Opis przedmiotu zamówienia

Projekt pn.: „Zwiększenie poziomu cyberbezpieczeństwa JST w Gminie Krzanowice" realizowany jest w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa.

1. Przedmiot zamówienia obejmuje zakup i dostawę zgodnie z zestawieniem opisanym w ust. 7, które opisuje wymagania Zamawiającego dot. przedmiotu zamówienia pn. „Zwiększenie poziomu cyberbezpieczeństwa JST w Gminie Krzanowice" - etap 2 dostawa sprzętu IT.
2. Sprzęt musi być kompletny, wolny od wad fizycznych (m.in. konstrukcyjnych, materiałowych, wykonawczych, technicznych) oraz prawnych, spełniającym poniższe wymagania przy czym Zamawiający dopuszcza złożenie oferty z wyposażeniem lepszym od wymagań minimalnych przedstawionych w ust. 7.
3. Przedmiot zamówienia powinien odpowiadać obowiązującym normom, parametrom technicznym, jakościowym, posiadać niezbędne homologacje i certyfikat zgodności CE lub równoważny.
4. Przedmiot zamówienia powinien być kompletnie wyposażony we wszystkie komponenty standardowo dostarczane przez producenta również niewymienione w SWZ przez Zamawiającego.
5. Parametry określone w ust. 7 stanowią minimum jakie musi spełnić oferowany przedmiot zamówienia. W przypadku gdy oferowany przedmiot zamówienia posiadał będzie parametry mniejsze od ustalonych jako minimalne, oferta Wykonawcy zostanie odrzucona jako nie spełniająca wymogów SWZ.
6. Zamawiający, oprócz zakupu i dostawy, wskazuje następujące wymagania dotyczące realizacji zamówienia.
   a) zamówienie obejmuje transport (na koszt i ryzyko Wykonawcy);
   b) za termin wykonania dostawy przyjmuje się przekazanie kompletnego, sprawnego sprzętu stanowiących przedmiot zamówienia;
   c) jeśli dostarczony sprzęt lub jego elementy są uszkodzone lub uległy uszkodzeniu podczas transportu, zostaną przez Wykonawcę wymienione na nowe lub naprawione przed zgłoszeniem zakończenia dostaw do odbioru;
   d) Wykonawca jest odpowiedzialny za zabezpieczenie dostarczonego sprzętu do czasu dokonania pisemnego odbioru końcowego /bez uwag/ potwierdzonego przez osoby odpowiedzialne ze strony Zamawiającego.
7. Charakterystyka techniczna:

I. Router sieciowy klasy UTM

a. Specyfikacja sprzętowa:

i. Parametry sprzętowe:

1. Interfejsy w pełni konfigurowalne (brak stałego przypisania roli portu do WAN/LAN);
2. 8 interfejsów 1Gb + 1 port USB 3.0 z możliwością obsadzenia w urządzenie pamięci masowej do przechowywania dzienników zdarzeń (event logs);
3. Interfejs konsoli lokalnej RJ-45;

ii. Wydajność:

1. Przepustowość zapory ogniowej SPI mierzona w standardzie RFC 2544 (pakiety 1,518 bajtów UDP): co najmniej 3,9Gbps;
2. Przepustowość VPN mierzona w standardzie RFC2544 (1,424 bajtów UDP): co najmniej 0,8Gbps;
3. Przepustowość modułu anti-malware (w trybie uproszczonym lub pełnym) mierzona w standardzie wydajności HTTP (pakiety 1460 bajtów HTTP z zastosowaniem wielu strumieni): co najmniej 0,9Gbps;
4. Przepustowość modułu IPS mierzona w standardzie wydajności HTTP (pakiety 1460 bajtów HTTP z zastosowaniem wielu strumieni): co najmniej 1,4Gbps;
5. Przepustowość łączona IPS wraz z Anti-Malware mierzona w standardzie wydajności HTTP (pakiety 1460 bajtów HTTP z zastosowaniem wielu strumieni): co najmniej 0,9Gbps;
6. Maksymalna łączna ilość nawiązanych sesji TCP mierzona oprogramowaniem IXIA IxLoad: co najmniej 0,3mln sesji;
7. Maksymalna jednoczesna ilość połączeń IPSec VPN bez względu na rodzaj – brama-brama, klient-brama: co najmniej 45 sesji;
8. Maksymalna jednoczesna ilość połączeń SSL VPN: co najmniej 20 połączeń;
9. Minimalna ilość obsługiwanych interfejsów VLAN: co najmniej 16 interfejsów;
10. Niezawodność mierzona parametrem MTBF określonym przez producenta na poziomie co najmniej 580000 godzin przy temperaturze co najmniej 25^{o}C;

iii. Monitorowanie:

1. Wykresy przepustowości interfejsów sieciowych oraz interfejsów VLAN na osi czasu (co najmniej 24 godzinnej);
2. Informacja tekstowa lub graficzna o alokacji zasobów sprzętowych urządzenia tj. obciążenia procesora CPU, zajęcie pamięci operacyjnej, wykorzystanie sesji, zajętość pamięci nieulotnej;
3. Informacja tekstowa i/lub graficzna wskazująca na utylizację przepustowości przez mechanizm:
    a. Analizy warstwy aplikacji;
    b. Określonego hosta w sieci wewnętrznej;
    c. Interfejs sieciowy;

d. Monitoring sesji NAT z typem usługi, IP inicjującym, IP docelowym oraz informacją o użytkowniku nawiązującym dane połączenia (np. w przypadku stosowania połączenia VPN przez użytkownika);

4. Statystyki wyświetlające efekty działania skanerów:
   a. Skanowania zawartości (Content Filtering);
   b. Filtra reputacji (IP/DNS/URL);
   c. Modułu IPS;
   d. Modułu anti-malware;
   e. Modułu inspekcji SSL;
   f. Modułu Sandboxingu;
5. Monitoring interfejsów sieciowych z następującymi informacjami:
   a. Typ interfejsu (WAN/LAN);
   b. Przypisanie typu interfejsu do fizycznego portu urządzenia;
   c. Przepustowość interfejsu;
   d. Rodzaj interfejsu LAN/WAN/VLAN;
   e. Adresacja routera przypisana na tym interfejsie (WAN/LAN/VLAN) wraz z numerem interfejsu VLAN jeżeli dotyczy (VLAN Tag);
6. Wizualizacja danych pasywnego skanera sieci:
   a. Adres MAC urządzenia;
   b. Adres IP;
   c. Nazwa hosta;
   d. Wykrycie w interfejsie LAN/VLAN;
   e. Typ urządzenia (komputer, urządzenie mobilne itp.);
   f. Wykryty system operacyjny;
   g. Data ostatniej detekcji w sieci wewnętrznej;
7. Lista użytkowników połączonych z urządzeniem w zakresie:
   a. Połączenia HTTP/HTTPS zarządzania;
   b. Połączeń VPN z tym połączenia VPN;
   c. Przypisany adres IP w sieci wewnętrznej w przypadku tunelowania połączenia VPN (mapowany adres);
   d. Adres IP hosta łączącego zdalnie np. poprzez VPN;
8. Tablica adresów serwera DHCP zawierająca:
   a. Przypisany interfejs LAN/VLAN;
   b. Przydzielony adres IP;
   c. Nazwa hosta;
   d. Wykryty adres MAC;
   e. Stan przypisania adresu (rezerwacja stała, dzierżawa);
   f. Funkcjonalność eksportu listy do pliku tekstowego;
9. Monitorowanie połączeń VPN:

a. Nazwa użytkownika;
b. Przypisany adres IP;
c. Zdalny adres IP inicjatora;
d. Czas sesji VPN;
e. Ilość wysłanych oraz odebranych danych;

10. Stan licencji z podziałem na typ licencji, datę wygaśnięcia licencji oraz stan aktywacji;
11. Wyświetlanie informacji o ostatniej aktualizacji sygnatur bezpieczeństwa dotycząca modułów wymagających synchronizacji z chmurą producenta, zawierająca informację o dacie publikacji sygnatur oraz dacie ich aktualizacji przez urządzenie;
12. Monitorowanie urządzenia za pomocą protokołu SNMPv2, v3 (z szyfrowaniem);

iv. Funkcjonalność podstawowa

1. Routing, wsparcie dla protokołów Ethernet oraz PPPoE dla portów WAN.
2. Trasowanie statyczne;
3. Trasowanie dynamiczne oparte na identyfikacji hosta/użytkownika w sieci wewnętrznej oparte m.in. na kryteriach:
   a. Użytkownik (obiekt/grupa);
   b. Okienko czasowe – harmonogram (obiekt/grupa);
   c. Źródło połączenia (obiekt/grupa);
   d. Cel połączenia (obiekt/grupa);
   e. Typ usługi / protokołu (obiekt/grupa);
   f. Port źródłowy (obiekt/grupa);
4. Trasowanie oparte o polisy NAT/SNAT;
5. Funkcjonalność DHCP (server, klient, relay);
6. Wsparcie dla protokołu DDNS (Dynamic DNS);
7. Rozkładanie obciążenia interfejsów WAN, przełączanie między WAN w przypadku awarii, zarządzanie przepustowością opartą na priorytetach;
8. Dziennik zdarzeń wewnętrzny (w pamięci ulotnej), zewnętrzny (przechowywany na nośniku USB), zdalny – sieciowy (komunikacja z co najmniej dwoma niezależnymi serwerami SYSLOG o różnej konfiguracji w zakresie poziomu przesyłanych zdarzeń. Dla każdego typu odbiorcy dzienników (wewnętrzny/USB/zdalny) istnieje możliwość ustalenia kategorii przesyłanych danych opartych na kryteriach:
   a. Wybór poziomu przesyłanych zdarzeń typu:
      i. Brak
      ii. Standardowe informacje
      iii. Informacje typu debug
   b. Ustalenie kategorii przesyłanych zdarzeń:
      i. Autoryzacja;

ii. Bezpieczeństwo;
iii. Systemowe;
iv. Usługi ochrony;
v. VPN;
vi. Licencje;
vii. Sieć;

