OPIS PRZEDMIOTU ZAMÓWIENIA

DOSTAWA PAKIETU ROZWIĄZAŃ DOTYCZĄCYCH CYBERBEZPIECZEŃSTWA W RAMACH PROJEKTU GRANTOWEGO „CYBERBEZPIECZNY SAMORZĄD”

1. Urządzenie UTM wraz ze wsparciem dla UG

Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa, instalacja i konfiguracja urządzenia klasy UTM (Unified Threat Management) wraz z licencją na 12 miesięcy obejmującą funkcje ochrony sieci takie jak: firewall, IPS, ochrona antywirusowa, filtrowanie treści internetowych, kontrola aplikacji oraz VPN w środowisku Zamawiającego. Urządzenie ma umożliwiać bezpieczną ochronę sieci lokalnej przed zagrożeniami zewnętrznymi i wewnętrznymi.

Minimalne wymagania techniczne

OBSŁUGA SIECI

1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.

ZAPORA KORPORACYJNA (Firewall)

2. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.

3. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.

4. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).

5. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.

6. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.

7. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.

8. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.

9. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.

10. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.

11. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).

12. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.

INTRUSION PREVENTION SYSTEM (IPS)

13. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.

14. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.

15. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.

16. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.

17. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS.

18. Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.

19. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.

20. Moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV).

21. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.

KSZTAŁTOWANIE PASMA (Traffic Shapping)

23. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.

24. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.

25. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).

26. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

OCHRONA ANTYWIRUSOWA

27. Urządzenie ma być dostarczone wraz z komercyjnym, zaawansowanym skanerem antywirusowym oraz umożliwiać skanowanie plików w oparciu o sandboxing zlokalizowany w Internecie na serwerach producenta i na terenie Unii Europejskiej. Nie dopuszcza się aby analiza sandboxingu była przeprowadzana na urządzeniu lub wymagała instalacji dodatkowego urządzenia lub oprogramowania. Nie dopuszcza się również żeby analiza sandboxingu była przeprowadzana przez firmy trzecie.

29. Administrator ma mieć możliwość określenia akcji w przypadku wykrycia zagrożenia bądź gdy analiza skanerem antywirusowym została zakończona błędem.

31. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.

32. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.

OCHRONA ANTYSPAM

33. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).

34. Ochrona antyspam ma działać w oparciu o:

a. białe/czarne listy,

b. DNS RBL,

c. Skaner heurystyczny.

35. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.

36. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.

WIRTUALNE SIECI PRYWATNE (VPN)

37. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).

38. Urządzenie ma wspierać co najmniej następujące typy sieci VPN:

a. PPTP VPN,

b. IPSec VPN,

c. SSL VPN.

39. SSL VPN ma działać w trybie tunelu.

40. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.

41. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal)

42. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).

43. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.

44. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.

FILTR DOSTĘPU DO STRON WWW

45. Urządzenie ma posiadać wbudowany filtr URL.

46. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 77 kategorii tematycznych stron internetowych

47. Klasyfikacja URL musi się odbywać w oparciu o komunikację z serwerami producenta znajdującymi się w sieci Internet, a nie na bazie danych przechowywanej lokalnie w urządzeniu.

48. Administrator ma mieć możliwość dodawania własnych kategorii URL.

49. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:

a. blokowanie dostępu do adresu URL,

b. zezwolenie na dostęp do adresu URL,

c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.

50. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.

51. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.

52. Filtr URL musi uwzględniać komunikację po protokole HTTPS.

53. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.

54. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.

55. Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania za pomocą systemu filtrowania treści internetowych.

UWIERZYTELNIANIE

56. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o:

a. lokalną bazę użytkowników (wewnętrzny LDAP),

b. zewnętrzną bazę użytkowników (zewnętrzny LDAP),

c. usługę katalogową Microsoft Active Directory.

57. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.

58. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły:

a. SSL,

b. Radius,

c. Kerberos.

59. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.

60. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.

61. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.

62. Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS).

63. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).

64. Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.

65. Rozwiązanie musi zapewniać Zero-Trust Network Access (ZTNA), dając dostęp do zasobów na podstawie analizy polityk bezpieczeństwa w oparciu co najmniej o weryfikację wersji systemu operacyjnego, statusu zapory sieciowej czy zainstalowanego programu antywirusowego na stacji roboczej.

ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)

66. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).

67. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:

a. równoważenie względem adresu źródłowego,

b. równoważenie względem połączenia.

68. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.

69. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).

70. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.

71. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).

72. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.

ROUTING (TRASOWANIE)

73. Urządzenie ma umożliwiać statyczne trasowanie pakietów.

74. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.

75. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).

76. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.

77. Rozwiązanie musi dawać możliwość wybrania predefiniowalnego obiektu typu blackhole.

ADMINISTRACJA URZĄDZENIEM

78. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.

79. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.

80. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.

81. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.

82. Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.

83. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH)

84. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.

85. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.

86. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup.

87. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.

88. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.

89. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording).

90. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).

91. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.

92. Urządzenie ma umożliwiać zapisywanie logów na wbudowanym dysku.

93. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).

94. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.

95. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:

a. manualnego eksportu do pliku w dowolnym momencie czasu,

b. automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu

96. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzącego bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.

97. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.

98. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.

RAPORTOWANIE

99. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.

100. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.

101. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.

102. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.

103. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.

104. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV.

105. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.

106. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.

107. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).

POZOSTAŁE USŁUGI I FUNKCJE

108. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.

109. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.

110. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).

111. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.

112. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny).

113. Urządzenie ma posiadać usługę DNS Proxy.

114. Urządzenie ma posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP).

115. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN.

116. Urządzenie musi mieć zaimplementowane Open API.

117. Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.

GWARANCJA I SERWIS

118. Urządzenie ma być objęte 12-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.

119. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.

PARAMETRY SPRZĘTOWE

120. Urządzenie ma być wyposażone w dysk SSD o pojemności co najmniej 200 GB.

121. Urządzenie wyposażone jest w redundantne zasilanie z sygnalizacją pracy poszczególnych zasilaczy.

122. Liczba portów Ethernet 2,5Gbps – min. 8 z możliwością rozszerzenia do 16.

123. Liczba portów światłowodowych 1Gbps – min. 2 z możliwością rozszerzenia do 10.

124. Urządzenie ma pozwalać na instalację modułu rozszerzeń z poniższej listy:

a. Moduł z 8 interfejsami miedzianymi 2,5Gbps

b. Moduł z 4 interfejsami miedzianymi 10Gbps.

c. Moduł z 8 interfejsami miedzianymi 1Gbps (4 pary interfejsów w trybie bypass).

d. Moduł z 8 interfejsami miedzianymi 1Gbps.

e. Moduł z 8 interfejsami światłowodowymi 1Gbps.

f. Moduł z 4 interfejsami światłowodowymi 10Gbps.

g. Moduł z 2 interfejsami światłowodowymi 25Gbps.

Urządzenie ma zostać wyposażone w moduł z 4 interfejsami światłowodowymi 10Gbps, 4 wkładkami SFP+ i 4 patchcord-ami do połączenia ze switch-ami.

125. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.

126. Urządzenie ma być wyposażone w min. 2, różniące się typem, porty konsolowe. Przynajmniej jeden port konsolowy ma być typu RJ45.

127. Przepustowość Firewall (1518 bajtów UDP) – minimum 10Gbps.

128. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 5Gbps.

129. Przepustowość filtrowania Antywirusowego – minimum 1.3 Gbps.

130. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 2.5Gbps.

131. Liczba tuneli VPN IPSec – minimum 1000.

132. Liczba tuneli typu SSL VPN (tryb tunelu) – minimum 150.

133. Obsługa interfejsów 802.11q (VLAN) – minimum 256.

134. Liczba równoczesnych sesji – minimum 600 000 i nie mniej niż 30 000 nowych sesji/sekundę.

135. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.

136. Urządzenie nie ma limitu na liczbę użytkowników.

137. Liczba reguł filtrowania – minimum 16 384.

138. Liczba tras statycznego routingu – minimum 5 120.

139. Liczba tras dynamicznego routingu – minimum 10 000.

140. Możliwość instalacji w szafie RACK 19”, wysokość urządzenia 1U.

141. Urządzenie musi być wyposażone w moduł TPM.

Instalacja i konfiguracja rozwiązania:

Poprzez instalację i konfigurację rozwiązania Zamawiający będzie wymagał następujących czynności:

- Montaż i uruchomienie oferowanego sprzętu w siedzibie Zamawiającego.
- Aktualizacja oprogramowania urządzenia do najnowszej wersji.
- Konfiguracja zgodnie z najlepszymi praktykami z uwzględnieniem wymaganych połączeń, konfiguracja interfejsów fizycznych i interfejsów VLAN.
- Opracowanie wraz z Zamawiającym i zastosowanie polityki Firewall, uruchomienie IDS/IPS oraz innych filtrów oraz ustawień.

