URZĄD MARSZAŁKOWSKI
WOJEWÓDZTWA PODLASKIEGO
15-888 BIAŁYSTOK
ul. Kardynała Stefana Wyszyńskiego 1

Białystok, 26.06.2023 r.
BZP.272.26.2023.AR

Wykonawcy
(uczestnicy postępowania)

Zamawiający informuje, iż w postępowaniu przetargowym nr **BZP.272.26.2023.AR** pn.: **Zakup oprogramowania zabezpieczającego pocztę elektroniczną w domenie podlaskie.eu oraz wrotapodlasia.pl wraz ze sprzętem wymaganym do jego uruchomienia;** wpłynęły pytania o następującej treści:

Pytanie nr 1
Zwracamy się z pytaniem, czy Zamawiający dopuszcza możliwość modyfikacji treści §5 ust. 2 w dokumencie Umowy powierzenia przetwarzania danych osobowych w następujący sposób (modyfikację wprowadzono kursywą):

Przekazanie powierzonych danych do państwa trzeciego (poza EOG) może nastąpić jedynie na pisemne polecenie Administratora chyba, że obowiązek taki nakładają na Podmiot przetwarzający przepisy prawa, któremu podlega Podmiot przetwarzający *lub w sytuacji kiedy konieczne będzie przekazanie powierzonych danych osobowych Producentowi oprogramowania stanowiącego przedmiot Umowy Głównej, w sytuacji, w której konieczne będzie podjęcie działań naprawczych, do których wykonania uprawniony jest jedynie Producent*.

W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.

Odpowiedź Zamawiającego:
Zmiana zapisu nie może zostać uwzględniona.

Zakres danych, jakie zawiera korespondencja e-mail dotyczy większości procesów w odniesieniu do których w ramach odrębnych klauzul informacyjnych administrator informuje, ze dane osobowe nie będą przekazywane do państw trzecich. Wymagało by to przeprowadzenia dla praktycznie każdej czynności odrębnej pogłębionej analizy ryzyka oraz ponownego uzupełnienia wcześniej przedstawionych klauzul informacyjnych.

Ponadto przekazanie danych zawartych w korespondencji e-mail w oparciu o późniejszą informacje skierowana do administratora może być zrealizowane WYŁĄCZNIE W OPARCIU O OBOWIĄZEK PRAWNY PODMIOTU PRZETWARZAJĄCEGO, co nie jest związane z wsparciem technicznym oprogramowania.

Pytanie nr 2
Czy Zamawiający wyraża zgodę na modyfikację paragrafu 11 wzoru umowy w ten sposób, że zostanie dodany punkt 11 o następującym brzmieniu:

11. „W przypadku wystąpienia wady, usterki lub awarii oprogramowania wymagającej opracowania przez producenta zmian w oprogramowaniu (np. opracowanie zmian konfiguracyjnych pomiędzy komponentami oprogramowania, wydania przez producenta tzw. patch'a lub fix'a do oprogramowania lub innych zmian wymagających ingerencji producenta w kod źródłowy lub inne komponenty oprogramowania) naprawa

oprogramowania procedowana jest zgodnie z warunkami serwisu gwarancyjnego producenta oprogramowania. W przypadku wystąpienia wady lub usterki lub awarii oprogramowania, Wykonawca zobowiązany jest do dołożenia należytej staranności mającej na celu niezwłoczne powiadomienie w tym:

a) zebrania i dostarczenia informacji jednostce wsparcia producenta oprogramowania;
b) monitorowania czasów odpowiedzi producenta oprogramowania oraz eskalacji opóźnień;
c) instalacji na środowiskach testowych poprawek (patchy) dostarczonych przez producenta oprogramowania (chyba że Zamawiający wskaże środowiska, na których instalacja będzie realizowana bezpośrednio przez Zamawiającego);
d) testowania poprawek dostarczonych przez producenta oprogramowania;"

Odpowiedź Zamawiającego:
Zamawiający wyraża zgodę na wprowadzenie powyższych zmian.
Zamawiający wprowadza zmiany w Umowie.

Zmiana z:

§ 11. GWARANCJA

1. Wykonawca udzieli gwarancji na dostarczony Przedmiot Umowy, zgodnie z warunkami określonymi w SOPZ i ofercie Wykonawcy.

2. Zamawiający może wykonywać uprawnienia z tytułu gwarancji niezależnie od uprawnień wynikających z tytułu rękojmi.

3. W okresie gwarancji Wykonawca zobowiązany jest do naprawy lub wymiany każdego z elementów podzespołów lub zespołów dostarczonego Przedmiotu Umowy, które uległy uszkodzeniu lub awarii. Decyzję o sposobie usunięcia wady dokonuje Zamawiający przyjmując, że naprawa będzie właściwym sposobem usunięcia wady, o ile będzie to możliwe i użyteczne z punktu widzenia jego potrzeb.

4. Na czas naprawy lub wymiany, Wykonawca zobowiązany jest dostarczyć Zamawiającemu sprzęt zastępczy wraz z usługą wdrożenia na miejscu, o równorzędnych lub wyższych parametrach użytkowych i konfiguracji, zgodnie z Przedmiotem Umowy.

5. Okres gwarancji i wsparcia serwisowego ulega przedłużeniu o czas ograniczonej możliwości używania Przedmiotu Umowy lub jego części wskutek trwania naprawy lub wymiany – do dnia protokolarnego potwierdzenia usunięcia wady.

6. W sytuacji, gdy Wykonawca po wezwaniu do usunięcia wady lub wymiany wadliwego sprzętu, nie dopełni ciążących na nim obowiązków, Zamawiający jest uprawniony do usunięcia wad w drodze naprawy lub wymiany sprzętu lub jego części na ryzyko i koszt Wykonawcy.

7. W okresie gwarancji usługi serwisowe sprzętu, jego naprawa lub wymiana następują w ramach wynagrodzenia wynikającego z niniejszej umowy.

8. W przypadku awarii dysku twardego, dysk pozostaje w siedzibie Zamawiającego.

9. Jeżeli z warunków gwarancji wynika obowiązek przeprowadzania bieżącej konserwacji lub dokonywania przeglądów okresowych, Wykonawca będzie ich dokonywał bez wezwania Zamawiającego. Wykonawca ma obowiązek uzgodnić z Zamawiającym dogodny termin dokonania powyższych czynności z co najmniej 7-dniowym wyprzedzeniem.

10. W okresie gwarancji Zamawiający ma prawo do instalowania, rekonfiguracji, wymiany podzespołów, zmian w konfiguracji oprogramowania itp. i odpowiedniej konserwacji sprzętu, co nie wpływa na ważność udzielonej gwarancji.

na:

§ 11. GWARANCJA

1. Wykonawca udzieli gwarancji na dostarczony Przedmiot Umowy, zgodnie z warunkami określonymi w SOPZ i ofercie Wykonawcy.

2. Zamawiający może wykonywać uprawnienia z tytułu gwarancji niezależnie od uprawnień wynikających z tytułu rękojmi.

3. W okresie gwarancji Wykonawca zobowiązany jest do naprawy lub wymiany każdego z elementów podzespołów lub zespołów dostarczonego Przedmiotu Umowy, które uległy uszkodzeniu lub awarii. Decyzję o sposobie usunięcia wady dokonuje Zamawiający przyjmując, że naprawa będzie właściwym sposobem usunięcia wady, o ile będzie to możliwe i użyteczne z punktu widzenia jego potrzeb.

4. Na czas naprawy lub wymiany, Wykonawca zobowiązany jest dostarczyć Zamawiającemu sprzęt zastępczy wraz z usługą wdrożenia na miejscu, o równorzędnych lub wyższych parametrach użytkowych i konfiguracji, zgodnie z Przedmiotem Umowy.

5. Okres gwarancji i wsparcia serwisowego ulega przedłużeniu o czas ograniczonej możliwości używania Przedmiotu Umowy lub jego części wskutek trwania naprawy lub wymiany – do dnia protokolarnego potwierdzenia usunięcia wady.

6. W sytuacji, gdy Wykonawca po wezwaniu do usunięcia wady lub wymiany wadliwego sprzętu, nie dopełni ciążących na nim obowiązków, Zamawiający jest uprawniony do usunięcia wad w drodze naprawy lub wymiany sprzętu lub jego części na ryzyko i koszt Wykonawcy.

7. W okresie gwarancji usługi serwisowe sprzętu, jego naprawa lub wymiana następują w ramach wynagrodzenia wynikającego z niniejszej umowy.

8. W przypadku awarii dysku twardego, dysk pozostaje w siedzibie Zamawiającego.

9. Jeżeli z warunków gwarancji wynika obowiązek przeprowadzania bieżącej konserwacji lub dokonywania przeglądów okresowych, Wykonawca będzie ich dokonywał bez wezwania Zamawiającego. Wykonawca ma obowiązek uzgodnić z Zamawiającym dogodny termin dokonania powyższych czynności z co najmniej 7-dniowym wyprzedzeniem.