9. Aktualizacja oprogramowania układowego poprzez załadowanie pliku z firmware lub bezpośrednio przez urządzenie z chmury producenta;
10. Możliwość ustalenia automatycznego harmonogramu instalowania aktualizacji firmware;
11. Możliwość przechowywania co najmniej dwóch różnych konfiguracji urządzenia w pamięci nieulotnej urządzenia.
12. Zastosowanie technologii podwójnego obrazu firmware;
13. Autoryzacja logowania do panelu zarządzania urządzenia oraz komunikacji VPN na podstawie wbudowanej bazy danych użytkowników lub synchronizowana z bazy zewnętrznej.
14. Zarządzanie urządzeniem za pomocą HTTPS, SSH, portem konsoli.
15. Wbudowane narzędzia diagnostyczne polegające na:
    a. Przechwytywaniu pakietów w oparciu o wybrany interfejs sieciowy, podsieć VLAN, określony adres IP, usługę, port na wbudowanej pamięci flash, nośnik USB lub na serwer FTP;
    b. Opcja pobrania dzienników systemowych (system log) przechowywanych w pamięci flash urządzenia;
    c. Wbudowane narzędzia NSLookup IPv4, PING IPv4, Traceroute IPv4, IPSec Trace Log;

v. Funkcjonalność z zakresu bezpieczeństwa:

1. Zapora ogniowa, routing, bridge, SPI, NAT Travelsar, ALG, Anti-DOS, możliwość importu zewnętrznych list IP/DNS do modułu blokad zapory ogniowej;
2. Polisy bezpieczeństwa wsparcie dla filtrowania zawartości (content filtering), monitoring warstwy aplikacyjnej, inspekcja pakietów SSL, ustalanie budowy polis bezpieczeństwa opartych na:
    a. Źródle (strefa - obiekt);
    b. Destynacji (strefa – obiekt);
    c. Inicjatorze (obiekt/grupa);
    d. Cel (obiekt/grupa);
    e. Usługa (obiekt/grupa);
    f. Użytkownik (obiekt/grupa);
    g. Czas (harmonogram – obiekt/grupa);
    h. Typ akcji;

i. Logowanie operacji (nie/tak/tak z ostrzeżeniem);
j. Przypisanie dodatkowych mechanizmów bezpieczeństwa do danej polisy:
   i. Kontrola warstwy aplikacji;
   ii. Filtrowanie zawartości DNS/URL/IP;
   iii. Inspekcja SSL;

3. Mechanizm zapobiegania podszywania się pod adres IP znanych urządzeń (IP/MAC Spoofing) obsługujący adresy IP przydzielone poprzez serwer DHCP urządzenia oraz adresy przypisane statycznie. Analiza odbywa się na zasadzie korelacji określonego adresu IP w połączeniu z adresem MAC. Istnieje możliwość zastosowania wyjątku dla określonych adresów IP które będą wyłączone z skanowania;
4. Moduł IPS bazujący m.in. na skanowaniu na podstawie sygnatur z możliwością stosowania białej i czarnej listy. Analizujący dane pod kątem zawartych w nich exploitów, ataków XSS lub SQL Injection.
5. Analityka warstwy aplikacyjnej pakietów IP umożliwiająca tworzenie reguł bezpieczeństwa opartych o komunikację danej aplikacji. Lista aplikacji z podziałem na kategorie i aktualizowana z bazą danych producenta w celu zachowania jej aktualności. Istnieje możliwość wyświetlenia statystyk komunikacyjnych dotyczących danej aplikacji.
6. Filtr przeciwdziałający szkodliwemu oprogramowaniu – Anti-Malware analizujący plik wg rozszerzeń, identyfikatorów szkodliwego oprogramowania (znanych cechach identyfikujących);
7. Sandboxing bazujący na chmurze producenta skanujący podejrzane pliki, synchronizujący sygnatury z chmurą producenta;
8. Filtr Reputacyjny adresów IP, nazw DNS oraz adresów URL polegający na oznaczaniu jako niebezpieczne adresów IP, nazw DNS oraz adresów URL klasyfikowanych i przechowywanych w usłudze producenta urządzenia z której korzysta router podczas pracy w przypadku aktywacji usługi na danej regule bezpieczeństwa. Filtr podzielony jest na kategorie aktualizowane przez producenta w ramach aktualizacji sygnatur. Wsparcia dla białej i czarnej listy określanej przez administratora. Analityka dla ruchu przychodzącego lub wychodzącego. Filtr może być zasilany zewnętrzną listą adresów publikowaną poprzez protokół HTTP z możliwością ustawienia interwału automatycznej aktualizacji.
9. Możliwość utworzenia białej/czarnej listy destynacji DNS/URL w celu całkowitego zablokowania komunikacji internetowej i dopuszczenia tylko do określonych destynacji;
10. Możliwość przekierowania wywołania dla zablokowanej strony internetowej na określoną w panelu konfiguracyjną stronę informacyjną.
11. Możliwość zmiany portów usług HTTP/HTTPS, SSH, FTP, SSL VPN;

12. Wysyłanie powiadomień poprzez wiadomość e-mail za pomocą autoryzowanego konta SMTP i z wsparciem szyfrowania TLS;
13. Możliwość konfiguracji co dziennego raportu o określonej godzinie zawierającego podstawowe informacje, m.in. zajętość procesora, pamięci operacyjnej, utylizacji przepustowości, stanu mechanizmów bezpieczeństwa (IPS, Anti-Malware, filt reputacji) z ich wykryciami, tablicą adresów DHCP w poszczególnych sieciach LAN/VLAN. Wizualizacja w formie wykresów lub tabel.
14. Możliwość konfiguracji automatycznego wykonywania kopii konfiguracji oraz wysyłki na wskazane adresy e-mail w określonym dniu, godzinie lub miesiącu.
15. Inspekcja SSL, głęboka analityka pakietów TLS (w tym TLS 1.3), możliwość blokowania certyfikatów uznanych za niezaufane, integracja modułu z mechanizmami IPS, Anti-Malware, Sandboxing, analityka aplikacji oraz filtrowanie ruchu HTTP/HTTPS.
16. Możliwość wygenerowania certyfikatu self-signed oraz importu gotowego certyfikatu z przydzieleniem funkcjonalności – autoryzacja serwera, autoryzacja klienta, certyfikat IKE (Key-Exchange);
17. Kontrola nad zachowaniem usług DoH – DNS over HTTPS w celu umożliwienia korzystania z usługi przez klientów sieci lub jej zablokowania;
18. Wbudowany skaner infrastruktury wewnętrznej polegający na pasywnym analizowaniu ruchu sieciowego oraz kategoryzowaniu urządzeń na elementy infrastruktury klienckiej, sieciowej, bezprzewodowej itp.
19. Tworzenie reguł zawierających klasyfikację celów i destynacji opartych o geolokalizację z możliwością stosowaniu reguł w oparciu co najmniej o kraj lub kontynent. Możliwość tworzenia grupy krajów i korzystania z niej w polisach bezpieczeństwa.
20. Możliwość wykluczania określonych adresów IP z filtrowania IPS, Anti-Malware, filtrowania DNS/URL.
21. Wsparcie dla protokołu IPSec VPN, SSL VPN z wsparciem dla tworzenia profili kompatybilnych z oprogramowaniem OpenVPN oraz konfiguracją kompatybilną z oprogramowaniem wbudowanym w systemie Windows. Wsparcie dla protokołów IKEv2, MS-CHAPv2, EAP, DES, 3DES, AES (256), MD5, SHA2, SHA2 (512). Grupy DH 2, 5, 14-16, 19-20, 28-30. Autoryzacja bazująca na certyfikatach PKI lub kluczach tekstowych (PSK). Wsparcie dla PFS, IPSSec NAT-T, DPD (Dead Peer Detection). Dla protokołu SSL obsługa trybu Full oraz Split tunelu VPN. Wsparcie dla autoryzacji 2FA opartej co najmniej o aplikację Google Authentication oraz Microsoft Authenticator. Możliwość określania routingu klienta VPN polegającego na maskowaniu adresu IP VPN klienta w sieci wewnętrznej i jego translację do określonego adresu IP w danym segmencie sieci/podsieci.