Prace wdrożeniowe będą prowadzone w terminie uzgodnionym z Zamawiającym (w dzień roboczy, w godzinach 8:00 – 16:00). Na zakończenie wdrożenia zostanie przeprowadzone instruktażowe szkolenie z wdrożonego systemu UTM obejmujące wdrożone mechanizmy i możliwości tego rozwiązania.

2. Urządzenie UTM wraz ze wsparciem dla JO

Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa, instalacja i konfiguracja urządzenia klasy UTM (Unified Threat Management) wraz z licencją na 12 miesięcy obejmującą funkcje ochrony sieci takie jak: firewall, IPS, ochrona antywirusowa, filtrowanie treści internetowych, kontrola aplikacji oraz VPN w środowisku Zamawiającego. Urządzenie ma umożliwiać bezpieczną ochronę sieci lokalnej przed zagrożeniami zewnętrznymi i wewnętrznymi.

Minimalne wymagania techniczne

OBSŁUGA SIECI

1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.

ZAPORA KORPORACYJNA (Firewall)

2. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.

3. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.

4. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).

5. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.

6. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.

7. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.

8. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.

9. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.

10. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.

11. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).

12. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.

INTRUSION PREVENTION SYSTEM (IPS)

13. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.

14. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.

15. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.

16. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.

17. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.

18. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS.

19. Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.

20. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.

21. Moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV).

22. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.

KSZTAŁTOWANIE PASMA (Traffic Shapping)

23. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.

24. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.

25. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).

26. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

OCHRONA ANTYWIRUSOWA

27. Urządzenie ma być dostarczone wraz z komercyjnym, zaawansowanym skanerem antywirusowym oraz umożliwiać skanowanie plików w oparciu o sandboxing zlokalizowany w Internecie na serwerach producenta i na terenie Unii Europejskiej. Nie dopuszcza się aby analiza sandboxingu była przeprowadzana na urządzeniu lub wymagała instalacji dodatkowego urządzenia lub oprogramowania. Nie dopuszcza się również żeby analiza sandboxingu była przeprowadzana przez firmy trzecie.

29. Administrator ma mieć możliwość określenia akcji w przypadku wykrycia zagrożenia bądź gdy analiza skanerem antywirusowym została zakończona błędem.

31. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.

32. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.

OCHRONA ANTYSPAM

33. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).

34. Ochrona antyspam ma działać w oparciu o:

a. białe/czarne listy,

b. DNS RBL,

c. Skaner heurystyczny.

35. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.

36. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.

WIRTUALNE SIECI PRYWATNE (VPN)

37. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).

38. Urządzenie ma wspierać co najmniej następujące typy sieci VPN:

a. PPTP VPN,

b. IPSec VPN,

c. SSL VPN.

39. SSL VPN ma działać w trybie tunelu.

40. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.

41. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal)

42. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).

43. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.

44. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.

FILTR DOSTĘPU DO STRON WWW

45. Urządzenie ma posiadać wbudowany filtr URL.

46. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 77 kategorii tematycznych stron internetowych.

47. Klasyfikacja URL musi się odbywać w oparciu o komunikację z serwerami producenta znajdującymi się w sieci Internet, a nie na bazie danych przechowywanej lokalnie w urządzeniu.

48. Administrator ma mieć możliwość dodawania własnych kategorii URL.

49. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:

a. blokowanie dostępu do adresu URL,

b. zezwolenie na dostęp do adresu URL,

c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.

50. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.

51. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.

52. Filtr URL musi uwzględniać komunikację po protokole HTTPS.

53. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.

54. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.

55. Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch.

UWIERZYTELNIANIE

56. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o:

a. lokalną bazę użytkowników (wewnętrzny LDAP),

b. zewnętrzną bazę użytkowników (zewnętrzny LDAP),

c. usługę katalogową Microsoft Active Directory.

57. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.

58. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły:

a. SSL,

b. Radius,

c. Kerberos.

59. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.

60. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.

61. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.

62. Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS).

63. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).

64. Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.

