Modyfikacja nr 1 z dn. 29.09.2023 r.
Załącznik nr 6 do SWZ - Opis Przedmiotu Zamówienia

na „Dostawę i wdrożenie specjalistycznych urządzeń i oprogramowania niezbędnych do podniesienia bezpieczeństwa systemów teleinformatycznych na potrzeby „Pro-Medica" w Ełku Sp. z o. o.”
Znak Sprawy 3532/2023

Przedmiot zamówienia finansowany jest ze środków pochodzących z Funduszu Przeciwdziałania COVID-19- działania w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych „Pro-Medica" w Ełku Sp. z o. o.”

I. Wymagania dotyczące systemu ochrony poczty elektronicznej

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 ochrony były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia w środowisku wirtualnym. W przypadku implementacji programowej dostawca musi zapewnić platformę w postaci odpowiednio zabezpieczonego systemu operacyjnego, na którym będzie instalowane rozwiązanie. Platformy muszą mieć możliwość uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi 6.0/6.5/7.0, Microsoft Hyper-V 2012 R2/2016/2019/2022, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, AWS (Amazon Web Services), Microsoft Azure.
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:

- Tryb Gateway.
- Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej).

Parametry fizyczne systemu antyspamowego

- System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności co najmniej 1 TB.

Ogólne funkcje systemu ochrony poczty

Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje:

- Wsparcie dla co najmniej 20 domen pocztowych.
- System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 25 tys. wiadomości/godzinę.
- Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all).
- Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP.
- Zarządzanie kolejkami wiadomości (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 zarówno poczty przychodzącej jak i wychodzącej.
- Szczegółowe, 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 poczty 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.
- Dostęp do kwarantanny użytkownika możliwy poprzez WebMail.
- Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki.
- Możliwość przechowywania poczty 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.

Kontrola antywirusowa i ochrona przed malware

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Skanowanie antywirusowe wiadomości SMTP.
2. Kwarantannę dla zainfekowanych plików.
3. Skanowanie załączników skompresowanych.
4. Definiowanie komunikatów powiadomień w języku polskim.
5. Blokowanie załączników w oparciu o typ pliku.
6. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antywirusowej.
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.
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.
9. Ochronę typu virus outbreak.
10. Ochronę przed zagrożeniami zawartymi wiadomościach pocztowych i w załącznikach (nie mniej niż: pliki MS Office, PDF, HTML, tekstowe) poprzez usuwanie treści będących zagrożeniem (makra, adresy URL zagnieżdżone w plikach, skrypty, ActiveX) i dostarczaniem oczyszczonych w ten sposób wiadomości.

Kontrola antyspamowa

System musi zapewniać poniższe funkcje i metody filtrowania spamu:

- Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta.
- Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania.
- Szczegółowa kontrola nagłówka wiadomości.
- Analiza Heurystyczna.
- Współpraca z zewnętrznymi serwerami RBL, SURBL.
- Filtrowanie w oparciu o filtry Bayes'a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen.
- Możliwością dostrajania filtrów Bayes'a przez poszczególnych użytkowników.
- Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF.
- Kontrola w oparciu o Greylisting oraz SPF.
- Filtrowanie treści wiadomości i załączników.
- Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości.
- Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antyspamowej.
- Ochrona typu outbreak.
- Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).
- Możliwość skanowania linków znajdujących się w przesyłkach pocztowych, w momencie ich kliknięcia przez adresata.
- Możliwość wykrywania i ochrony przed podszywaniem się (spoofing) pod wiadomości wysyłane przez osoby na stanowiskach kierowniczych (C-level)
- 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.

Ochrona przed atakami na usługę poczty
System musi zapewniać poniższe funkcje i metody filtrowania:

- Ochrona przed atakami na adres odbiorcy (m.in. email bombing).
- Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.
- Defniowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu.
- Kontrola Reverse DNS (ochrona przed Anty-Spoofing).
- Weryfikacja poprawności adresu e-mail nadawcy.

Funkcje logowania i raportowania
W tym zakresie dostarczony system ochrony poczty musi zapewniać:

- 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 pocztowych.
- Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu.
- Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.

Funkcje pracy w trybie wysokiej dostępności (HA)
System ochrony poczty musi zapewniać poniższe funkcje:

- Konfigurację HA w każdym z trybów: gateway, transparent.
- Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP.
- Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu.
- Monitorowanie stanu pracy klastra.