22. Wszystkie moduły bezpieczeństwa aktualizowane są wg zadanego w panelu administracyjnym interwału jednakże czas ten musi umożliwiać aktualizację w interwałach co najmniej 24 godzin;

b. **Licencje -** urządzenie dostarczone z licencjami na łączny okres 24 miesięcy obejmującymi wszystkie funkcjonalności opisane w specyfikacji urządzenia oraz jego mechanizmów zabezpieczających;

c. **Gwarancja producenta:** 60 miesięcy;

II. Przełącznik sieciowy – zarządzalny PoE

a. Parametry techniczne:

i. Typ przełącznika: SMART, zarządzalny;
ii. Łączna liczba portów: minimum 28 portów;
iii. Ilość portów 100/1000Mbps Ethernet – miedzianych – minimum 24 w tym 24 porty PoE 802.3af/at;
iv. Budżet mocy PoE 8023.af/at przełącznika sieciowego: minimum 370W;
v. Ilość portów 10Gigabit Ethernet – światłowodowych typu SFP+ - minimum 4 sztuki;
vi. Przepustowość magistrali wewnętrznej: minimum 120 Gigabitów/sekundę;
vii. Tablica adresów MAC: 15000 wpisów;
viii. Napięcie wejściowe: 220 - 240V/AC 50/60Hz;
ix. Wysokość instalacyjna RACK: 19” 1U;
x. Czas bezawaryjnej pracy (parametr MTBF): minimum 750000 godzin;
xi. Konfiguracja: minimum poprzez przeglądarkę WWW z użyciem protokołu SSL, opcjonalnie poprzez interfejs Telnet;
xii. Konfiguracja: możliwość importu oraz eksportu konfiguracji do pliku;
xiii. Ustawianie czasu wewnętrznego urządzenia w oparciu o serwer czasu: NTP lub SNTP;
xiv. Aktualizacja firmware urządzenia: poprzez przeglądarkę WWW, FTP;
xv. Obsługa wkładek w slotach SFP+: jedno oraz wielomodowych o przepustowościach 1Gbps oraz 10Gbps działających na dystansach minimum 250m dla światłowodów wielomodowych oraz minimum 8km dla światłowodów jedno-modowych. Wsparcie dla kabli DAC (Direct Attach Cable) o przepustowościach do 10Gbps;
xvi. Wymagane wsparcie dla protokołów: IEEE 802.3z 1000BASE-X, IEEE 802.3ab 1000BASE-T Ethernet, , IEEE 802.3ae 10 Gbit/s Ethernet, IEEE 802.3ad LACP aggregation, IEEE 802.1D Spanning Tree Protocol (STP), IEEE 802.1w Rapid Spanning Tree Protocol (RSTP), IEEE 802.1s Multiple Spanning Tree Protocol (MSTP), IEEE 802.1X port authentication, ochrona przed pętlą w sieci LAN, 802.1Q – statyczne oraz dynamiczne VLAN, PVID VLAN, VLAN TAG, VLAN Trunking, SYSLOG IPv4, SNMP (v1,v2c, v3), SNMP trap, RMON;

b. Gwarancja producenta: „do końca życia produktu” co oznacza że podlega ciągłej gwarancji producenta oraz 60-cio miesięcznej gwarancji producenta od publikacji informacji o zakończeniu produkcji modelu urządzenia;

III. Urządzenie pamięci masowej NAS

a. Parametry techniczne:

i. Procesor: dwu-rdzeniowy o taktowaniu bazowym minimum 2,0GHz z sprzętowym wsparciem szyfrowania AES-NI i wydajnością na poziomie minimum 2900 pkt., wg testów wydajności opublikowanych na stronie internetowej https://www.cpubenchmark.net/cpu_list.php;

ii. Pamięć operacyjna: minimum 2GB DDR4 SODIMM z możliwością rozbudowy o dodatkowy moduł pamięci operacyjnej;

iii. Obsługiwane dyski twarde: minimum 4 dyski twardych 3,5” lub 2,5”, kompatybilność z dyskami twardymi HDD oraz SSD. Każdy z dysków umieszczony w kieszeni umożliwiającej wyciągnięcie dysku podczas pracy urządzenia „na gorąco” (hot-plug) bez dodatkowych narzędzi;

iv. Obsadzenie dysków twardych: minimum 2 dyski HDD w formacie 3,5” o pojemności minimum 8TB, prędkości obrotowej 7200 obr./min. w pełni kompatybilne z oferowaną macierzą dyskową oraz wykazane na liście kompatybilności z możliwością aktualizacji oprogramowania układowego dysku twardego z poziomu konsoli zarządzania pamięcią masową;

v. Porty zewnętrzne: minimum 2 porty USB 3.2 1-wszej generacji;

vi. Obudowa: obudowa stojąca typu desktop;

vii. Interfejsy LAN Ethernet: minimum 1 porty LAN Ethernet 1Gbps oraz 1 port LAN Ethernet 2,5Gbps;

viii. Zaplanowane włączanie oraz wyłączanie wg ustalonego harmonogramu: dostępne;

ix. Zasilanie wejściowe: 230V/AC w zasilaczem wbudowanym lub zewnętrznym;

x. Funkcjonalność programowa dostępna bez konieczności zakupu dodatkowych licencji:

xi. Funkcjonalność ustalania limitów przydzielonych zasobów plikowych (tzw. quota) dla udostępnianych zasobów plikowych;

xii. Wewnętrzne mechanizmy analizujące stan pamięci masowej, jej podzespołów oraz stan działania macierzy RAID skonfigurowanej w serwerze macierzy dyskowej wraz z raportowaniem stanu poprzez protokół SNMP, oraz powiadomienia e-mail do wyznaczonych odbiorców;

xiii. Możliwość monitorowania dostępności aktualizacji firmware poprzez protokół SNMP;

xiv. Wsparcie dla przesyłania dzienników do zewnętrznego systemu logowania opartego o SYSLOG;

xv. Technologia migawek danych zawartych na pamięci masowej - folderów współdzielonych, partycji utworzonych przez użytkownika lub zbiorów danych np. jednostek LUN, umożliwiająca w zależności od typu przechowywanych danych (plików, folderów, obrazów dysków wirtualnych) przywracanie poszczególnych plików lub folderów z danego zakresu czasowego, objętego migawką. Migawki wykonywane

według ustalonego harmonogramu umożliwiającego ustalenie precyzji do dnia, godziny, minuty z konfigurowalną powtarzalnością w ciągu dnia, tygodnia, miesiąca;

xvi. Funkcjonalność polegająca na instalacji oprogramowania agentowego na stacjach roboczych oraz serwerach pracujących pod kontrolą m.in. systemu Microsoft Windows oraz Linux, polegająca na ustalaniu harmonogramu wykonywania kopii zapasowych wyznaczonych plików oraz folderów z przestrzeni dyskowej klienta oprogramowania wraz z możliwością tworzenia pełnych obrazów dysku twardego komputera klienckiego umożliwiające odtworzenia klienta oprogramowania w trybie „bare-metal" wraz z funkcjonalnością przygotowania środowiska odzyskiwania służącego przeprowadzeniu procesu odtworzenia kopii dysku twardego w trybie „bare-metal". Wymagana jest obsługa wykonywania migawek przy użyciu Volume Shadow Copy lub innego rozwiązania producenta, realizującego tą samą funkcję – wykonanie kopii danych które są w użyciu;

xvii. Funkcjonalność polegająca na wykonywaniu replikacji poza zasoby pamięci masowej wcześniej wykonanych migawek na urządzeniu w celu zapewnienia możliwości ich odtworzenia w przypadku krytycznej awarii pamięci masowej i potrzeby jej wymiany na nowy egzemplarz;

xviii. Funkcjonalność tworzenia kompletnej kopii danych zawartych na pamięci masowej wraz z aplikacjami zainstalowanymi w obrębie pamięci masowej w wybranej przestrzeni dyskowej – lokalnej (osobnej macierzy RAID lub na nośniku USB) lub zdalnej za pomocą protokołu SMB bądź FTP;

xix. Wszystkie procesy kopii zapasowych oraz migawek posiadają możliwość konfiguracji okresu przechowywania, opartego co najmniej o wartość liczbową ilości ostatnio wykonanych kopii;

xx. Wspierane protokoły sieciowe (co najmniej): SNMP, SSH, iSCSI, FTP, NFS, SMB;

xxi. Zewnętrzne systemu plików (co najmniej) – np. poprzez podłączenie nośnika USB: BTFRS, EXT4, EXT3, FAT32, exFAT, NTFS, NFS+;

xxii. Obsługiwane typy wewnętrznej macierzy dyskowej (RAID) (co najmniej): RAID0, RAID1, RAID10, RAID5, RAID6;

xxiii. Maksymalny rozmiar pojedynczego woluminu: minimum 80TB;

xxiv. Maksymalna liczba migawek systemu: minimum 80;

xxv. Maksymalna liczba połączeń sieciowych SMB: minimum 8;

xxvi. Wsparcie dla kontroli uprawnień systemu plików NTFS poprzez listy ACL: dostępne;

xxvii. Wsparcie dla tworzenia oraz udostępniania zasobów sieciowych za pomocą protokołu plików SMB/CIFS w środowiskach domenowych Active Directory z rozpoznawaniem oraz ustawianiem uprawnień dostępu ACL systemu plików NTFS oraz uwierzytelnianiem przy pomocy aktywnych serwerów Active Directory Services: TAK:

xxviii. Wbudowana zapora ogniowa (Firewall), konfigurowalna dla konkretnego interfejsu sieciowego z regułami ustawianymi na poziomie usług oraz portów z rozróżnieniem ruchu TCP/UDP oraz przychodzącego adresu IP, grupy adresów lub podsieci;

xxix. Wsparcie dla segmentacji sieci LAN poprzez ustawienie identyfikatora VLAN TAG dla interfejsu sieciowego;

xxx. Zarządzanie oraz konfiguracja urządzenia za pomocą protokołu HTTP, HTTPS, opcjonalnie SSH;

xxxi. Wsparcie dla zasilaczy awaryjnych UPS podłączonych za pomocą interfejsu USB, „zasilacz awaryjny UPS o mocy pozornej 750VA – TYP A" wykazany na liście kompatybilności pamięci masowej;

b. **Gwarancja producenta na pamięć masową:** 36 miesięcy;

c. **Gwarancja producenta na dyski HDD:** 36 miesięcy;