65. Rozwiązanie musi zapewniać Zero-Trust Network Access (ZTNA), dając dostęp do zasobów na podstawie analizy polityk bezpieczeństwa w oparciu co najmniej o weryfikację wersji systemu operacyjnego, statusu zapory sieciowej czy zainstalowanego programu antywirusowego na stacji roboczej.

ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)

66. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).

67. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:

a. równoważenie względem adresu źródłowego,

b. równoważenie względem połączenia.

68. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.

69. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).

70. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.

71. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).

72. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.

ROUTING (TRASOWANIE)

73. Urządzenie ma umożliwiać statyczne trasowanie pakietów.

74. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.

75. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).

76. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.

77. Rozwiązanie musi dawać możliwość wybrania predefiniowalnego obiektu typu blackhole.

ADMINISTRACJA URZĄDZENIEM

78. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.

79. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.

80. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.

81. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.

82. Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.

83. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH)

84. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.

85. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.

86. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup.

87. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.

88. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.

89. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording).

90. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).

91. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.

92. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).

93. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.

94. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:

a. manualnego eksportu do pliku w dowolnym momencie czasu,

b. automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany

przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu

95. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.

96. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.

97. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.

RAPORTOWANIE

98. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.

99. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.

100. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.

101. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.

102. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.

103. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV.

104. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.

105. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.

106. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).

POZOSTAŁE USŁUGI I FUNKCJE

107. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.

108. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.

109. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).

110. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.

111. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny).

112. Urządzenie ma posiadać usługę DNS Proxy.

113. Urządzenie ma posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP).

114. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN.

115. Urządzenie musi mieć zaimplementowane Open API.

116. Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.

GWARANCJA I SERWIS

117. Urządzenie ma być objęte 12-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.

118. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.

PARAMETRY SPRZĘTOWE

119. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash.

120. Urządzenie ma być wyposażone w zintegrowany port na kartę microSD.

121. Liczba portów Ethernet 2,5Gbps – min. 8.

122. Liczba portów światłowodowych 1Gbps – min. 1.

Urządzenie ma zostać wyposażone w 1 x wkładkami SFP i patchcord do połączenia ze switch-em.

123. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.

124. Przepustowość Firewall (1518 bajtów UDP) – minimum 8Gbps.

125. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 4Gbps.

126. Przepustowość filtrowania Antywirusowego – minimum 1Gbps.

127. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 2Gbps.

128. Liczba tuneli VPN IPSec – minimum 100.

129. Liczba tuneli typu SSL VPN (tryb tunelu) – minimum 100.

130. Obsługa interfejsów 802.11q (VLAN) – minimum 128

131. Liczba równoczesnych sesji – minimum 400 000 i nie mniej niż 25 000 nowych sesji/sekundę.

132. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.

133. Urządzenie nie ma limitu na liczbę użytkowników.

134. Liczba reguł filtrowania – minimum 8 192.

135. Liczba tras statycznego routingu – minimum 512.

136. Liczba tras dynamicznego routingu – minimum 10 000.

137. Urządzenie ma umożliwiać podłączenie zewnętrznego nadmiarowego zasilacza (zasilanie redundantne). Stan pracy każdego zasilacza musi być sygnalizowany bezpośrednio na obudowie urządzenia.

138. Urządzenie musi być wyposażone w moduł TPM

Instalacja i konfiguracja rozwiązania:

Poprzez instalację i konfigurację rozwiązania Zamawiający będzie wymagał następujących czynności:

- Montaż i uruchomienie oferowanego sprzętu w siedzibie Zamawiającego.
- Aktualizacja oprogramowania urządzenia do najnowszej wersji.
- Konfiguracja zgodnie z najlepszymi praktykami z uwzględnieniem wymaganych połączeń, konfiguracja interfejsów fizycznych i interfejsów VLAN.
- Opracowanie wraz z Zamawiającym i zastosowanie polityki Firewall, uruchomienie IDS/IPS oraz innych filtrów oraz ustawień.

Prace wdrożeniowe będą prowadzone w terminie uzgodnionym z Zamawiającym (w dzień roboczy, w godzinach 8:00 – 16:00). Na zakończenie wdrożenia zostanie przeprowadzone instruktażowe szkolenie z wdrożonego systemu UTM obejmujące wdrożone mechanizmy i możliwości tego rozwiązania.