10. W okresie gwarancji Zamawiający ma prawo do instalowania, rekonfiguracji, wymiany podzespołów, zmian w konfiguracji oprogramowania itp. i odpowiedniej konserwacji sprzętu, co nie wpływa na ważność udzielonej gwarancji.

11. W przypadku wystąpienia wady, usterki lub awarii oprogramowania wymagającej opracowania przez producenta zmian w oprogramowaniu (np. opracowanie zmian konfiguracyjnych pomiędzy komponentami oprogramowania, wydania przez producenta tzw. patch'a lub fix'a do oprogramowania lub innych zmian wymagających ingerencji producenta w kod źródłowy lub inne komponenty oprogramowania) naprawa oprogramowania procedowana jest zgodnie z warunkami serwisu gwarancyjnego producenta oprogramowania. W przypadku wystąpienia wady lub usterki lub awarii oprogramowania, Wykonawca zobowiązany jest do dołożenia należytej staranności mającej na celu niezwłoczne powiadomienie w tym:

1) niezwłocznego poinformowania Zamawiającego o wystąpieniu tego rodzaju wady, usterki lub awarii oprogramowania;
2) zebrania i dostarczenia informacji jednostce wsparcia producenta oprogramowania;
3) monitorowania czasów odpowiedzi producenta oprogramowania oraz eskalacji opóźnień;
4) instalacji na środowiskach testowych poprawek (patchy) dostarczonych przez producenta oprogramowania (chyba że Zamawiający wskaże środowiska, na których instalacja będzie realizowana bezpośrednio przez Zamawiającego);
5) testowania poprawek dostarczonych przez producenta oprogramowania.

Pytanie nr 3

Zwracamy się z pytaniem dotyczącym opisu przedmiotu zamówienia pkt 5 a)

Producent oferowanego rozwiązania nie realizuje szkoleń certyfikowanych. Czy Zamawiający zaakceptuje przeprowadzenie warsztatów szkoleniowych przez Wykonawcę w zakresie podstawowej i zaawansowanej konfiguracji oprogramowania do ochrony poczty elektronicznej, zakończone autorskim egzaminem wiedzy i wystawionym certyfikatem uczestnictwa? Wykonawca posiada najwyższy - platynowy status partnerski oferowanego rozwiązania.

Odpowiedź Zamawiającego:

Zamawiający zaakceptuje przeprowadzeń szkoleń przez Wykonawcę.
Zamawiający wprowadza zmiany w Szczegółowym Opisie Przedmiotu Zamówienia.
Zmiana z:
5. Wymagania dotyczące szkoleń:

a) w ramach realizacji Przedmiotu Umowy Wykonawca zapewni uczestnictwo w autoryzowanych przez producenta szkoleniach w zakresie podstawowej i zaawansowanej konfiguracji oprogramowania do ochrony poczty elektronicznej, zakończone autoryzowanym egzaminem wiedzy co najmniej czterech pracowników Zamawiającego, w terminie zaakceptowanym przez Zamawiającego;

b) Wykonawca dostarczy autoryzowane materiały szkoleniowe w języku polskim lub angielskim;

na:

5. Wymagania dotyczące szkoleń;

a) w ramach realizacji Przedmiotu Umowy Wykonawca zapewni uczestnictwo w autoryzowanych przez producenta szkoleniach w zakresie podstawowej i zaawansowanej konfiguracji oprogramowania do ochrony poczty elektronicznej, zakończone autoryzowanym egzaminem wiedzy co najmniej czterech pracowników Zamawiającego, w terminie zaakceptowanym przez Zamawiającego. W przypadku gdy Producent oferowanego rozwiązania nie realizuje szkoleń certyfikowanych, Zamawiający dopuszcza możliwość przeprowadzenia niecertyfikowanych szkoleń przez Wykonawcę w zakresie nie mniejszym niż podstawowa i zaawansowana konfiguracja i obsługa systemu, zajmujących min. 24 godziny lekcyjne. W tym przypadku Wykonawca przedstawi Zamawiającemu program szkolenia do akceptacji w terminie 10 dni roboczych od dnia podpisania umowy. Wykonawca ma obowiązek dostosować program szkoleń do uwag Zamawiającego;
b) Wykonawca dostarczy autoryzowane materiały szkoleniowe w języku polskim lub angielskim w przypadku szkoleń certyfikowanych lub w języku polskim w przypadku szkoleń niecertyfikowanych, realizowanych przez Wykonawcę;

Pytanie nr 4

Zwracamy sie z pytaniem dotyczącym opisu przedmiotu zamówienia pkt 6.2 b), 6.4 b), 6.6 b), 7.1

Głównym aspektem w przypadku ochrony poczty email jest ochrona kont pocztowych Zamawiającego, a więc poczty przychodzącej. Analiza poczty wychodzącej powinna być realizowana przez system klasy AntySpam, aby nie dopuścić do wysyłania niechcianych wiadomości (Spam).
Czy Zamawiający zaakceptuje rozwiązanie, które nie realizuje funkcjonalności analizy poczty wychodzącej?

Odpowiedź Zamawiającego:
Zamawiający zaakceptuje rozwiązanie, które nie realizuje funkcjonalności analizy poczty wychodzącej.
Zamawiający wprowadza zmiany w Szczegółowym Opisie Przedmiotu Zamówienia.
Zmiana punktów 6 i 7 z:

6. **Wymagania w zakresie wdrożenia:**
   6.1. przeprowadzenie analizy środowiska pocztowego Zamawiającego;
   6.2. przygotowanie koncepcji wdrożenia Systemu w zakresie poniższych punktów:
      a) ochrona w trybie inline (MTA) poczty przychodzącej obsługiwanej przez lokalny serwer Zimbra;
      b) ochrona w trybie inline (MTA) poczty wychodzącej obsługiwanej przez lokalny serwer Zimbra.
   6.3. Przygotowanie projektu technicznego obejmującego swoim zakresem co najmniej:
      a) schemat przepływu poczty przychodzącej oraz wychodzącej;
      b) opis konfiguracji przepływu poczty przychodzącej oraz wychodzącej (email routing);

c) opis konfiguracji polityk bezpieczeństwa;
d) opis konfiguracji kwarantanny oprogramowania do ochrony poczty elektronicznej;
e) opis dostępu do spersonalizowanej kwarantanny użytkowników.

6.4. Konfiguracja oprogramowania do ochrony poczty elektronicznej zgodnie z zaakceptowanym przez zespół odbiorowy projektem wdrożenia w zakresie:
a) konfiguracji obsługiwanych przez System domen pocztowych;
b) konfiguracji przepływu poczty przychodzącej oraz wychodzącej;
c) konfiguracji weryfikacji połączeń przychodzących pod względem rekordów SPF, DKIM oraz DMARC;
d) konfiguracji wpisów SPF, DKIM oraz DMARC Zamawiającego;
e) konfiguracji polityk bezpieczeństwa;
f) konfiguracji mechanizmów analizy wiadomości;
g) konfiguracji funkcjonalności przepisywania adresów URL w wiadomościach;
h) konfiguracji kwarantanny, uprawnień dla odbiorców oraz spersonalizowanego dostępu do kwarantanny dla użytkowników Zamawiającego.

6.5. Asysta podczas rekonfiguracji ruchu pocztowego uwzględniającego oprogramowanie do ochrony poczty elektronicznej.

6.6. Przeprowadzenie testów weryfikujących działanie oprogramowania do ochrony poczty elektronicznej pod względem:
a) dla poczty przychodzącej: poprawnego dostarczania wiadomości do odbiorcy;
b) dla poczty wychodzącej: poprawnego wysyłania wiadomości;
c) poprawnej analizy procesowanych wiadomości przychodzących oraz wychodzących;
d) poprawnego zatrzymywania zainfekowanych wiadomości w kwarantannie oraz poprawnego ich zwalniania z kwarantanny.

6.7. Przygotowanie dokumentacji powdrożeniowej opisującej co najmniej punkty projektu technicznego oraz opis wszelkich wprowadzonych konfiguracji do Systemu.

6.8. Miejsca realizacji przedmiotu Umowy: ul. Wyszyńskiego 1, 15-888 Białystok oraz ul. Poleska 89, 15-874 Białystok.

6.9. Montaż urządzeń, dostarczanych przez Wykonawcę, w szafie RACK wskazanej przez Zamawiającego. Montaż urządzeń Systemu będzie polegał na instalacji w dwóch budynkach Zamawiającego, oddalonych od siebie w odległości ok. 1 km i połączonych ze sobą ciemnymi włóknami światłowodowymi.