IV. Zasilacz awaryjny UPS o mocy pozornej 750VA – TYP A

a. Parametry techniczne:

i. Napięcie wejściowe: 220 - 240V/AC 50/60Hz;
ii. Napięcie wyjściowe: 220-240V;
iii. Moc znamionowa: 500W;
iv. Wejście zasilania: IEC 320 C14;
v. Wyjścia zasilania: minimum 6x IEC 320 C13;
vi. Typ obudowy: Tower – stojąca;
vii. Czas podtrzymania bateryjnego przy obciążeniu 100W: minimum 45 minut;
viii. Czas podtrzymania bateryjnego przy obciążeniu 200W: minimum 20 minut;
ix. Czas podtrzymania bateryjnego przy obciążeniu 300W: minimum 11 minut;
x. Topologia UPS-a: Line-Interactive;
xi. Typ przebiegu wyjściowego podczas zasilania bateryjnego: Sinusoida;
xii. Interfejsy komunikacyjne: USB, RS-232, Ethernet;
xiii. Zarządzanie przez panel LCD z przyciskami sterującymi umożliwiający weryfikację podstawowych parametrów pracy (m.in. obciążenia, czasu podtrzymania akumulatorowego, napięcie wejściowe, wyjściowe, uruchomienie procedury diagnostycznej, stanu naładowania akumulatorów);
xiv. Funkcjonalność oprogramowania instalowanego w systemie operacyjnym: komunikacja przy użyciu portu komunikacyjnego USB musi posiadać możliwość pracy w trybie usługi pod kontrolą systemu Windows lub Linux co wiąże się z jego automatycznym uruchomieniem podczas startu systemu operacyjnego oraz rozpoczęciu komunikacji z zasilaczem awaryjnym. Dostęp do aplikacji chroniony poprzez login oraz hasło ustawiane podczas instalacji lub po pierwszym uruchomieniu. Konfiguracja aplikacji poprzez interfejs WWW udostępniany przez usługę pracującą w tle z możliwością zarządzania zasilaczem awaryjnym, podgląd stanu obciążenia oraz szacowanego czasu podtrzymania, przeglądanie dzienników historycznych pracy urządzenia w tym stanów odnotowanych w dzienniku zdarzeń (np. zanik zasilania, powrót zasilania), konfiguracja grup wyjść zasilania, czasów opóźnień oraz sposobu działania w wypadku utraty zasilania sieciowego. Możliwość konfiguracji skryptu .bat/.sh (w zależności od systemu operacyjnego) wywoływanego w sytuacji zaniku zasilania oraz doprowadzenia do określonego poziomu naładowania baterii lub pozostałego czasu podtrzymania zasilania; Możliwość ustawienia opóźnienia uruchomienia UPS-a w postaci interwału czasowego lub określonego poziomu naładowania baterii.
xv. Funkcjonalność portu Ethernet: komunikacja bezpośrednio z chmurą producenta z możliwością konfigurowania powiadomień generowanych przez urządzenie i przesyłanych przez system producenta do administratora w postaci wiadomości e-mail;

b. Gwarancja producenta na elektronikę zasilacza: 36 miesięcy;

c. Gwarancja producenta na pakiet bateryjny: 24 miesiące;

V. Serwer obliczeniowy

a. Parametry techniczne:

i. Format obudowy: desktop, stojąca lub leżąca;
ii. Porty USB: z przodu 2 porty USB 3.2 Type-A, z tyłu 4 porty USB 3.2 Type-A;
iii. Złącza wideo: VGA, DisplayPort;
iv. Port RS-232: 1 sztuka;
v. Interfejsy sieciowe: 4 porty 1Gbps RJ45;
vi. Interfejsy diagnostyczne (sieciowe): 1 port 1Gbps RJ45;
vii. Zasilacz: wewnętrzny lub zewnętrzy 230V/AC;
viii. Złącza M.2: pojedynczy wewnętrzny port M.2;
ix. Ilość złączy pamięci RAM: 4 gniazda DDR5
x. Moduł TPM 2.0: wbudowany;
xi. Sloty PCI-E: 2 sloty PCI-E x8;
xii. Procesor: Czterordzeniowy, INTEL Xeon E2434 lub równoważny o wydajności co najmniej 14800 punktów wg testów wydajności opublikowanych na stronie internetowej https://www.cpubenchmark.net/cpu_list.php;
xiii. Pamięć operacyjna: 32GB DDR5;
xiv. Kontroler pamięci masowej RAID: zainstalowany w slocie PCI-E, obsługa co najmniej macierzy typu RAID 1, 0, 1+0;
xv. Obsadzenie dysków twardych:
    1. Dyski SSD: 2 dyski 960GB SSD SATA 2,5” obsadzone w adapterach z formatu 2,5” do 3,5”, zainstalowane wewnątrz serwera i w pełni kompatybilne z zaproponowanym urządzeniem;
    2. Dyski HDD: 2 dyski 4TB HDD SATA 3,5” w pełni kompatybilne z zaproponowanym urządzeniem;
xvi. Sygnalizacja diodowa: sygnalizacja diodowa stanu serwera (wykrycia nieprawidłowej pracy komponentów) zlokalizowana z przodu obudowy;
xvii. Konfiguracja systemu oraz inne parametry: wsparcie dla uruchomienia typu Secure Boot, wbudowany interfejs zarządzania UEFI SHELL, graficzna konfiguracja BIOS/UEFI włącznie z konfiguracją kontrolera pamięci masowej łącznie z tworzeniem oraz konfiguracją macierzy dyskowych na wbudowanych dyskach HDD/SSD. Konfiguracja graficzna karty zarządzania w zakresie podstawowych parametrów pracy m.in. konfiguracji adresu IP;
xviii. Interfejs zarządzania oraz diagnostyki: Zarządzanie co najmniej poprzez HTTPS oraz SSH z wsparciem dla segmentacji sieci VLAN;
xix. Zakres funkcjonalny interfejsu zarządzania: Dostępność interfejsu oraz interakcja z serwerem w sytuacji wyłączenia serwera ale z podłączonym zasilaniem sieciowym AC. Możliwość włączenia, wyłączenia oraz restartu serwera. Możliwość interakcji z systemem operacyjnym zainstalowanym na serwerze równoważny z pracą za pomocą

podłączonego monitora, klawiatury oraz myszy (IP-KVM) wraz z przekazywaniem wybranego urządzenia pamięci masowej USB między komputerem zarządzającym a serwerem zarządzanym. Zapewniona funkcjonalność raportowania poprzez mechanizm SYSLOG oraz powiadomienia e-mail. Możliwość wygenerowania dzienników diagnostycznych w formacie kompatybilnym z systemem diagnostycznym producenta, umożliwiającym zdalną diagnostykę przebiegu pracy serwera oraz komponentów które uległy awarii. Raportowanie kompletnego wyposażenia sprzętowego wraz z określeniem poprawności pracy komponentu. Autoryzacja dostępu do interfejsu zarządzania za pomocą tworzonych użytkowników wraz z określeniem poziomu dostępu do elementów interfejsu diagnostycznego. Funkcjonalność wykonywania aktualizacji oprogramowania sprzętowego komponentów serwera a także aktualizacji oprogramowania oraz sterowników na poziomie zainstalowanego systemu operacyjnego poprzez oprogramowanie realizujące synchronizację komunikacji pomiędzy układem zarządzania a systemem operacyjnym w celu dokonania aktualizacji;