3. Oprogramowanie do inwentaryzacji

Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa i wdrożenie systemu informatycznego klasy IT Infrastructure Management (ITIM) w celu centralnego monitorowania, zarządzania i automatycznego audytu zasobów IT zamawiającego.

- **Wymagane funkcjonalności:**
  - **Inwentaryzacja sprzętu i oprogramowania:** System musi umożliwiać automatyczne wykrywanie i gromadzenie danych o wszystkich urządzeniach w sieci (stacje robocze, serwery, urządzenia sieciowe), w tym ich parametrach technicznych oraz zainstalowanym oprogramowaniu.
  - **Audyt legalności oprogramowania (Software Asset Management - SAM):** Funkcjonalność wspierająca zarządzanie licencjami, w tym możliwość generowania raportów niezgodności licencyjnych, monitorowania wykorzystania licencji oraz zarządzania kluczami produktów.
  - **Monitoring sieci (Network Monitoring System - NMS):** Ciągły nadzór nad dostępnością i wydajnością urządzeń sieciowych (np. przełączniki, routery, serwery) w czasie rzeczywistym, z możliwością generowania alertów w przypadku awarii lub przekroczenia progów wydajności (np. wykorzystanie procesora, pamięci, pasma sieciowego).
  - **Zarządzanie użytkownikami (Helpdesk/Ticketing):** Opcjonalnie: moduł umożliwiający rejestrowanie zgłoszeń serwisowych, przypisywanie ich do odpowiednich techników, śledzenie statusu realizacji oraz raportowanie czasu pracy.
  - **Zdalny pulpit:** Możliwość zdalnego dostępu do stacji roboczych użytkowników w celu świadczenia wsparcia technicznego, z zachowaniem mechanizmów autoryzacji i bezpieczeństwa.
  - **Generowanie raportów:** Rozbudowany moduł raportowania i analizy danych inwentaryzacyjnych, licencyjnych oraz monitoringu.
- **Parametry techniczne:** Usługa serwisu i wsparcia technicznego na okres 12 miesięcy dla 50 stanowisk.

4. Oprogramowanie antywirusowe dla JO

Przedmiotem zamówienia jest dostawa, wdrożenie oraz świadczenie wsparcia technicznego dla licencji na zintegrowaną platformę do zarządzania bezpieczeństwem punktów końcowych (Endpoint Protection Platform - EPP) z zaawansowanymi funkcjonalnościami wykrywania i reagowania na zagrożenia (Endpoint Detection and Response - EDR lub Extended Detection and Response - XDR), dla infrastruktury Zamawiającego.

1. Wymagania Ogólne

- Zamawiający wymaga dostawy oprogramowania klasy korporacyjnej, które zapewni kompleksową ochronę przed szerokim spektrum zagrożeń cybernetycznych, w tym: złośliwym oprogramowaniem (malware), oprogramowaniem wymuszającym okup (ransomware), atakami bezplikowymi, phishingiem, exploitami oraz atakami typu zero-day.
- Rozwiązanie musi działać w architekturze scentralizowanej konsoli zarządzania (dopuszcza się model lokalny lub chmurowy) oraz agentów instalowanych na punktach końcowych (stacje robocze, serwery fizyczne i wirtualne).
- **Neutralność technologiczna:** Wszelkie odniesienia do konkretnych produktów lub technologii (np. "Bitdefender GravityZone") należy traktować jako przykładowe. Zamawiający **dopuszcza rozwiązania równoważne**, które spełniają poniższe parametry techniczne i funkcjonalne w stopniu nie gorszym niż opisano.

2. Wymagania Funkcjonalne

System musi realizować następujące funkcje:

L.p.	Funkcjonalność / Cecha	Opis Wymagania
1	Ochrona antywirusowa i antymalware	Wielowarstwowa ochrona wykorzystująca sygnatury, heurystykę, analizę behawioralną oraz technologie uczenia maszynowego do identyfikacji i blokowania zagrożeń.
2	Ochrona przed ransomware	Specjalistyczne mechanizmy monitorujące zachowania procesów i blokujące próby szyfrowania danych przez złośliwe oprogramowanie.
3	Centralna Konsola Zarządzania	Intuicyjny interfejs umożliwiający zarządzanie politykami bezpieczeństwa, wdrażaniem agentów, monitorowaniem stanu ochrony oraz generowaniem raportów dla całej infrastruktury.
4	EDR / Widoczność zagrożeń	Funkcjonalności EDR/XDR zapewniające pełną widoczność procesów i aktywności na punktach końcowych, umożliwiające analizę incydentów, badanie śledcze oraz wizualizację wektorów ataku.