Aktualizacje sygnatur, dostęp do bazy spamu
W tym zakresie dostarczony system ochrony poczty musi zapewniać:

- Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym.
- Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.

Zarządzanie
System ochrony poczty musi zapewniać poniższe funkcje:

- System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH.
- Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy.
- Powinna istnieć możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych.

Serwisy i licencje
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.
W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

- Kontrola Antyspam, URL Filtering, kontrola antywirusowa, ochrona typu Virus Outbreak, Sandbox w chmurze, ochrona typu Click Protect, Content Disarm & Reconstruction, Business Email Compromise na okres [36] miesięcy.

Gwarancja oraz wsparcie

- System musi być objęty serwisem producenta przez okres [36] miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

Raport z testu skuteczności

Wdrożenie systemu ochrony poczty musi zawierać raport z przeprowadzonego testu skuteczności działania systemu w zakresie poprawność konfiguracji i podatność systemu pocztowego.

II. Wymagania dotyczące elementów rozbudowy systemu archiwizacji danych

1. Rozszerzenie posiadanej licencji oprogramowania do wykonywania kopii zapasowych

Zamawiający wymaga poniższych licencji oprogramowania backupowego.

- Zamiana posiadanych licencji:
- z wersji Veeam Data Platform Essentials Enterprise Plus w wersji perpetual na 4 procesory na wersję Veeam Data Platform Foundation Enterprise Plus w wersji perpetual na 4 procesory
- Zakup dodatkowych licencji Veeam Data Platform Foundation Enterprise Plus w wersji perpetual na 2 procesory wraz ze wsparciem do dnia 6 czerwca 2027

Raport z testu działania systemu

Wdrożenie nowych elementów systemu kopii zapasowych musi zawierać raport z przeprowadzonego testu działania systemu w zakresie Poprawność konfiguracji, podatność kopii zapasowej oraz z odtworzenia danych z kopii zapasowej do środowiska testowego.

2.. Zakup serwera do kopii zapasowych

Szczegółowe minimalne parametry:

Element konfiguracji	Wymagania minimalne
Obudowa	Maksymalnie 2U RACK 19 cali (wraz z szynami montażowymi oraz ramieniem do prowadzenia kabli, umożliwiającymi serwisowanie serwera w szafie RACK bez wyłączania urządzenia) Serwer wyposażony w zdejmowany panel przedni z możliwością instalacji zamka chroniącego przed nieuprawionym dostępem do dysków oraz czujnika otwarcia obudowy współpracującego z BIOS/UEFI.
Procesor	Zainstalowany jeden procesor ośmiordzeniowy, x86 - 64 bity, pracujący z częstotliwością bazową min. 2.8GHz i osiągający w testach SPECrate2017_int_base wynik nie gorszy niż 133 punkty, dla testu oferowanego modelu serwera z 2 procesorami. W przypadku zaoferowania procesora równoważnego, wynik testu musi być opublikowany na stronie www.spec.org Płyta główna wspierająca zastosowanie procesorów od 4 do 40 rdzeni, mocy do min. 270W i taktowaniu CPU do min. 3.6GHz.
Liczba procesorów	Min. 1 procesor
Pamięć operacyjna	Min. 64GB RDIMM DDR4 3200 MT/s w modułach pamięci o pojemności min. 32 GB każdy Płyta główna z minimum 32 slotami na pamięć i umożliwiająca instalację do minimum 8TB.
Sloty rozszerzeń	Min. 3 aktywne gniazda PCI-Express generacji 4, gniazda pełnej wysokości (full height) gotowe do obsadzenia kartami z portami zewnętrznymi, w tym min. 1 slot x16 (szybkość slotu – bus width).
Dysk twardy	Zatoki dyskowe gotowe do zainstalowania min. 12 dysków LFF typu Hot Swap, SAS/SATA/SSD 3,5”. Serwer umożliwiający instalację pamięci flash w postaci kart microSD/SD