xx. Diagnostyka serwera w czasie rzeczywistym: realizowana co najmniej za pomocą protokołów SNMP w wersji minimum SNMPv2. Protokół SNMP przekazujący do systemu monitorowania co najmniej następujące parametry:
    1. Stan interfejsów sieciowych – podłączony, odłączony wraz z aktualną przepustowością;
    2. Obsadzenie slotów pamięci operacyjnej RAM wraz z stanem działania;
    3. Stan działania wentylatorów;
    4. Informacja o temperaturze serwera w różnych obszarach wnętrza oraz temperaturą otoczenia (Ambient);
    5. Stan obsadzenia dyskami twardymi wraz z stanem pracy – poprawny, awaria;
xxi. Licencje programowe dostarczone z serwerem:
    1. Microsoft Windows Server Essentials 2025;
xxii. Wirtualizacja: serwer wspiera wirtualizację oraz producent deklaruje wsparcie wirtualizacji dla systemów z rodziny Microsoft Windows oraz VMWare ESXi, RedHat Enterprise Linux;
xxiii. Wsparcie serwisowe, aktualizacje: producent zapewnia stronę internetową dedykowaną dla serwera z filtrowaniem do numeru seryjnego urządzenia na której zawarte są aktualizację dla komponentów sprzętowych oraz programowych zgodnych z wyposażeniem serwera. Ponad to producent dystrybuuje aktualizacje zbiorcze w postaci pakietów serwisowych które uruchamiane są z poziomu systemu operacyjnej lub w trybie offline poprzez rozruch serwera z obrazu ISO załadowanego lokalnie lub zdalnie. Pakiety serwisowe zapewniają aktualizację sterowników, oprogramowania oraz pakietów oprogramowania sprzętowego (firmware) w przypadku uruchomienia pakietu w systemie operacyjnym lub aktualizacje oprogramowania sprzętowego (firmware) w przypadku uruchomienia pakietu serwisowego w trybie offline tzn. z nośnika ISO/USB;

b. **Gwarancja producenta:** Gwarancja producenta na okres 36 miesięcy z możliwością przedłużania pakietami serwisowymi producenta do minimum 7 lat obejmująca wszystkie zainstalowane komponenty serwera (w tym dyski twarde oraz karty sieciowe) w całym okresie trwania gwarancji. W ramach usług gwarancyjnych producent serwera zapewnia:
   i. Dostęp telefoniczny do ekspertów;
   ii. Czat z ekspertami na żywo;
   iii. Całodobowy dostęp do funkcji samoobsługi i samodzielnego rozwiązywania problemów online;
   iv. Całodobowe rejestrowanie zdarzeń;
   v. Zdalna diagnoza problemu i wsparcie;
   vi. Wsparcie dla sprzętu w miejscu instalacji;
   vii. Przesyłanie dzienników diagnostycznych w ramach prowadzonej sprawy dotyczącej usterki;
   viii. Części zamienne i materiały;
   ix. 2-godzinny czas reakcji na zgłoszenie w godzinach od 9:00 do 17:00 w dni robocze;
   x. Przybycie na miejsce w celu dokonania naprawy przez autoryzowanego przedstawiciela serwisu producenta w następnym dniu roboczym w przypadku dostępności części w magazynie serwisu producenta;
   xi. W uzasadnionych przypadkach, możliwa wysyłka części z magazynu producenta w celu dokonania naprawy samodzielnej przez klienta;
   xii. Możliwość rozbudowy gwarancji podstawowej do wyższych poziomów zapewniających wsparcie serwisu 24 godziny na dobę, 7 dni w tygodniu z czasami reakcji serwisu z naprawą poniżej 24 godzin;

VI. Rozszerzenie licencji oprogramowania do inwentaryzacji zasobów informatycznych oraz oprogramowania kryptograficzno-analitycznego

a. Zakres funkcjonalny

i. Analiza e-mail – monitorowanie wiadomości przesyłanych za pomocą poczty e-mail, blokowanie przesyłania plików, alarmy, powiadomienia, wyzwalanie akcji na podstawie kryteriów, logi zdarzeń;

ii. Analiza usług przechowywania w chmurze – monitorowanie danych przesyłanych do chmury, blokowanie dostępu, alarmy, powiadomienia, wyzwalanie akcji na podstawie kryteriów, logi zdarzeń;

iii. Analiza danych w ruchu, plików – monitorowanie i blokowanie operacji na plikach, utworzenie, otwarcie, usunięcie, zmiana nazwy;

b. Licencjonowanie:

i. Licencja w pełni kompatybilna i rozszerzająca istniejący system BTC eAuditor, nie dopuszcza się zaoferowania innego produktu niż rozszerzenie istniejącej licencji przez oficjalny kanał dystrybucji producenta;

ii. Kompatybilny moduł: Ochrony danych w ruchu (DR);

iii. Ilość stanowisk: rozszerzenie z 50 do 60 stanowisk;

c. Uwagi:

i. Rozszerzenie licencji potwierdzone certyfikatem wystawionym przez producenta systemu;

VII. Aktywny skaner podatności

a. Zarys funkcjonalny:

i. Moduł skanowania w sieci TCP/IP realizowany za pomocą sondy dystrybuowanej jako maszyna wirtualna. Skanowanie wskazanych adresów IP lub nazw domenowych w sieci wewnętrznej polegający na wykrywaniu usług sieciowych publikowanych przez dany adres IP oraz próba identyfikacji występujących podatności w tychże usługach. W zależności od typu skanowanej usługi oraz zastosowanego protokołu pobierane są informacje m.in. o wersji zastosowanego oprogramowania (np. w przypadku serwisów wbudowanych WEB urządzeń typu IoT) oraz identyfikowane w ten sposób możliwe podatności zidentyfikowane w bazie CVE (Common Vulnerabilities and Exposures);

ii. Moduł skanowania oraz analizy platform WEB: skanowanie wskazanych nazw serwisów WWW polegający na analizie publikowanych usług, określaniu ich wersji oraz potencjalnych lub bezpieczeństwa wynikających z zastosowanej wersji serwera web-owego, silnika bazodanowego itp. mechanizmów komponujących serwis webowy;

iii. Testy penetracyjne świadomości (awarness) oraz wyłudzeń (phishing): moduł polegający na zautomatyzowanym przesyłaniu do wybranej grupy użytkowników wiadomości spreparowanych w taki sposób aby skłaniały użytkownika do podjęcia określonych działań lub kliknięcia w wskazane LINK-i w wiadomości e-mail. Moduł ma polegać na tworzenia szablonu oraz grupy dystrybucyjnych do których kierowane są treści potencjalnie w ich obszarze zainteresowania i pracy, próbujące wymusić określone, niepożądane zachowania. Moduł ma za zadanie trenować oraz weryfikować stan wiedzy użytkowników końcowych tym samym wskazywać potencjalne punkty na które należy zwrócić większa uwagę podczas szkoleń z zakresu cyberbezpieczeństwa dla użytkowników końcowych;

b. Zarządzanie podatnościami:

i. Platforma zarządzania podatnościami musi być w stanie zapewnić funkcje pulpitu nawigacyjnego (i konfigurowalne) z następującymi widżetami:

1. Wyniki skanowania podatności sieci według ważności (z opcjami wykresu: słupkowy i kołowy);
2. Wyniki skanowania podatności aplikacji internetowych według ważności (z opcjami wykresu: słupkowy i kołowy);
3. Otwarte zgłoszenia według ważności (z opcjami wykresu: słupkowy i kołowy);
4. Top 10 wyników skanowania sieci (dostępna opcja ustawienia celu zasobu jako wszystkich lub wybranych adresów IP/tagów);
5. 10 największych podatności w aplikacjach sieciowych (dostępna opcja ustawienia celu zasobu jako wszystkie lub wybrane aplikacje sieciowe/etykiety);
6. Zgodność z OWASP (z opcjami wykresów: słupkowy i kołowy oraz dostępną opcją ustawienia dla wszystkich lub wybranych aplikacji internetowych);
7. Ostatnie skanowania;

8. Nadchodzące skanowania;
9. Ostatnie 10 raportów;
10. Liczba podatności w zabezpieczeniach w czasie (dostępna opcja ustawienia celu zasobu jako wszystkich lub wybranych aplikacji IPS/web/tagów wraz z ustawieniem czasu, aby ustawić czas trwania i interwał);
11. Ocena wyników kampanii phishingowych;
12. Ciągłe monitorowanie alertów (dostępna opcja ustawienia okresu na dzień/tydzień;

ii. Platforma zarządzania podatnościami musi mieć możliwość sortowania, grupowania i priorytetyzacji podatności:

1. Możliwość tworzenia wielu zakładek w celu filtrowania następujących kryteriów:
   a. Według stanu: wszystkie, nie ignorowane/wyłączone i ignorowane/wyłączone;
   b. Według typu: host i aplikacja internetowa;
   c. Według statusu: nowy, aktywny, ponownie otwarty, naprawiony;
   d. Według ważności: informacja, niski, średni, wysoki, krytyczny;
   e. Według tagów (opcja uwzględnienia/wykluczenia tagu);
   f. Według pierwszego i ostatniego wykrycia;
   g. Według kategorii: podatności w skanowaniu sieci i podatności w aplikacjach internetowych;
2. Możliwość filtrowania listy podatności według podatności lub aplikacji internetowych/hosta;
3. Możliwość tworzenia raportów bezpośrednio z menedżera podatności poprzez wybranie jednej lub więcej podatności;
4. Możliwość dalszego administrowania/zarządzania listą luk w zabezpieczeniach za pomocą następujących funkcji:
   a. Co ignorować: wyłącz tę podatność dla wszystkich hostów/aplikacji internetowych i ignoruj tę podatność;
   b. Powód ignorowania: fałszywie dodatni, ryzyko zaakceptowane, nieistotny;
   c. Opcja ustawienia czasu wygaśnięcia dla ignorowanych podatności;
5. Możliwość tworzenia notatek do celów uwag i notatek, które pojawią się w raporcie po jego wygenerowaniu;
6. Opcja wyświetlania następujących informacji na temat podatności:
   a. Wpływ;
   b. Rozwiązanie;
   c. Podsumowanie;
   d. Wgląd;
   e. Wykrywanie;
   f. Odniesienie;
   g. Łatki;
   h. Środki zaradcze;

iii. Platforma zawiera wbudowany system ticketowy dla procesu naprawczego.