6.10. Wykonanie okablowania oraz podłączenie do istniejącej infrastruktury Zamawiającego.

6.11. Wykonawcy nie przysługuje dodatkowe wynagrodzenie ani zwrot poniesionych jakichkolwiek kosztów z tytułu realizacji prac w siedzibie Zamawiającego.

6.12. Potwierdzeniem prawidłowej realizacji Przedmiotu Umowy, w zakresie dokumentacji projektowej, będzie odbiór dostawy potwierdzony na podstawie sporządzonego zgodnie z wzorem załącznika nr 3 do Umowy

6.13. Potwierdzeniem prawidłowej realizacji Przedmiotu Umowy w zakresie uruchomienia i skonfigurowania Systemu będzie dostarczony raport z przeprowadzonych Testów Akceptacyjnych oraz odbiór dostawy potwierdzony na podstawie sporządzonego zgodnie z wzorem załącznika nr 3 do Umowy.

7. **Opis funkcjonalny Oprogramowania do ochrony poczty:**

7.1. Oprogramowanie musi umożliwić analizę wiadomości email zarówno przychodzących jak i wychodzących.

7.2. Oprogramowanie musi::
a) umożliwiać wdrożenie w trybach:
- inline – działanie jako MTA, będąc pośrednikiem w ruchu email do serwerów poczty;
- BCC – działanie na pasywnej kopii wiadomości email generowanej przez inny system pocztowy;

b) umożliwiać instalację zarówno jako pierwszy system ochrony poczty w środowisku Zamawiającego jak i na instalację pomiędzy innymi systemami bezpieczeństwa poczty;
c) obsługiwać wiele domen pocztowych;
d) umożliwiać oddzielną konfigurację wszystkich typów polityk dla różnych domen pocztowych;
e) umożliwiać akceptowanie połączeń przychodzących wyłącznie z podanych adresów IP;
f) umożliwiać weryfikację parametrów SPF, DKIM oraz DMARC nadawcy wiadomości;

g) umożliwiać podejmowanie określonych akcji w zależności od werdyktu weryfikacji parametrów SPF, DKIM oraz DMARC, co najmniej: automatyczna kwarantanna wiadomości, odrzucenie połączenia, modyfikacja tematu wiadomości oraz dodanie nagłówka;
h) umożliwiać konfigurację mechanizmu DKIM dla wiadomości wychodzących;
i) wykrywać zagrożenia w poczcie email bazując na sygnaturach;
j) wykrywać zagrożenia w poczcie email wykonując analizę dynamiczną nieznanych zagrożeń w odizolowanym środowisku typu sandbox bazującym na autorskich mechanizmach wirtualizacji (hypervisor). Nie może wykorzystywać to tego celu dostępnych rozwiązań takich jak VMware, MS Hyper-V czy VirtualBox.

7.3. Oprogramowanie musi zapewnić wykrywanie zaawansowanych ataków przenoszonych w załącznikach do poczty oraz kontrolę adresów URL umieszczanych w treści wiadomości oraz analizę samej wiadomości, przy czym:
a) po wykryciu wcześniej znanego, szkodliwego adresu URL musi być możliwe wygenerowanie alertu i umieszczenie wiadomości w kwarantannie;
b) po wykryciu nieznanego wcześniej adresu URL prowadzącego do pliku (co najmniej PDF, ZIP, EXE, DOC/DOCX) musi być możliwe automatyczne nawiązanie połączenia do Internetu przez oprogramowanie, pobranie pliku i przeanalizowanie go, a następnie w razie wykrycia zagrożenia, wygenerowanie alertu i zapisanie wiadomości email w kwarantannie.

7.4. Oprogramowanie musi rozpoznawać i wyodrębniać malware oraz inne szkodliwe oprogramowanie w załącznikach do poczty niezależnie od użytego rozszerzenia pliku.

7.5. Oprogramowanie musi umożliwiać wykorzystanie reguł, stworzonych samodzielnie przez Zamawiającego, opisujących cechy podejrzanych obiektów w formacie YARA.

7.6. Oprogramowanie musi posiadać dodatkowe mechanizmy chroniące pocztę email Zamawiającego przed atakami:
a) phishing/spear phishing - podszywanie się pod inną organizację lub osobę w celu wyłudzenia m.in. danych uwierzytelniających);
b) impersonation (CEO fraud) - kradzieży informacji lub wywierania wpływu na podejmowane decyzje, w wyniku podszywania się pod osoby będące członkami kadry zarządzającej;
c) infekcją kodu JavaScript, VBScript;
d) spywre/adware - niebezpieczne aplikacje, odnośniki URL lub załączniki będące częścią ataku.

7.7. Oprogramowanie musi posiadać mechanizmy analizujące wiadomości email pod kątem spamu, newsletterów oraz ataków typu APT.

7.8. Oprogramowanie musi umożliwiać deszyfrację załączników przesyłanych przez pocztę email Zamawiającego przy użyciu listy najczęściej używanych haseł lub inteligentnego wyszukiwania haseł w treści maila.

7.9. Oprogramowanie musi umożliwiać deszyfrację załączników w oparciu o hasło odczytane z obrazu graficznego (OCR) przesłanego w tej samej wiadomości.

7.10. Oprogramowanie musi posiadać środowiska wirtualne służące do analizy zagrożeń co najmniej w systemach operacyjnych: Windows 7, Windows 10, Windows 11, MacOS i Linux. Maszyny wirtualne muszą być aktualizowane przez producenta oraz nie mogą wymagać posiadania dodatkowych licencji przez Zamawiającego.

7.11. Oprogramowanie musi wykonywać analizę dynamiczną równocześnie w różnych wersjach systemów operacyjnych, różnych aplikacjach i różnych ich wersjach.

7.12. Rozwiązanie musi analizować co najmniej następujące rodzaje plików:
a) rozszerzenia używane przez pakiet OFFICE, np. DOC/DOCX, XLS/XLSX, PPT/PPTX;
b) pliki wykonywalne, np. EXE, DLL;
c) inne, np. CHM, RAR, ACE, SCR, PDF, PUB, ZIP, MP3, 7Z, BZ, GZ, JAR, MHT, RTF, CAB.

7.13. Oprogramowanie musi zapewniać dostęp do sekwencyjnego (krok po kroku) zapisu zmian wykonywanych przez załącznik w środowisku wirtualnym co najmniej w rejestrze, procesach, systemie plików, sposobie startu systemu, próby nawiązania połączenia sieciowego (wraz z zapisem tych prób w postaci plików PCAP dostępnych w GUI Oprogramowania) oraz umożliwiać pobranie artefaktów z przeprowadzonej analizy co najmniej w zakresie analizowanej próbki.