	zapewniających minimalną pojemność 32GB i redundancję danych RAID-1. Zastosowane rozwiązanie musi posiadać gwarancję producenta serwera. Zainstalowane min. 8 szt. dysków 8TB SAS 7.2k 3,5”. Zainstalowane min. 2 dyski 480GB NVMe M.2 pracujące w RAID 1.
Kontroler	Serwer wyposażony w kontroler sprzętowy z min. 4GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, obsługujący poziomy: RAID 0/1/10/5/50/6/60. Kontroler wraz z niezbędnymi elementami zapewniający obsługę min. 12 napędów dyskowych SSD/SATA/SAS.
Interfejsy sieciowe	Minimum 2 wbudowane porty Ethernet 10Gb BaseT, które nie zajmują gniazd PCIe opisanych w sekcji „Sloty rozszerzeń”. Minimum 2 porty 16Gb FC obsadzone wkładkami MM.
Karta graficzna	Zintegrowana karta graficzna
Porty	5 x USB 3.0 (w tym 2 porty wewnętrzne) 1x VGA Wewnętrzny slot na kartę micro SD. Możliwość rozbudowy/rekonfiguracji o: - port szeregowy typu DB9/DE-9 (9 pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45 oraz bez konieczności instalowania kart w slotach PCI-Express
Zasilacz	2 szt., typu Hot-plug, redundantne, każdy o mocy minimum 800W.
Chłodzenie	Zestaw wentylatorów redundantnych typu hot-plug
Diagnostyka	Możliwość zainstalowania elektronicznego panelu diagnostycznego dostępnego z przodu serwera pozwalającego uzyskać informacje o stanie: procesora, pamięci, wentylatorów, zasilaczy, temperaturze.
System Operacyjny	Zainstalowany Windows Server 2022 Standard w wersji odpowiadającej liczbie dostarczonych rdzeni procesora.
Bezpieczeństwo	Serwer wyposażony w moduł TPM 2.0
Karta/moduł zarządzający	Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność: • monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski (fizyczne i logiczne), karty sieciowe • praca w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP • dostęp do karty zarządzającej poprzez 1. dedykowany port RJ45 z tyłu serwera lub 2. przez współdzielony port zintegrowanej karty sieciowej serwera dostęp do karty możliwy 3. z poziomu przeglądarki webowej (GUI) 4. z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP) 5. z poziomu skryptu (XML/Perl) 6. poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface) • wbudowane narzędzia diagnostyczne • zdalna konfiguracji serwera (BIOS) i instalacji systemu operacyjnego • obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie

	• wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników • przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough) • obsługa zdalnego serwera logowania (remote syslog) • wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i i wirtualnych folderów • mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie • funkcja zdalnej konsoli szeregowej - Textcons przez SSH (wirtualny port szeregowy) z funkcją nagrywania i odtwarzania sekwencji zdarzeń i aktywności • monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji • konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping) • zdalna aktualizacja oprogramowania (firmware) • zarządzanie grupami serwerów, w tym: 1. tworzenie i konfiguracja grup serwerów 2. sterowanie zasilaniem (wł/wył) 3. ograniczenie poboru mocy dla grupy (power capping) 4. aktualizacja oprogramowania (firmware) 5. wspólne wirtualne media dla grupy • możliwość równoczesnej obsługi przez 6 administratorów • autentykacja dwuskładnikowa (Kerberos) • wsparcie dla Microsoft Active Directory • obsługa SSL i SSH • enkrypcja AES/3DES oraz RC4 dla zdalnej konsoli • wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API • wsparcie dla Integrated Remote Console for Windows clients • możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP)
Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych	Zapewnia wsparcie dla: Microsoft Windows Server 2016, 2019, 2022 Ubuntu 20.04 LTS Red Hat Enterprise Linux (RHEL) 7.9 oraz 8.2 SUSE Linux Enterprise Server (SLES) 12 SP5 oraz 15 SP2 VMware ESXi 7.x, 8.x
Wsparcie techniczne	Minimum 3-letnia gwarancja producenta na części, robociznę i naprawę w miejscu instalacji typu On-Site z czasem reakcji NBD. W razie awarii dyski pozostają własnością Zamawiającego. Usługa wsparcia technicznego musi być świadczona przez serwis producenta oferowanych urządzeń.

3. Zakup biblioteki taśmowej LTO

Biblioteka musi obsługiwać co najmniej 24 gniazda na taśmy.
Obudowa maksymalnie RACK 2U.
Biblioteka wyposażona w napęd FC LTO8 (lub nowszy).
Interfejsy: minimum jeden interfejs sieciowy RJ45; minimum jeden interfejs FC do podłączenia do serwera kopii zapasowych – serwer kopii zapasowych musi być wyposażony w kompatybilny interfejs.
Kabel złącza FC długości min. 2m.
W zestawie min. 12 taśm LTO-8 + taśma czyszcząca.
Wsparcie producenta On-Site, 3 lata z czasem reakcji NBD.