iv. Platforma zapewnia możliwość dostarczania informacji o zgłoszeniach takich jak:

1. Numerowanie ich w celu łatwego śledzenia i powiadamiania za pośrednictwem poczty elektronicznej;
2. Możliwość podawania i aktualizowania statusu zgłoszenia, takiego jak: otwarte, zamknięte lub rozwiązane;
3. Możliwość podania nazwy powiązanej podatności w zabezpieczeniach wraz z jej zasobami
4. Możliwość podania wagi podatności w zabezpieczeniach zarejestrowanego zgłoszenia
5. Możliwość przypisania do wyznaczonego właściciela i terminu
6. Możliwość tworzenia wielu zakładek do utrzymywania i zarządzania zgłoszeniami zgodnie z poniższymi zasadami:
   a. Status;
   b. Typ zasobu;
   c. Kategoria usługi;
   d. Tagi;
   e. Termin;
   f. Kategoria skanowania sieci i aplikacji internetowych;
   g. Istotność;
   h. System operacyjny;
   i. Porty;
   j. Możliwość zapewnienia proaktywnej obsługi zgłoszeń;

v. Platforma musi zapewniać możliwość uruchomienia ciągłego monitorowania oraz ustawiania profili monitorowania zmian za pomocą powiadomień i alarmów;

vi. Menadżer podatności musi zapewniać możliwość utworzenia własnych widoków podatności zapewniających odfiltrowane rekordy zgodnie z konfiguracją użytkownika;

vii. Menadżer podatności musi zapewniać funkcję ignorowania wykrytych podatności wg zadanego okresu czasowego;

c. System raportujący:

i. Skanowanie sieci - raport;

ii. Aplikacje sieciowe - raport;

iii. Aktualizacje / łatki / poprawki - raport;

iv. Środki zaradcze - raport;

v. Ocena phisingu e-mail - raport;

vi. Porównanie raportów;

vii. Raporty zgodności wg następujących kryteriów;

1. OWASP Top 10;
2. ISO/IEC 27001;

3. Ogólne rozporządzenie o ochronie danych;
4. Bezpieczeństwo sieci i informacji;
5. Ustawa o ochronie danych osobowych;

viii. System powinien mieć możliwość importu nowych typów raportów w ramach udostępniania ich przez producenta;

ix. System powinien mieć możliwość tworzenia i dostosowywania raportów na podstawie następujących kryteriów:

1. Raport oparty na określonym czasie skanowania;
2. Raport oparty na wszystkich bieżących informacjach o podatnościach;
3. Raport trendów z historią podatności;
4. Zzawartość raportu: szczegóły raportu, przegląd podatności, podsumowanie podatności, lista podatności (według podatności i hosta) z opcjami wglądu, podsumowania, wykrywania, odniesień i ograniczenia tekstu;
5. Sposób prezentacji raportu: podatności według ważności w czasie, podatności według statusu, podatności według ważności, 5 najbardziej narażonych kategorii;
6. filtrowanie: selektywne raportowanie podatności (pełne i niestandardowe) i wykluczenia, uwzględnione systemy operacyjne, filtry zasobów, filtry podatności;

x. Funkcjonalność tworzenia raportów skróconych posiadających formę podsumowania o określonym interwale powiadomień np. tygodniowe, miesięczne poprzez wysyłkę e-mail na określony adres;

d. Licencjonowanie:

i. Czas trwania licencji: 24 miesiące;

ii. Zakres licencjonowania:

1. Moduł skanowania w sieci TCP/IP:
   a. 25 stanowisk IP - urządzeń końcowych (switche, routery, punkty WiFi, urządzenia IoT oraz inne urządzenia IP) skanowane w warstwie protokołów sieciowych (m.in. TCP/IP, ICMP itd.);
2. Moduł skanowania oraz analizy platform WEB:
   a. 2 licencje skanowania aplikacji typu WEB (strony Internetowe) pod kątem wykrywania podatności w zastosowanych rozwiązaniach informatycznych (np. serwer WEB, bazy MsSQL / MariaDB itp.);
3. Testy penetracyjne świadomości (awarness) oraz wyłudzeń (phishing):
   a. 32 stanowiska pracownicze podlegające testom socjotechnicznym, testom phishingowy, świadomości w przestrzeni informatycznej wobec których będą realizowane zautomatyzowane ataki sprawdzające poziom kompetencji;

e. Zakres usługowy:

i. Wykonawca instaluje oprogramowanie na dedykowanej maszynie wirtualnej nie wymagającej dodatkowego licencjonowania (płatnego systemu operacyjnego) oraz po uruchomieniu modułów monitorowania dostępnych w dostarczonym oprogramowaniu,

dokonuje przeszkolenia informatyka jednostki w zakresie obsługi oraz analizy rejestrowanych danych;

f. Wsparcie techniczne:

1. Wykonawca zapewnia wsparcie technicznie przez cały okres licencjonowania w dni robocze w godzinach od 8:00 do 16:00 w zakresie wyjaśnień dotyczących funkcjonalności systemu, wsparcia w jego konfiguracji oraz realizacji zgłoszonych usterek technicznych bez ograniczenia liczby zgłoszeń oraz czasu realizacji;
2. Wsparcie polega na analizie w siedzibie Zamawiającego lub za pomocą udostępnionego przez informatyka Urzędu kanału zdalnego zgłoszonego problemu technicznego;
3. Czas reakcji od przyjęcia zgłoszenia do fizycznego rozpoczęcia prac w konsultacji z informatykiem Urzędu nie może przekraczać 24 godzin;
4. Jeżeli rozwiązanie problemu technicznego nie może zostać zrealizowane w przeciągu 24 godzin od zgłoszenia usterki, wymagane jest powiadomienie informatyka Urzędu o charakterze usterki, podjętych w międzyczasie pracach wraz z uzasadnieniem;

VIII. Usługa serwera pocztowego w infrastrukturze technicznej Zamawiającego

a. Zarys funkcjonalny: serwer pocztowy instalowany w infrastrukturze Zamawiającego w postaci maszyny wirtualnej zapewniający obsługę poczty elektronicznej e-mail z wsparciem dla protokołów POP3S/SMTPS/IMAPS oraz ActiveSync Exchange w celu synchronizacji kontaktów oraz kalendarzy danego użytkownika z serwerem oraz programami pocztowymi a także wspieranymi urządzeniami mobilnymi. Serwer pocztowy musi zapewniać pełną obsługę wszystkich standardowych protokołów zabezpieczeń SSL/TLS oraz DKIM. Użytkownicy mogą korzystać z serwera pocztowego za pomocą aplikacji tradycyjnych typu desktop/mobile (np. Thunderbird, Outlook) oraz za pomocą klienta WWW wspierającego autoryzację dwuskładnikową 2FA za pomocą bezpłatnie dostępnych narzędzi bazujących na mechanizmie TOTP. Serwer pocztowy musi posiadać wsparcie integracji z usługami antywirusowymi oraz anti-spam opierającymi się na rozwiązaniu producenta serwera pocztowego objętych zakupioną licencją na system pocztowy.

b. Zakres funkcjonalny:

i. Pakiety instalacyjne dostępne dla platform Microsoft Windows Server 2019+ oraz Windows 11, dystrybucji LINUX (RedHat, CentOS, Oracle Linux, Rocky Linux, Ubuntu, Debian) oraz w postaci kontenerów DOCKER;

ii. Wsparcie dla środowisk klastrowania: Windows Fileover Cluster, RedHat Clustering Suite,

iii. Możliwość ustawienia limitu objętości skrzynki e-mail, rozmiaru załączników, rozmiaru objętości całej wiadomości, czasu nieaktywności sesji, ilości wysłanych wiadomości w przeciągu 60 minut oraz filtrowania wiadomości HTML;

iv. Wielowarstwowe funkcje filtrowania wiadomości e-mail na poziomie serwera, domeny, użytkownika poprzez konfigurowanie filtrów, określanie ich kolejności wykonywania oraz określania zadań do wykonania na podstawie wyników filtrowania.

