiający wymaga dostarczenia platformy sprzętowej dla oferowanego systemu niezbędnej do spełnienia wymaganych funkcjonalności i parametrów. W przypadku braku możliwości oceny spełnienia przez system wskazanych w opisie parametrów, zamawiający będzie wymagać uszczegółowienia specyfikacji oferowanego przedmiotu zamówienia i dostarczenia wersji testowej systemu w celu weryfikacji i wyboru oferty. W ramach wdrożenia niezbędne jest przeszkolenie 3 osób w zakresie pełnej obsługi i utrzymania wdrażanego systemu. Szkolenie musi być przeprowadzone w formie stacjonarnej.