7.14. Oprogramowanie musi posiadać mechanizm do wykrywania podszycia się pod inną osobę (na poziomie adresu email i wyświetlanej nazwy użytkownika oraz adresu email nadawcy i pola reply to).
7.15. Oprogramowanie musi posiadać dodatkowy mechanizm wykrywania zdarzeń tak zwanych "commodity malware", takich jak zaszyfrowane dokumenty, pliki wykonywalne, pliki z załączonymi obiektami, nietypowe rozszerzenia plików, formularz HTTP_request, wykorzystanie MagicBytes, przekierowania HTML w załączniku. Zdarzenia te powinny być konfigurowalne jako alert lub automatyczna kwarantanna.
7.16. Oprogramowanie musi posiadać dodatkowych mechanizm wykrywający obiekty lub zdarzenia, które mogą wskazywać, że są elementem ataku:
   a) skrypty przesyłane w wiadomości email;
   b) pliki wykonywalne przesyłane w załączniku lub URL;
   c) dokumentów MS OFFICE z zaimplementowanym makro lub kodem wykonywalnym;
   d) nietypowych załączników przesyłanych w wiadomości takich jak: BAT, CPL, LNK, COM, CMD, MHT, PIF, PUB, HLP, HTA, ISO;
   e) wiadomości email ze skróconymi linkami (tiny URL);
   f) dokumentów MS OFFICE z flash;
   g) plików JAR;
   h) haseł przesyłanych w treści wiadomości HTTP request;
   i) zaszyfrowanych plików PDF;
   j) pliki typu wygaszacz ekranu;
   k) nieznanych plików konfiguracyjnych .SettingContent-ms.
7.17. Oprogramowanie musi mieć możliwość przepisania nieznanych adresów URL w przesyłanej wiadomości, tak aby pomimo kliknięcia, użytkownik nie był przekierowany do potencjalnie złośliwej treści, a do strony producenta informującej (w języku polskim) o zablokowaniu tej komunikacji.
7.18. Oprogramowanie musi posiadać mechanizm ekstrakcji (rozpoznawania) adresów URL z załączników przesyłanych w wiadomości email i możliwość detonowania ich w środowisku wirtualnym w przypadku pliku zlokalizowanego w URL.
7.19. Oprogramowanie musi posiadać możliwość automatycznego generowania "screenshotów" stron phishingowych w przypadku wykrytego alertu.
7.20. Oprogramowanie musi umożliwiać konfigurację reguł bazujących na wyrażeniach regularnych w celu modyfikacji ochrony w zakresie: adresu e-mail nadawcy, domeny nadawcy, adresu IP nadawcy, kraju nadawcy, adresu e-mail odbiorcy, treści wiadomości i jej tytułu (zarówno whitelisty jak i blacklisty).
7.21. Oprogramowanie musi umożliwiać konfigurację reguł bazujących na wystąpieniu konkretnego nagłówka wiadomości oraz jego wartości i podejmować wskazaną akcję.
7.22. Oprogramowanie musi dla punktów 7.20 oraz 7.21 umożliwiać podejmowanie wskazanych akcji w zakresie co najmniej: przeniesienie do kwarantanny, dostarczenie, utworzenie i wysłanie BCC, przesłanie na inny serwer pocztowy, zmodyfikowanie tytułu oraz dopisanie wskazanego nagłówka wraz z jego wartością. Niniejsze reguły muszą umożliwiać stosowanie wyjątków oraz stosowania kilku akcji jednocześnie.
7.23. Oprogramowanie musi mieć zaimplementowany mechanizm wyszukiwania analizowanych wiadomości pocztowych zawierający filtry wyszukujące co najmniej przy użyciu: adresu email odbiorcy, adresu email nadawcy, adresu IP nadawcy, tematu wiadomości, nazwy załącznika, MD5 oraz SHA256 załącznika, werdyktu analizy z uwzględnieniem mechanizmów, które wygenerowały ewentualny alert (np. SPAM, AV, custom rules). Niniejszy mechanizm musi umożliwiać wyszukiwanie wiadomości co najmniej do 30 dni wstecz.
7.24. Oprogramowanie musi analizować wiadomości email nawet po ich dostarczeniu i alertować o możliwej podmianie zawartości URL na złośliwą (analiza wsteczna).
7.25. Oprogramowanie musi udostępniać spersonalizowaną dla każdego odbiorcy kwarantannę.
7.26. Oprogramowanie musi umożliwiać precyzowanie uprawnień dla odbiorców wiadomości do zwalniania zablokowanych przez oprogramowanie wiadomości z jego spersonalizowanej kwarantanny w zależności od wykrytego zagrożenia.
7.27. Oprogramowanie musi dostarczać do odbiorców powiadomienia mailowe z listą wiadomości znajdujących się w jego spersonalizowanej kwarantannie. Oprogramowanie musi mieć możliwość sprecyzowania częstotliwości dostarczania powiadomień oraz konfiguracji dostarczanej formatki.

7.28. Oprogramowanie musi umożliwiać wysyłanie alertów o zdarzeniach poprzez protokoły SMTP oraz RSYSLOG.
7.29. Oprogramowanie musi umożliwiać administratorom systemu pobranie wiadomości, która została zablokowana, jej wyświetlenie zarówno w formie sparsowanej, jak i tekstowo z uwzględnieniem jej nagłówków.
7.30. Oprogramowanie musi umożliwić ręczne zwalnianie zablokowanych wiadomości z kwarantanny przez administratorów systemu.
7.31. Oprogramowanie musi umożliwiać tworzenie dedykowanych pulpitów w GUI rozwiązania z możliwością dostosowania wyświetlanych informacji.
7.32. Oprogramowanie musi umożliwiać generowanie raportów zawierających co najmniej:
   a) statystyki wykrytych alertów z rozbiciem na kategorie zagrożenia (co najmniej spam, impersonation, viruses, itp.);
   b) statystyki przeanalizowanych wiadomości email;
   c) statystyki najpopularniejszych adresów email oraz adresów IP nadawców oraz adresów email odbiorców;
   d) statystyki formatów przeanalizowanych załączników;
   e) powyższe statystyki powinny umożliwiać filtrowanie pod względem podłączonych do oprogramowania domen pocztowych.
7.33. Raporty muszą mieć możliwość eksportu do formatu CSV lub PDF wraz z możliwością ustalenia okresu czasu dla generowanego raportu (co najmniej ostatnie 24 godziny, ostatni 7 dni, ostatnie 30 dni).
7.34. Interfejs oprogramowania musi być w języku polskim lub angielskim.
7.35. Dostęp do oprogramowania musi być zabezpieczone kryptograficznie poprzez szyfrowanie komunikacji.
7.36. Oprogramowanie musi pozwalać na zdefiniowanie wielu administratorów o różnych poziomach uprawnień.

na:

6. **Wymagania w zakresie wdrożenia:**
6.1. przeprowadzenie analizy środowiska pocztowego Zamawiającego - przygotowanie koncepcji wdrożenia Systemu w zakresie ochrony w trybie inline (MTA) poczty przychodzącej obsługiwanej przez lokalny serwer Zimbra.
6.2. Przygotowanie projektu technicznego obejmującego swoim zakresem co najmniej:
   a) schemat przepływu poczty przychodzącej oraz wychodzącej;
   b) opis konfiguracji przepływu poczty przychodzącej oraz wychodzącej (email routing);
   c) opis konfiguracji polityk bezpieczeństwa;
   d) opis konfiguracji kwarantanny oprogramowania do ochrony poczty elektronicznej.
6.3. Konfiguracja oprogramowania do ochrony poczty elektronicznej zgodnie z zaakceptowanym przez zespół odbiorowy projektem wdrożenia w zakresie:
   a) konfiguracji obsługiwanych przez System domen pocztowych;
   b) konfiguracji przepływu poczty przychodzącej;
   c) konfiguracji polityk bezpieczeństwa;
   d) konfiguracji mechanizmów analizy wiadomości;
   e) konfiguracji funkcjonalności przepisywania adresów URL w wiadomościach.
6.4. Asysta podczas rekonfiguracji ruchu pocztowego uwzględniającego oprogramowanie do ochrony poczty elektronicznej.
6.5. Przeprowadzenie testów weryfikujących działanie oprogramowania do ochrony poczty elektronicznej pod względem:
   a) dla poczty przychodzącej: poprawnego dostarczania wiadomości do odbiorcy;
   b) poprawnej analizy procesowanych wiadomości przychodzących oraz wychodzących;
   c) poprawnego zatrzymywania zainfekowanych wiadomości w kwarantannie oraz poprawnego ich zwalniania z kwarantanny.
6.6. Przygotowanie dokumentacji powdrożeniowej opisującej co najmniej punkty projektu technicznego oraz opis wszelkich wprowadzonych konfiguracji do Systemu.

6.7. Miejsca realizacji przedmiotu Umowy: ul. Wyszyńskiego 1, 15-888 Białystok oraz ul. Poleska 89, 15-874 Białystok.
6.8. Montaż urządzeń, dostarczanych przez Wykonawcę, w szafie RACK wskazanej przez Zamawiającego. Montaż urządzeń Systemu będzie polegał na instalacji w dwóch budynkach Zamawiającego, oddalonych od siebie w odległości ok. 1 km i połączonych ze sobą ciemnymi włóknami światłowodowymi.
6.9. Wykonanie okablowania oraz podłączenie do istniejącej infrastruktury Zamawiającego.
6.10. Wykonawcy nie przysługuje dodatkowe wynagrodzenie ani zwrot poniesionych jakichkolwiek kosztów z tytułu realizacji prac w siedzibie Zamawiającego.
6.11. Potwierdzeniem prawidłowej realizacji Przedmiotu Umowy, w zakresie dokumentacji projektowej, będzie odbiór dostawy potwierdzony na podstawie sporządzonego zgodnie z wzorem załącznika nr 3 do Umowy
6.12. Potwierdzeniem prawidłowej realizacji Przedmiotu Umowy w zakresie uruchomienia i skonfigurowania Systemu będzie dostarczony raport z przeprowadzonych Testów Akceptacyjnych oraz odbiór dostawy potwierdzony na podstawie sporządzonego zgodnie z wzorem załącznika nr 3 do Umowy.