v. Skanowanie wiadomości odbywa się poprzez weryfikację rekordów SPF, filtrowanie antywirusowe, weryfikację w oparciu o listy anty-spam, weryfikację DMARC (połączenie DKIM i SPF). Istnieje możliwość integracji oprogramowania z otwartymi modułami takimi jak SpamAssassin, Rpamd, ClamAV lub innymi mechanizmami posiadającymi interfejs API dzięki językowi skryptowemu umożliwiającemu tworzenie połączeń z systemami zewnętrznymi;

vi. Funkcjonalność klastrowania umożliwiająca delegację zadań serwera pocztowego do różnych instancji maszyn wirtualnych w zakresie obsługi SMTP, serwera WEB, POP lub IMAP;

vii. Zarządzanie administracyjne oraz funkcje: zarządzanie poprzez serwis WWW, automatyzacja operacji za pomocą poleceń CLI lub API, możliwość ustawienia stałej sesji Administracyjnej (bez automatycznego wylogowania), tworzenie wysyłki masowej na poziomie domeny/serwera/grupy użytkowników, powiadomienia o przekroczeniu przydzielonych limitów (np. konta), automatyzacja czyszczenia kosza oraz folderu SPAM,

tworzenie losowych haseł dla nowo tworzonych kont użytkowników, wymuszenie polityki bezpieczeństwa haseł (ilość znaków, typy znaków), automatyzacja tworzenia kont na podstawie kont Active Directory, możliwość stosowania certyfikatów Let's Encrypt oraz automatyzacja ich instalacji, możliwość instalowania w panelu zarządzania własnych komponentów graficznych (np. LOGO), zarządzanie certyfikatami SSL (instalacja własnych certyfikatów SSL, odnawianie, tworzenie i odnowienie certyfikatów Let's Encrypt), włączenie wymuszenia stosowania autoryzacji 2FA dla użytkowników domeny na poziomie każdego użytkownika;

viii. Kategoryzacja użytkowników: możliwość przydzielania ograniczeń dotyczących kont e-mail bazujących na grupach lub indywidualnych użytkownikach, możliwość określenia przyjmowania lub wysyłania wiadomości do określonej grupy odbiorców lub nadawców, określenia grup ograniczeń przydziałów dyskowych z możliwością ręcznego nadpisania dla danego użytkownika uprawnień dziedziczonych z grupy;

ix. Inteligentne przetwarzania wiadomości przychodzących polegające na kolejkowaniu na bazie domeny nadawcy wiadomości oraz nakładaniu filtrów wiadomości;

x. Określanie polityk ponawiania połączeń dotyczących wysyłanych wiadomości pocztowych na wypadek niedostępności usług np. sieci Internet dla serwera pocztowego;

xi. Wbudowany cache nazw DNS oraz możliwość przydzielania odmiennych zewnętrznych adresów IP którymi prezentuje się serwer dla różnych domen zaparkowanych w usłudze;

xii. Raportowanie i statystyki zawierające m.in.: statystyki serwera (obciążenie, zajętość), statystyki utylizacji interfejsów sieciowych, wykresy graficzne, szczegółowe raporty zużycia przestrzeni dyskowej wraz z funkcjonalnością przekazywania danych za pomocą metryk SNMP;

xiii. Archiwizacja dzienników zdarzeń na określonych poziomach ważności z podziałem na usługi wewnętrzne;

xiv. Możliwość rozszerzania dostępnej powierzchni dyskowej przydzielonej dla systemu, funkcjonalność deduplikacji wiadomości pocztowych (w przypadku wysyłania tej samej wiadomości do wielu odbiorców z wnętrza domeny);

xv. Funkcjonalność dla użytkownika końcowego – użytkownika konta pocztowego:

1. Klient WEB HTML5 w wersji dla urządzeń desktop oraz wersja mobilna;
2. Książka adresowa: kontakty, grupy, listy dystrybucyjne (osobiste, domenowe, globalne);
3. Platforma WEB wielojęzykowa z różnymi skórkami graficznymi i obsługą języka polskiego;
4. Kalendarz, zadania, notatki;
5. Możliwość tworzenia własnych reguł wiadomości oraz własnych czarnych list;
6. Importowanie, eksportowanie list kontaktów;
7. Ustawienie wymagań dotyczących potwierdzeń wiadomości;
8. Współdzielenie z innymi użytkownikami kalendarza, kontaktów, zadań;

9. Dodawanie urządzenia bazującego na TOTP do przeprowadzania weryfikacji dwuetapowej (2FA);

xvi. Funkcje z zakresu bezpieczeństwa: filtrowanie opierające się na wyniku (score) mechanizmów Antispam i Antivirus, filtrowanie na poziomie serwera, domeny, użytkownika, białe/czarny listy na poziomie IP/Domeny, weryfikacja nadawcy wiadomości w oparciu o DMARC (SPF/DKIM), filtrowanie wiadomości bazujące na kraju serwera pocztowego nadawcy, ograniczenia w zakresie rozmiaru wiadomości, ograniczenie ilości maksymalnie nawiązanych jednoczesnych połączeń, weryfikacja adresu IP serwera pocztowego poprzez ReverseDNS, wymuszenie połączeń SSL/TLS, filtrowanie wiadomości na podstawie rozszerzenia załącznika;

xvii. Kopie bezpieczeństwa: tworzenie oraz odtwarzanie kopii całościowych lub częściowych w hierarchii: wiadomość, folder wiadomości, odbiorca wiadomości, grupa, lista mailingowa, konto e-mail, folder publiczny, domena. Serwer zapewnia funkcjonalność umożliwiającą tworzenie regularnych kopii udostępnianych poprzez protokół FTP za pomocą których istnieje możliwość odtworzenia serwera pocztowego.

c. Licencjonowanie:

i. Czas trwania licencji: 24 miesiące;

ii. Zakres licencji:

1. Ilość użytkowników: 70 kont;
2. Moduły dla wszystkich kont: Antispam, Antivirus, ActiveSync Exchange;

d. Zakres usługowy:

i. Zakres zadań do wykonania w ramach instalacji systemu pocztowego:

1. Instalacja nowego systemu poczty elektronicznej na przygotowanej przez informatyka Urzędu maszynie wirtualnej;
2. Konfiguracja systemu pocztowego w zakresie funkcjonalnym w konsultacji z informatykiem, m.in. uruchomienie usług poczty elektronicznej, kalendarzy, grup dystrybucyjnych, wspólnej bazy kontaktów oraz domyślnej budowy podpisów wiadomości e-mail;
3. Odtworzenie listy kont pocztowych w nowym systemie pocztowym odzwierciedlające wszystkie konta w obecnym systemie pocztowym oraz przekazanie dokumentacji dotyczącej każdego konta pocztowego informatykowi Urzędu;
4. **Przeprowadzenie szkolenia dla użytkowników systemu zrealizowanego w siedzibie Zamawiającego** w wymiarze minimum 2 godzin uwzględniającego wszystkie elementy użytkowania systemu m.in. obsługa poczty, konfiguracja filtrów, obsługa listy kontaktów, kalendarza, automatyczne odpowiedzi na czas nieobecności, przekierowania poczty do innego użytkownika systemu, okresowa zmiana hasła;

5. **Przygotowanie instrukcji w formie plików PDF lub nagrań wideo dla użytkowników końcowych** opisujących i przedstawiających w formie przykładów prawidłowe wykorzystywanie omówionych funkcji;
6. Przygotowanie konfiguracji serwera pocztowego w konsultacji z informatykiem Urzędu pod kątem odbioru oraz wysyłki elektronicznej z uwzględnieniem analizy rekordów DKIM/DMARC/SPF;
7. Ustalenie w konsultacji z informatykiem Urzędu formy i parametrów modyfikacji rekordów DNS dla MX, DKIM, DMARC, SPF wraz z przekazaniem wartości rekordów;
8. Uruchomienie usługi uwierzytelniania do systemu pocztowego za pomocą panelu WWW poprzez mechanizm 2FA oparty o protokół TOTP **indywidualnie przy każdym użytkowniku konta pocztowego w miejsc pracy użytkownika. Wszyscy użytkownicy znajdują się na terenie Gminy Zamawiającego.**
9. Dokonanie weryfikacji prawidłowego pobierania oraz wysyłania poczty elektronicznej z kont użytkowników;
10. Wykonanie przeniesienia zawartości każdego z kont pocztowych na konto odzwierciedlone w nowym systemie pocztowym;

e. Wsparcie techniczne:

1. Wykonawca zapewnia wsparcie technicznie przez cały okres licencjonowania w dni robocze w godzinach od 8:00 do 16:00 w zakresie wyjaśnień dotyczących funkcjonalności systemu, wsparcia w jego konfiguracji oraz realizacji zgłoszonych usterek technicznych bez ograniczenia liczby zgłoszeń oraz czasu realizacji;
2. Wsparcie polega na analizie w siedzibie Zamawiającego lub za pomocą udostępnionego przez informatyka Urzędu kanału zdalnego zgłoszonego problemu technicznego z działaniem usługi pocztowej;
3. Czas reakcji od przyjęcia zgłoszenia do fizycznego rozpoczęcia prac w konsultacji z informatykiem Urzędu nie może przekraczać 2 godzin;
4. Jeżeli rozwiązanie problemu technicznego nie może zostać zrealizowane w przeciągu 4 godzin od zgłoszenia usterki, wymagane jest powiadomienie informatyka Urzędu o charakterze usterki, podjętych w międzyczasie pracach wraz z uzasadnieniem;

IX. Rozbudowa istniejącej pamięci masowej NAS za pomocą modułu rozszerzającego – TYP A

a. Parametry techniczne:

i. Jednostka rozszerzająca w formacie RACK 19” o wysokości użytkowej 1U z wszystkimi niezbędnymi akcesoriami do jej montażu w szafie dystrybucyjnej 19”:

1. w zestawie dołączone szyny montażowe do montażu w szafie RACK o długości 800mm;

ii. Obsługa 4 dodatkowych dysków twardych w formacie 2,5” lub 3,5” z dostarczonymi adapterami oraz komponentami instalacyjnymi umożliwiającymi obsadzenie dysków w urządzeniu;

iii. Połączenie z jednostką główną za pomocą interfejsu eSATA;

iv. Obsadzone dyski twarde w jednostce rozszerzającej są widoczne indywidualnie (każdy dysk z osobna) w jednostce głównej podłączonej do jednostki rozszerzającej za pomocą interfejsu eSATA;

v. Urządzenie wyposażone w układ chłodzenia zapewniający przepływ powietrza w zainstalowanych dyskach twardych w wymiarze minimum 2 wentylatorów;

vi. Złącze zasilania IEC obsługujące standardowe napięcie 230V 50/60Hz;

vii. Jednostka rozszerzająca obsadzona w 4 dyski SSD o pojemności minimum 960GB w formacie 2,5” w pełni kompatybilne z oferowaną macierzą dyskową oraz wykazane na liście kompatybilności z funkcjonalnością aktualizacji oprogramowania układowego dysku SSD bezpośrednio z interfejsu zarządzania pamięcią masową. Odczyt sekwencyjny 128kB/QD32 – minimum 500MB/s, zapis sekwencyjny 128kB/QD32 – minimum 500MB/s, odczyt losowy 4kB/QD32 – minimum 90000 IOPS, zapis losowy 4kB/QD32 – minimum 30000 IOPS. Współczynnik TBW – minimum 1700TB, parametr MTBF co najmniej 1mln godzin. Dysk wyposażony w układ zabezpieczający przed nagłą utratą zasilania;

b. Kompatybilność:

i. Urządzenie wykazane na liście kompatybilności jednostek rozszerzających dla modelu Synology RS822RP+;

c. Zakres usługowy:

i. Wykonawca dostarcza urządzenie wyposażone w komponenty wykazane w specyfikacji do siedziby Zamawiającego oraz instaluje je w wyznaczonym miejscu w szafie dystrybucyjnej RACK19” w konsultacji z informatykiem Urzędu;

d. Gwarancja producenta na moduł rozszerzający: 36 miesięcy;

e. Gwarancja producenta na dyski SSD: 60 miesięcy;

X. Rozbudowa istniejącej pamięci masowej NAS za pomocą modułu rozszerzającego – TYP B

a. Parametry techniczne:

i. Jednostka rozszerzająca w formacie RACK 19” o wysokości użytkowej 1U z wszystkimi niezbędnymi akcesoriami do jej montażu w szafie dystrybucyjnej 19”:

1. w zestawie dołączone szyny montażowe do montażu w szafie RACK o długości 1000mm;

ii. Obsługa 4 dodatkowych dysków twardych w formacie 2,5” lub 3,5” z dostarczonymi adapterami oraz komponentami instalacyjnymi umożliwiającymi obsadzenie dysków w urządzeniu;

iii. Połączenie z jednostką główną za pomocą interfejsu eSATA;

iv. Obsadzone dyski twarde w jednostce rozszerzającej są widoczne indywidualnie (każdy dysk z osobna) w jednostce głównej podłączonej do jednostki rozszerzającej za pomocą interfejsu eSATA;

v. Urządzenie wyposażone w układ chłodzenia zapewniający przepływ powietrza w zainstalowanych dyskach twardych w wymiarze minimum 2 wentylatorów;

vi. Złącze zasilania IEC obsługujące standardowe napięcie 230V 50/60Hz;

vii. Jednostka rozszerzająca obsadzona w 4 dyski SSD o pojemności minimum 960GB w formacie 2,5” w pełni kompatybilne z oferowaną macierzą dyskową oraz wykazane na liście kompatybilności z funkcjonalnością aktualizacji oprogramowania układowego dysku SSD bezpośrednio z interfejsu zarządzania pamięcią masową. Odczyt sekwencyjny 128kB/QD32 – minimum 500MB/s, zapis sekwencyjny 128kB/QD32 – minimum 500MB/s, odczyt losowy 4kB/QD32 – minimum 90000 IOPS, zapis losowy 4kB/QD32 – minimum 30000 IOPS. Współczynnik TBW – minimum 1700TB, parametr MTBF co najmniej 1mln godzin. Dysk wyposażony w układ zabezpieczający przed nagłą utratą zasilania;

b. Kompatybilność:

i. Urządzenie wykazane na liście kompatybilności jednostek rozszerzających dla modelu Synology RS822RP+;

c. Zakres usługowy:

i. Wykonawca dostarcza urządzenie wyposażone w komponenty wykazane w specyfikacji do siedziby Zamawiającego oraz instaluje je w wyznaczonym miejscu w szafie dystrybucyjnej RACK19” w konsultacji z informatykiem Urzędu;

d. Gwarancja producenta na moduł rozszerzający: 36 miesięcy;

e. Gwarancja producenta na dyski SSD: 60 miesięcy;

XI. Rozbudowa istniejącej pamięci masowej NAS za pomocą modułu rozszerzającego – TYP C

a. Parametry techniczne:

i. Jednostka rozszerzająca w formacie RACK 19” o wysokości użytkowej 1U z wszystkimi niezbędnymi akcesoriami do jej montażu w szafie dystrybucyjnej 19”:

1. w zestawie dołączone szyny montażowe do montażu w szafie RACK o długości 800mm;

ii. Obsługa 4 dodatkowych dysków twardych w formacie 2,5” lub 3,5” z dostarczonymi adapterami oraz komponentami instalacyjnymi umożliwiającymi obsadzenie dysków w urządzeniu;

iii. Połączenie z jednostką główną za pomocą interfejsu eSATA;

iv. Obsadzone dyski twarde w jednostce rozszerzającej są widoczne indywidualnie (każdy dysk z osobna) w jednostce głównej podłączonej do jednostki rozszerzającej za pomocą interfejsu eSATA;

v. Urządzenie wyposażone w układ chłodzenia zapewniający przepływ powietrza w zainstalowanych dyskach twardych w wymiarze minimum 2 wentylatorów;

vi. Złącze zasilania IEC obsługujące standardowe napięcie 230V 50/60Hz;

vii. Jednostka rozszerzająca obsadzona w 4 dyski HDD SATA w pełni kompatybilne z oferowaną macierzą dyskową oraz wykazane na liście kompatybilności. Pojemności dyski twardego 8TB, prędkość obrotowa 7200 obr./min., 256MB pamięci cache, technologia zapisu CMR. Dysk przeznaczony do zastosowania w pamięciach masowych NAS, parametr MTBF określony na minimum 1mln godzin, gwarancja dysku twardego 36 miesięcy;

b. Kompatybilność:

i. Urządzenie wykazane na liście kompatybilności jednostek rozszerzających dla modelu Synology RS822RP+;

c. Zakres usługowy:

i. Wykonawca dostarcza urządzenie wyposażone w komponenty wykazane w specyfikacji do siedziby Zamawiającego oraz instaluje je w wyznaczonym miejscu w szafie dystrybucyjnej RACK19” w konsultacji z informatykiem Urzędu;

d. Gwarancja producenta na moduł rozszerzający: 36 miesięcy;

e. Gwarancja producenta na dyski HDD: 36 miesięcy;

XII. Rozbudowa istniejącej pamięci masowej NAS w zakresie interfejsów sieciowych

a. **Parametry techniczne:**
   i. Interfejs komunikacyjny z pamięcią masową: PCIe 3.0 x8;
   ii. Zgodność z specyfikacją: IEEE 802.3ae 10Gb/s oraz IEEE 802.3ad;
   iii. Złącza sieciowe: SFP+ - 2 sztuki 10Gb/s, pełny dupleks;
   iv. Obsługa Jumbo Frame z jednostką MTU minimum 4000;
   v. Obsadzenie slotów SFP+ w moduły SFP+;
      1. Slot nr 1 – moduł SFP+ MultiMod, LC Duplex, 850nm, 10Gb/s;
      2. Slot nr 2 – moduł SFP+, RJ45, 10Gb/s;

b. **Kompatybilność:**
   i. Karta sieciowa wykazana na liście kompatybilności modelu Synology RS822RP+;

c. **Zakres usługowy:**
   i. Pamięć masowa pracuje w trybie wysokiej dostępności (High Availability) z drugą taką samą pamięcią masową. Wykonawca dostarcza moduł sieciowy oraz dokonuje jego wymiany w urządzeniu odtwarzając zastaną konfigurację urządzenia w zakresie interfejsów sieciowych oraz reguł zapory ogniowej firewall. Po wykonaniu instalacji modułów sieciowych oraz uruchomieniu komunikacji światłowodowej za pomocą istniejącej już infrastruktury światłowodowej, dokonywana jest weryfikacja poprawności pracy pamięci masowej oraz funkcjonalności wysokiej dostępności wraz z automatycznym przełączaniem się urządzeń;

d. **Gwarancja producenta na kartę sieciową:** 60 miesięcy;

e. **Gwarancja producenta na moduły SFP+:** 12 miesięcy;