5	Automatyczne reagowanie	Możliwość automatycznego reagowania na wykryte zagrożenia, np. poprzez izolację zainfekowanego hosta od sieci, zatrzymanie złośliwego procesu.
6	Zapora sieciowa (Firewall)	Zarządzanie regułami firewalla na punktach końcowych z poziomu konsoli centralnej.
7	Zarządzanie urządzeniami (Device Control)	Kontrola dostępu do portów USB, Bluetooth oraz innych urządzeń peryferyjnych.
8	Kompatybilność	Wsparcie dla systemów operacyjnych: Windows, macOS, Linux, Android/iOS.

3. Wymagania Techniczne i Licencyjne

- **Liczba licencji:** Wymagana łączna liczba licencji wynosi: 15 dla stacji roboczych oraz 1 dla serwera.
- **Okres licencji:** Licencje wraz ze wsparciem i aktualizacjami powinny zostać dostarczone na okres 24 miesięcy.
- **Wsparcie techniczne:** Wymagany jest dostęp do wsparcia technicznego producenta lub autoryzowanego partnera w języku polskim, w godzinach 8:00-16:00 w dni robocze.

5. Oprogramowanie DLP

Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa, instalacja i wdrożenie systemu klasy DLP (Data Loss Prevention) oraz monitorowania aktywności 50 użytkowników roboczych w wersji on-premise w modelu licencjonowania Livetime.

Minimalne wymagania funkcjonalne i techniczne systemu

1. System operacyjny:

a. Windows 10 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi

b. Windows 11 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi

c. MacOS 12 lub nowszy.

2. Serwer administracyjny musi obsługiwać instalację na systemach:

a. Windows Server 2016 (64-bit) i nowszych.

3. Serwer administracyjny musi obsługiwać bazy danych:

a. MS SQL Server 2016 lub nowsze,

b. MS SQL Express,

c. AzureSQL S3 lub nowsze.

4. Pomoc i dokumentacja programu dostępne w języku polskim.

5. Konsola administracyjna i komunikaty klienta muszą być w języku polskim.

6. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.

7. Serwer administracyjny musi umożliwiać instalację/dezinstalację zdalnego klienta na stacjach roboczych.

8. Brak połączenia klienta z serwerem zarządzającym musi umożliwiać lokalne przechowywanie informacji i zebranych danych do czasu ponownego połączenia.

9. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsoli.

10. Serwer administracyjny musi automatycznie pobierać aktualizacje definicji kategoryzowania stron internetowych, aplikacji i rozszerzeń plików, z opcją wyłączenia automatycznego pobierania.

11. Administrator musi mieć możliwość aby tworzyć, usuwać i konta administratorów w konsoli programu.

12. Administrator musi mieć możliwość przypisywania i odbierania uprawnień do wybranych modułów programu, podzielonych na ustawienia (konfiguracja modułu) i logi (wyświetlanie logów modułu).

13. Serwer musi synchronizować użytkowników i stacje robocze z domeną Active Directory.

14. Administrator musi móc wymusić synchronizację ustawień i logów między stacją roboczą, a serwerem w czasie rzeczywistym.

15. Administrator musi mieć możliwość wykonać audyt stacji roboczych/użytkowników w oparciu o różne czynności, takie jak uruchomione aplikacje, podłączone urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, wysyłane i odebrane wiadomości email oraz czynności na plikach.

16. Administrator musi mieć możliwość filtrowania i sortowania zebranych danych.

17. Serwer musi posiadać możliwość wysyłania alertów, przynajmniej za pośrednictwem wiadomości email.

18. Dashboardy muszą być generowane na podstawie wskazanych stacji roboczych, użytkowników lub grup w określonym przedziale czasu.

19. Serwer administracyjny musi posiadać wbudowany serwer SMTP dostarczony przez producenta oprogramowania.

20. Konsola musi umożliwiać konfigurację/zmianę domyślnego serwera SMTP.

21. Konsola webowa musi pozwalać na weryfikację wersji zainstalowanego oprogramowania klienta, a także umożliwia aktualizację do nowej wersji lub dezaktywację tego oprogramowania. o rozszerzeniu mdf.