7. **Opis funkcjonalny Oprogramowania do ochrony poczty:**

7.1. Oprogramowanie musi umożliwić analizę wiadomości email zarówno przychodzących.
7.2. Oprogramowanie musi::
   a) umożliwiać wdrożenie w trybach:
      - inline – działanie jako MTA, będąc pośrednikiem w ruchu email do serwerów poczty;
      - BCC – działanie na pasywnej kopii wiadomości email generowanej przez inny system pocztowy;
   b) umożliwiać instalację pomiędzy innymi systemami bezpieczeństwa poczty;
   c) obsługiwać wiele domen pocztowych;
   d) umożliwiać konfigurację mechanizmu DKIM dla wiadomości wychodzących;
   e) wykrywać zagrożenia w poczcie email bazując na sygnaturach;
   f) wykrywać zagrożenia w poczcie email wykonując analizę dynamiczną nieznanych zagrożeń w odizolowanym środowisku typu sandbox bazującym na autorskich mechanizmach wirtualizacji (hypervisor). Nie może wykorzystywać to tego celu dostępnych rozwiązań takich jak VMware, MS Hyper-V czy VirtualBox.
7.3. Oprogramowanie musi zapewnić wykrywanie zaawansowanych ataków przenoszonych w załącznikach do poczty oraz kontrolę adresów URL umieszczanych w treści wiadomości oraz analizę samej wiadomości, przy czym:
   c) po wykryciu wcześniej znanego, szkodliwego adresu URL musi być możliwe wygenerowanie alertu i umieszczenie wiadomości w kwarantannie;
   d) po wykryciu nieznanego wcześniej adresu URL prowadzącego do pliku (co najmniej PDF, ZIP, EXE, DOC/DOCX) musi być możliwe automatyczne nawiązanie połączenia do Internetu przez oprogramowanie, pobranie pliku i przeanalizowanie go, a następnie w razie wykrycia zagrożenia, wygenerowanie alertu i zapisanie wiadomości email w kwarantannie.
7.4. Oprogramowanie musi rozpoznawać i wyodrębniać malware oraz inne szkodliwe oprogramowanie w załącznikach do poczty niezależnie od użytego rozszerzenia pliku.
7.5. Oprogramowanie musi umożliwiać wykorzystanie reguł, stworzonych samodzielnie przez Zamawiającego, opisujących cechy podejrzanych obiektów w formacie YARA.
7.6. Oprogramowanie musi posiadać dodatkowe mechanizmy chroniące pocztę email Zamawiającego przed atakami:
   e) phishing/spear phishing - podszywanie się pod inną organizację lub osobę w celu wyłudzenia m.in. danych uwierzytelniających);
   f) impersonation (CEO fraud) - kradzieży informacji lub wywierania wpływu na podejmowane decyzje, w wyniku podszywania się pod osoby będące członkami kadry zarządzającej;
   g) infekcją kodu JavaScript, VBScript;
   h) spywre/adware - niebezpieczne aplikacje, odnośniki URL lub załączniki będące częścią ataku.
7.7. Oprogramowanie musi posiadać mechanizmy analizujące wiadomości email pod kątem spamu, newsletterów oraz ataków typu APT.

7.8. Oprogramowanie musi umożliwiać deszyfrację załączników przesyłanych przez pocztę email Zamawiającego przy użyciu listy najczęściej używanych haseł lub inteligentnego wyszukiwania haseł w treści maila.
7.9. Oprogramowanie musi umożliwiać deszyfrację załączników w oparciu o hasło odczytane z obrazu graficznego (OCR) przesłanego w tej samej wiadomości.
7.10. Oprogramowanie musi posiadać środowiska wirtualne służące do analizy zagrożeń co najmniej w systemach operacyjnych: Windows 7, Windows 10, MacOS i Linux. Maszyny wirtualne muszą być aktualizowane przez producenta oraz nie mogą wymagać posiadania dodatkowych licencji przez Zamawiającego.
7.11. Oprogramowanie musi wykonywać analizę dynamiczną równocześnie w różnych wersjach systemów operacyjnych, różnych aplikacjach i różnych ich wersjach.
7.12. Rozwiązanie musi analizować co najmniej następujące rodzaje plików:
    a) rozszerzenia używane przez pakiet OFFICE, np. DOC/DOCX, XLS/XLSX, PPT/PPTX;
    b) pliki wykonywalne, np. EXE, DLL;
    c) inne, np. CHM, RAR, ACE, SCR, PDF, PUB, ZIP, MP3, 7Z, BZ, GZ, JAR, MHT, RTF, CAB.
7.13. Oprogramowanie musi zapewniać dostęp do sekwencyjnego (krok po kroku) zapisu zmian wykonywanych przez załącznik w środowisku wirtualnym co najmniej w rejestrze, procesach, systemie plików, sposobie startu systemu, próby nawiązania połączenia sieciowego (wraz z zapisem tych prób w postaci plików PCAP dostępnych w GUI Oprogramowania) oraz umożliwiać pobranie artefaktów z przeprowadzonej analizy co najmniej w zakresie analizowanej próbki.
7.14. Oprogramowanie musi posiadać mechanizm do wykrywania podszycia się pod inną osobę (na poziomie adresu email i wyświetlanej nazwy użytkownika oraz adresu email nadawcy i pola reply to).
7.15. Oprogramowanie musi posiadać dodatkowy mechanizm wykrywania zdarzeń tak zwanych "commodity malware", takich jak zaszyfrowane dokumenty, pliki wykonywalne, pliki z załączonymi obiektami, nietypowe rozszerzenia plików, wykorzystanie MagicBytes, przekierowania HTML w załączniku. Zdarzenia te powinny być konfigurowalne jako alert lub automatyczna kwarantanna.
7.16. Oprogramowanie musi posiadać dodatkowych mechanizm wykrywający obiekty lub zdarzenia, które mogą wskazywać, że są elementem ataku:
    a) skrypty przesyłane w wiadomości email;
    b) pliki wykonywalne przesyłane w załączniku lub URL;
    c) dokumentów MS OFFICE z zaimplementowanym makro lub kodem wykonywalnym;
    d) nietypowych załączników przesyłanych w wiadomości takich jak: BAT, CPL, LNK, COM, CMD, MHT, PIF, PUB, HLP, HTA, ISO;
    e) wiadomości email ze skróconymi linkami (tiny URL);
    f) dokumentów MS OFFICE z flash;
    g) plików JAR;
    h) haseł przesyłanych w treści wiadomości HTTP request;
    i) zaszyfrowanych plików PDF;
    j) pliki typu wygaszacz ekranu;
    k) nieznanych plików konfiguracyjnych .SettingContent-ms.
7.17. Oprogramowanie musi mieć możliwość przepisania nieznanych adresów URL w przesyłanej wiadomości, tak aby pomimo kliknięcia, użytkownik nie był przekierowany do potencjalnie złośliwej treści, a do strony producenta informującej (w języku polskim) o zablokowaniu tej komunikacji.
7.18. Oprogramowanie musi posiadać mechanizm ekstrakcji (rozpoznawania) adresów URL z załączników przesyłanych w wiadomości email i możliwość detonowania ich w środowisku wirtualnym w przypadku pliku zlokalizowanego w URL.
7.19. Oprogramowanie musi posiadać możliwość automatycznego generowania "screenshotów" stron phishingowych w przypadku wykrytego alertu.
7.20. Oprogramowanie musi umożliwiać konfigurację reguł bazujących na wyrażeniach regularnych w celu modyfikacji ochrony w zakresie: adresu e-mail nadawcy, domeny nadawcy, adresu e-mail odbiorcy, treści wiadomości i jej tytułu (zarówno whitelisty jak i blacklisty).

7.21. Oprogramowanie musi umożliwiać konfigurację reguł bazujących na wystąpieniu konkretnego nagłówka wiadomości oraz jego wartości i podejmować wskazaną akcję.
7.22. Oprogramowanie musi dla punktów 7.20 oraz 7.21 umożliwiać przeniesienie wiadomości do kwarantanny po jej skorelowaniu z regułami bezpieczeństwa.
7.23. Oprogramowanie musi mieć zaimplementowany mechanizm wyszukiwania analizowanych wiadomości pocztowych zawierający filtry wyszukujące co najmniej przy użyciu: adresu email odbiorcy, adresu email nadawcy, tematu wiadomości, nazwy załącznika. Niniejszy mechanizm musi umożliwiać wyszukiwanie wiadomości co najmniej do 30 dni wstecz.
7.24. Oprogramowanie musi analizować wiadomości email nawet po ich dostarczeniu i alertować o możliwej podmianie zawartości URL na złośliwą (analiza wsteczna).
7.25. Oprogramowanie musi umożliwiać wysyłanie alertów o zdarzeniach poprzez protokoły SMTP oraz RSYSLOG.
7.26. Oprogramowanie musi umożliwiać administratorom systemu pobranie wiadomości, która została zablokowana, jej wyświetlenie zarówno w formie sparsowanej, jak i tekstowo z uwzględnieniem jej nagłówków.
7.27. Oprogramowanie musi umożliwić ręczne zwalnianie zablokowanych wiadomości z kwarantanny przez administratorów systemu.
7.28. Oprogramowanie musi umożliwiać tworzenie dedykowanych pulpitów w GUI rozwiązania z możliwością dostosowania wyświetlanych informacji.
7.29. Oprogramowanie musi umożliwiać generowanie raportów zawierających co najmniej:
    a) statystyki wykrytych alertów z rozbiciem na kategorie zagrożenia (co najmniej spam, impersonation, viruses, itp.);
    b) statystyki przeanalizowanych wiadomości email;
    c) statystyki najpopularniejszych adresów email nadawców oraz adresów email odbiorców;
    d) statystyki formatów przeanalizowanych załączników.
7.30. Raporty muszą mieć możliwość eksportu do formatu CSV lub PDF wraz z możliwością ustalenia okresu czasu dla generowanego raportu (co najmniej ostatnie 24 godziny, ostatni 7 dni, ostatnie 30 dni).
7.31. Interfejs oprogramowania musi być w języku polskim lub angielskim.
7.32. Dostęp do oprogramowania musi być zabezpieczone kryptograficznie poprzez szyfrowanie komunikacji.
7.33. Oprogramowanie musi pozwalać na zdefiniowanie wielu administratorów o różnych poziomach uprawnień.

Pytanie nr 5

Zwracamy się z pytaniem dotyczącym opisu przedmiotu zamówienia pkt 6.4 c), 6.4 d), 7.2 f), 7.2 g)

Główną funkcjonalnością oferowanego Systemu jest analiza poczty pod względem zagrożeń typu APT (zaawansowane trwałe zagrożenia) z czego wynika fakt, że nie posiada wszystkich funkcjonalności typowych dla bramek AntySpam. Dobrą praktyką jest weryfikacja rekordów SPF, DKIM oraz DMARC i powinna być realizowana przez pierwszy system ochrony poczty w środowisku Zamawiającego (AntySpam).

Czy Zamawiający z uwagi na powyższe zgodzi się na dostarczenie Systemu nieposiadającego mechanizmów weryfikacji powyżej wskazanych rekordów?

Odpowiedź Zamawiającego:

Tak, Zamawijący wyraża zgodę na dostarczenie systemu nie posiadającego wszytskich funkcjonalności typowych dla bramek AntySpam wymienionych w powyższych punktach.
Zamawiający wprowadza zmiany w Szczegółowym Opisie Przedmiotu Zamówienia.
Zmiana punktów 6 i 7 tak jak w odpowiedzi na pytanie 4.

Pytanie nr 6

Zwracamy się z pytaniem dotyczącym opisu przedmiotu zamówienia pkt 6.3 e) i 6.4 h)

Oferowany System głównym swoim założeniem skupia się na ochronie poczty przed atakami typu APT, a funkcje AntySpam są jego dopełnieniem. Udzielenie dostępu do spersonalizowanej kwarantanny użytkownikom końcowym może prowadzić do dostarczenia zainfekowanej wiadomości do skrzynki odbiorczej.

Czy Zamawiający zgodzi się na zaakceptowanie Systemu nieposiadającego spersonalizowanej kwarantanny?

Odpowiedź Zamawiającego:

Tak, Zamawiający wyraża zgodę na dostarczenie Systemu nieposiadającego spersonalizowanej kwarantanny dla użytkowników.
Zamawiający wprowadza zmiany w Szczegółowym Opisie Przedmiotu Zamówienia.
Zmiana punktu 6 tak jak w odpowiedzi na pytanie 4.

Pytanie nr 7

Zwracamy się z pytaniem dotyczącym opisu przedmiotu zamówienia pkt 7.2 b)

Głównym założeniem oferowanego Systemu jest ochrona przed zagrożeniami typu APT oraz zapewnienie drugiego punktu ochrony ścieżki pocztowej Zamawiającego. Zgodnie z ogólnodostępną informacją potwierdzoną wynikami przetargu DSI-I.1333.18.2022 Zamawiający posiada rozwiązanie Barracuda Email Security Gateway realizujące funkcje AntySpam.

Czy Zamawiający zaakceptuje rozwiązanie przeznaczone do instalacji jako drugi lub kolejny system bezpieczeństwa poczty?

Odpowiedź Zamawiającego:

Tak, Zamawiający zaakceptuje takie rozwiązanie.
Zamawiający wprowadza zmiany w Szczegółowym Opisie Przedmiotu Zamówienia.
Zmiana punktu 7 tak jak w odpowiedzi na pytanie 4.

Pytanie nr 8

Zwracamy się z pytaniem dotyczącym opisu przedmiotu zamówienia pkt 7.2 d)

Z uwagi na spójność mechanizmów wykrywania w oferowanym Systemie, nie ma konieczności rozgraniczania polityk dla każdej z obsługiwanych domen pocztowych. Czy Zamawiający zaakceptuje System nieposiadający tej funkcjonalności?

Odpowiedź Zamawiającego:

Tak, Zamawiający zaakceptuje takie rozwiązanie.
Zamawiający wprowadza zmiany w Szczegółowym Opisie Przedmiotu Zamówienia.
Zmiana punktu 7 tak jak w odpowiedzi na pytanie 4.

Pytanie nr 9

Zwracamy się z pytaniem dotyczącym opisu przedmiotu zamówienia pkt 7.10

Z uwagi na fakt, że system Windows 11 charakteryzuje się dużą dynamiką wprowadzanych zmian w kolejnych jego wydaniach, co może prowadzić do wystąpień dużej ilości alertów False Positive podczas analizy dynamicznej, system Windows 11 nie został zaimplementowany do oferowanego rozwiązania przez jego Producenta.

Czy Zamawiający zaakceptuje rozwiązanie, które nie posiada obrazu systemu Windows 11 przeznaczonego do wykonywania analizy dynamicznej?

Odpowiedź Zamawiającego:

Tak, Zamawiający zaakceptuje takie rozwiązanie.
Zamawiający wprowadza zmiany w Szczegółowym Opisie Przedmiotu Zamówienia.
Zmiana punktu 7 tak jak w odpowiedzi na pytanie 4.

Pytanie nr 10

Zwracamy się z pytaniem dotyczącym opisu przedmiotu zamówienia pkt 7.20

Zgodnie z ogólnodostępną informacją potwierdzoną wynikami przetargu DSI-I.1333.18.2022 Zamawiający posiada rozwiązanie Barracuda Email Security Gateway realizujące funkcje AntySpam. Oferowany System przeznaczony jest do instalacji jako drugie rozwiązanie ochrony poczty w środowisku Zamawiającego. Z tego względu nie jest świadomy adresu IP oraz kraju nadawcy wiadomości. Czy Zamawiający zaakceptuje rozwiązanie umożliwiające konfigurację reguł bazujących na adresie e-mail nadawcy, domenie nadawcy, adresie e-mail odbiorcy, treści wiadomości i jej tytule?

Odpowiedź Zamawiającego:

Tak, Zamawiający zaakceptuje takie rozwiązanie.
Zamawiający wprowadza zmiany w Szczegółowym Opisie Przedmiotu Zamówienia.
Zmiana punktu 7 tak jak w odpowiedzi na pytanie 4.

Pytanie nr 11

Zwracamy się z pytaniem dotyczącym opisu przedmiotu zamówienia pkt 7.22

Czy Zamawiający zaakceptuje rozwiązanie, które umożliwia jedynie przeniesienie wiadomości do kwarantanny po jej skorelowaniu z regułami bezpieczeństwa?

Odpowiedź Zamawiającego:

Tak, Zamawiający zaakceptuje takie rozwiązanie.
Zamawiający wprowadza zmiany w Szczegółowym Opisie Przedmiotu Zamówienia.
Zmiana punktu 7 tak jak w odpowiedzi na pytanie 4.

Pytanie nr 12

Zwracamy się z pytaniem dotyczącym opisu przedmiotu zamówienia pkt 7.23

Czy Zamawiający zaakceptuje System, który umożliwia przeszukiwanie analizowanych mail po: adresie email odbiorcy, adresie email nadawcy, temacie wiadomości lub nazwie załącznika?

Czy Zamawiający zaakceptuje System, który posiada funkcjonalność dostarczania do zewnętrznego systemu klasy SIEM informacji takich jak: adres email odbiorcy, adres email nadawcy, temat wiadomości, nazwy załączników, MD5 oraz SHA256 załączniku, werdykt analizy?

Odpowiedź Zamawiającego:

Tak, Zamawiający zaakceptuje takie rozwiązanie.
Zamawiający wprowadza zmiany w Szczegółowym Opisie Przedmiotu Zamówienia.
Zmiana punktu 7 tak jak w odpowiedzi na pytanie 4.

Pytanie nr 13

Zwracamy się z pytaniem dotyczącym opisu przedmiotu zamówienia pkt 7.25, 7.26, 7.27

Głównym założeniem oferowanego Systemu jest ochrona przed atakami typu APT. Analiza incydentu wymaga posiadania wiedzy przez administratora/analityka z zakresu bezpieczeństwa, więc udzielenie dostępu do spersonalizowanej kwarantanny użytkownikom końcowym może prowadzić do dostarczenia zainfekowanej wiadomości do skrzynki odbiorczej.

Czy Zamawiający zaakceptuje System, który nie umożliwia dostępu do spersonalizowanej kwarantanny odbiorcy?

Odpowiedź Zamawiającego:

Tak, Zamawiający zaakceptuje takie rozwiązanie.
Zamawiający wprowadza zmiany w Szczegółowym Opisie Przedmiotu Zamówienia.
Zmiana punktu 7 tak jak w odpowiedzi na pytanie 4.

Pytanie nr 14

Zwracamy się z pytaniem dotyczącym opisu przedmiotu zamówienia pkt 7.32 c)

Zgodnie z ogólnodostępną informacją potwierdzoną wynikami przetargu DSI-I.1333.18.2022 Zamawiający posiada rozwiązanie Barracuda Email Security Gateway realizujące funkcje AntySpam. Oferowany System może zostać zainstalowany jako drugie lub kolejne rozwiązanie ochrony poczty w środowisku Zamawiającego, więc nie posiada adresów IP nadawców. Czy Zamawiający zaakceptuje takie rozwiązanie?

Odpowiedź Zamawiającego:

Tak, Zamawiający zaakceptuje takie rozwiązanie.
Zamawiający wprowadza zmiany w Szczegółowym Opisie Przedmiotu Zamówienia.
Zmiana punktu 7 tak jak w odpowiedzi na pytanie 4.

Pytanie nr 15

Zwracamy się z pytaniem dotyczącym opisu przedmiotu zamówienia pkt 7.32 e)

Czy Zamawiający zaakceptuje rozwiązanie przedstawiające wymienione statystki w sposób zbiorczy?

Odpowiedź Zamawiającego:

Tak, Zamawiający zaakceptuje takie rozwiązanie.
Zamawiający wprowadza zmiany w Szczegółowym Opisie Przedmiotu Zamówienia.
Zmiana punktu 7 tak jak w odpowiedzi na pytanie 4.

Pytanie nr 16

Zwracamy się z pytaniem czy Zamawiający wyrazi zgodę na modyfikacje zapisu w pkt 3.2 d) podpkt b)

W miejsce zapisu „Zamawiający może zawiesić czas usunięcia Awarii Niekrytycznej na maksymalnie 40 dni kalendarzowych, jeśli zachodzi potrzeba wydania poprawki producenta do Systemu, zawieszenie odbywa się na wniosek Wykonawcy złożony w formie elektronicznej lub papierowej.“

Wprowadzić zapis:

„W przypadku wystąpienia wady, usterki lub awarii oprogramowania wymagającej opracowania przez producenta zmian w oprogramowaniu (np. opracowanie zmian konfiguracyjnych pomiędzy komponentami oprogramowania, wydania przez producenta tzw. patch’a lub fix’a do oprogramowania lub innych zmian wymagających ingerencji producenta w kod źródłowy lub inne komponenty oprogramowania) naprawa oprogramowania procedowana jest zgodnie z warunkami serwisu gwarancyjnego producenta oprogramowania. W przypadku wystąpienia wady lub usterki lub awarii oprogramowania, Wykonawca zobowiązany jest do dołożenia należytej staranności mającej na celu niezwłoczne powiadomienie w tym:

a) zebrania i dostarczenia informacji jednostce wsparcia producenta oprogramowania;

b) monitorowania czasów odpowiedzi producenta oprogramowania oraz eskalacji opóźnień;

c) instalacji na środowiskach testowych poprawek (patchy) dostarczonych przez producenta oprogramowania (chyba że Zamawiający wskaże środowiska, na których instalacja będzie realizowana bezpośrednio przez Zamawiającego);

d) testowania poprawek dostarczonych przez producenta oprogramowania;"

Uzasadnienie:

Wykonawca nie jest producentem oferowanego oprogramowania i nie ma wpływu na terminy realizacji i wprowadzania poprawek przez producenta. Warunki realizacji wprowadzania zmian są opisane w dokumentacji producenta.

Odpowiedź Zamawiającego:

Tak, Zamawiający zaakceptuje zmiany zapisów w Szczegółowym Opisie Przedmiotu Zamówienia.
Zamawiający wprowadza zmiany w Szczegółowym Opisie Przedmiotu Zamówienia.
Zmiana z:

3.2. Klasyfikowanie, diagnozowanie oraz rozwiązywanie błędów zgłaszanych przez administratorów Systemu:

a) fakt wystąpienia błędu, oraz jego ewentualną charakterystykę, ocenia się zawsze w odniesieniu do ostatniej wersji opisu funkcjonalnego Systemu, uzgodnionej pomiędzy Zamawiającym a Wykonawcą;

b) przez rozwiązanie błędu lub ostateczne rozwiązanie błędu, rozumie się wdrożenie działań, dzięki którym dany błąd przestaje występować podczas zgodnego z przeznaczeniem korzystania z funkcji Systemu;

c) przez obejście błędu rozumie się przekazanie do wiadomości Zamawiającego lub administratora Systemu szczegółowego opisu działań, dzięki którym procedury użycia Systemu, będące normalnie pod wpływem danego błędu, mogą zostać przeprowadzone w sposób wykluczający powstanie lub wpływ tego błędu;

d) w ramach udzielonej gwarancji, wsparcia i asysty technicznej, Wykonawca będzie realizował zgłoszenia serwisowe awarii Systemu w następujący sposób:

   a) Awaria Krytyczna - wada skutkująca nieprawidłowym działaniem Systemu powodująca albo całkowity brak możliwości korzystania z Systemu przez co najmniej jednego użytkownika końcowego albo takie ograniczenie możliwości korzystania z niego, że przestaje on spełniać swoje podstawowe funkcje. Czas Reakcji: do 4 godzin od chwili zgłoszenia serwisowego przez Zamawiającego, Czas Naprawy: do 24 godzin od chwili zgłoszenia serwisowego przez Zamawiającego;

   b) Awaria Niekrytyczna – wada skutkująca nieprawidłowym działaniem Systemu powodująca ograniczenie korzystania z Systemu, nie powodując skutków opisanych dla Awarii Krytycznej: Czas Reakcji: do 4 godzin od chwili zgłoszenia serwisowego przez Zamawiającego, Czas Naprawy: do 72 godzin od chwili zgłoszenia serwisowego przez Zamawiającego.

   Zamawiający może zawiesić czas usunięcia Awarii Niekrytycznej na maksymalnie 40 dni kalendarzowych, jeśli zachodzi potrzeba wydania poprawki producenta do Systemu, zawieszenie odbywa się na wniosek Wykonawcy złożony w formie elektronicznej lub papierowej.

e) przez reakcję rozumie się dowolny sposób komunikacji ze strony przedstawiciela Wykonawcy, potwierdzający przyjęcie zgłoszenia oraz rozpoczęcie działań diagnostycznych;

f) gdy zgłoszenia dokonano poza godzinami pracy Zamawiającego, zgłoszenie traktowane jest jako przyjęte o godzinie 7:30 wraz z rozpoczęciem najbliższego dnia roboczego Zamawiającego (**nie dotyczy awarii krytycznych**);

g) w wyjątkowych wypadkach, za zgodą Zamawiającego czas realizacji przywrócenia pełnej funkcjonalności Systemu (rozwiązanie lub obejście awarii) lub termin ostatecznego rozwiązania problemu, może zostać uzgodniony pomiędzy Wykonawcą i Zamawiającym i tym samym różnić się od wartości parametrów czasowych opisanych powyżej.

na:

3.2. Klasyfikowanie, diagnozowanie oraz rozwiązywanie błędów zgłaszanych przez administratorów Systemu:

a) fakt wystąpienia błędu, oraz jego ewentualną charakterystykę, ocenia się zawsze w odniesieniu do ostatniej wersji opisu funkcjonalnego Systemu, uzgodnionej pomiędzy Zamawiającym a Wykonawcą;

b) przez rozwiązanie błędu lub ostateczne rozwiązanie błędu, rozumie się wdrożenie działań, dzięki którym dany błąd przestaje występować podczas zgodnego z przeznaczeniem korzystania z funkcji Systemu;

c) przez obejście błędu rozumie się przekazanie do wiadomości Zamawiającego lub administratora Systemu szczegółowego opisu działań, dzięki którym procedury użycia Systemu, będące normalnie pod wpływem danego błędu, mogą zostać przeprowadzone w sposób wykluczający powstanie lub wpływ tego błędu;

d) w ramach udzielonej gwarancji, wsparcia i asysty technicznej, Wykonawca będzie realizował zgłoszenia serwisowe awarii Systemu w następujący sposób:

   i. Awaria Krytyczna - wada skutkująca nieprawidłowym działaniem Systemu powodująca albo całkowity brak możliwości korzystania z Systemu przez co najmniej jednego użytkownika końcowego albo takie ograniczenie możliwości korzystania z niego, że przestaje on spełniać swoje podstawowe funkcje. Czas Reakcji: do 4 godzin od chwili zgłoszenia serwisowego przez Zamawiającego, Czas Naprawy: do 24 godzin od chwili zgłoszenia serwisowego przez Zamawiającego;

   ii. Awaria Niekrytyczna – wada skutkująca nieprawidłowym działaniem Systemu powodująca ograniczenie korzystania z Systemu, nie powodując skutków opisanych dla Awarii Krytycznej: Czas Reakcji: do 4 godzin od chwili zgłoszenia serwisowego przez Zamawiającego, Czas Naprawy: do 72 godzin od chwili zgłoszenia serwisowego przez Zamawiającego.

e) w przypadku wystąpienia wady, usterki lub awarii oprogramowania wymagającej opracowania przez producenta zmian w oprogramowaniu (np. opracowanie zmian konfiguracyjnych pomiędzy komponentami oprogramowania, wydania przez producenta tzw. patch'a lub fix'a do oprogramowania lub innych zmian wymagających ingerencji producenta w kod źródłowy lub inne komponenty oprogramowania) naprawa oprogramowania procedowana jest zgodnie z warunkami serwisu gwarancyjnego producenta oprogramowania. W przypadku wystąpienia wady lub usterki lub awarii oprogramowania, Wykonawca zobowiązany jest do dołożenia należytej staranności mającej na celu niezwłoczne powiadomienie w tym:

   i. niezwłocznego poinformowania Zamawiającego o wystąpieniu tego rodzaju wady, usterki lub awarii oprogramowania;

   ii. zebrania i dostarczenia informacji jednostce wsparcia producenta oprogramowania;

   iii. monitorowania czasów odpowiedzi producenta oprogramowania oraz eskalacji opóźnień;

   iv. instalacji na środowiskach testowych poprawek (patchy) dostarczonych przez producenta oprogramowania (chyba że Zamawiający wskaże środowiska, na których instalacja będzie realizowana bezpośrednio przez Zamawiającego);

   v. testowania poprawek dostarczonych przez producenta oprogramowania.

f) przez reakcję rozumie się dowolny sposób komunikacji ze strony przedstawiciela Wykonawcy, potwierdzający przyjęcie zgłoszenia oraz rozpoczęcie działań diagnostycznych;

g) gdy zgłoszenia dokonano poza godzinami pracy Zamawiającego, zgłoszenie traktowane jest jako przyjęte o godzinie 7:30 wraz z rozpoczęciem najbliższego dnia roboczego Zamawiającego (**nie dotyczy awarii krytycznych**);

h) w wyjątkowych wypadkach, za zgodą Zamawiającego czas realizacji przywrócenia pełnej funkcjonalności Systemu (rozwiązanie lub obejście awarii) lub termin ostatecznego rozwiązania problemu, może zostać uzgodniony pomiędzy Wykonawcą i Zamawiającym i tym samym różnić się od wartości parametrów czasowych opisanych powyżej.

Pytanie nr 17

Zamawiający w postępowaniu BZP.272.26.2023.AR w punkcie 7.9 Szczegółowego Opisu Przedmiotu Zamówienia wskazuje, że „Oprogramowanie musi umożliwiać deszyfrację załączników w oparciu o hasło odczytane z obrazu graficznego (OCR) przesłanego w tej samej wiadomości”. Czy Zamawiający dopuszcza oprogramowanie nie spełniające tego zapisu? Pozwoli to zaproponować rozwiązanie konkurencyjne cenowo.

Odpowiedź Zamawiającego:

Zamawiający nie dopuszcza oprogramowania nie spełniającego tego zapisu.

Pytanie nr 18

Zamawiający w postępowaniu BZP.272.26.2023.AR w punkcie 7.9 Szczegółowego Opisu Przedmiotu Zamówienia wskazuje, że „Oprogramowanie musi posiadać środowiska wirtualne służące do analizy zagrożeń co najmniej w systemach operacyjnych: Windows 7, Windows 10, Windows 11, MacOS i Linux. Maszyny wirtualne muszą być aktualizowane przez producenta oraz nie mogą wymagać posiadania dodatkowych licencji przez Zamawiającego.”. Czy Zamawiający dopuszcza rozwiązanie, które na dzień składania oferty nie będzie jeszcze zawierało wsparcia dla systemu Windows 11, ale wspiera wszystkie pozostałe wymagane przez Zamawiającego systemy, a dodatkowo systemy Windows 8.1 oraz Android.

Odpowiedź Zamawiającego:

Tak, Zamawiający dopuszcza takie rozwiązanie. Powyższy opis jest zawarty w punkcie 7.10 a nie Zamawiający wprowadza zmiany w Szczegółowym Opisie Przedmiotu Zamówienia

Zmiana punktu 7.10 z:

7.10 Oprogramowanie musi posiadać środowiska wirtualne służące do analizy zagrożeń co najmniej w systemach operacyjnych: Windows 7, Windows 10, Windows 11, MacOS i Linux. Maszyny wirtualne muszą być aktualizowane przez producenta oraz nie mogą wymagać posiadania dodatkowych licencji przez Zamawiającego.

na:

7.10 Oprogramowanie musi posiadać środowiska wirtualne służące do analizy zagrożeń co najmniej w systemach operacyjnych: Windows 7, Windows 10, MacOS i Linux. Maszyny wirtualne muszą być aktualizowane przez producenta oraz nie mogą wymagać posiadania dodatkowych licencji przez Zamawiającego.

Pytanie nr 19

Zamawiający w postępowaniu BZP.272.26.2023.AR w punkcie 7.15 Szczegółowego Opisu Przedmiotu Zamówienia wskazuje, że „Oprogramowanie musi posiadać dodatkowy mechanizm wykrywania zdarzeń tak zwanych "commodity malware", takich jak zaszyfrowane dokumenty, pliki wykonywalne, pliki z załączonymi obiektami, nietypowe rozszerzenia plików, wykorzystanie MagicBytes, przekierowania HTML w załączniku. Zdarzenia te powinny być konfigurowalne jako alert lub automatyczna kwarantanna.”. Prosimy o doprecyzowanie, o jakie dokładnie formularze HTTP_request oraz przekierowania HTML w załączniku chodzi i przykładowe zastosowanie lub o zrezygnowanie z tych zapisów.

Odpowiedź Zamawiającego:

Zamawiający wyjaśnia – „przekierowania HTML w załączniku” to jakiekolwiek linki znajdujące się w załącznikach widomości email, przenoszące użytkownika we wskazane w linku miejsce. Zapis „formularz HTTP_request” zostaje usunięty.

Zamawiający wprowadza zmiany w Szczegółowym Opisie Przedmiotu Zamówienia.

Zmiana punktu 7.15 z:

7.15 Oprogramowanie musi posiadać dodatkowy mechanizm wykrywania zdarzeń tak zwanych "commodity malware", takich jak zaszyfrowane dokumenty, pliki wykonywalne, pliki z załączonymi obiektami, nietypowe rozszerzenia plików, formularz HTTP_request, wykorzystanie MagicBytes, przekierowania HTML w załączniku. Zdarzenia te powinny być konfigurowalne jako alert lub automatyczna kwarantanna.

na:

7.15 Oprogramowanie musi posiadać dodatkowy mechanizm wykrywania zdarzeń tak zwanych "commodity malware", takich jak zaszyfrowane dokumenty, pliki wykonywalne, pliki z załączonymi obiektami, nietypowe rozszerzenia plików, wykorzystanie MagicBytes, przekierowania HTML w załączniku. Zdarzenia te powinny być konfigurowalne jako alert lub automatyczna kwarantanna.

Pytanie nr 20

Zamawiający w postępowaniu BZP.272.26.2023.AR w punkcie 7.24 Szczegółowego Opisu Przedmiotu Zamówienia wskazuje, że „Oprogramowanie musi analizować wiadomości email nawet po ich dostarczeniu i alertować o możliwej podmianie zawartości URL na złośliwą (analiza wsteczna).”. Czy Zmawiający w powyższym zapisie oczekuje rozwiązania analizującego zmiany zawartości URL w momencie kliknięcia linku we wiadomości mailowej przez użytkownika?

Odpowiedź Zamawiającego:

Rozwiązanie analizujące zmianę zawartości URL może być realizowane zarówno w momencie kliknięcia linku w wiadomości jak i cyklicznie realizowane przez samo oprogramowanie.

W związku z wprowadzonymi zmianami w opisie przedmiotu zamówienia oraz we wzorze umowy Zamawiający załącza aktualny opz oraz wzór umowy.

z up. MARSZAŁKA WOJEWÓDZTWA
Marian Malinowski
Dyrektor Biura Zamówień Publicznych
/podpisano elektronicznie/