ZAŁĄCZNIK 7 DO SWZ

|  |  |
| --- | --- |
| **Kategoria funkcjonalności** | **Funkcjonalność** |
| Informacje ogólne | 1. System musi zapewniać ochronę przed zagrożeniami związanymi z przesyłaniem poczty elektronicznej (wirusy, spam, phishing, niedozwolone treści itp.) 2. System musi zapewnić ochronę przed atakami ukierunkowanymi. 3. System musi zapewnić możliwość automatycznego wyciągania złośliwych wiadomości od użytkowników końcowych. 4. System musi być dostarczony w postaci zamkniętego rozwiązania sprzętowego lub obrazu maszyny wirtualnej. 5. Licencje muszą obejmować 15600 skrzynek pocztowych. 6. Należy zapewnić odpowiednie licencje na okres 12 miesięcy. 7. Wszystkie moduły rozwiązania muszą pochodzić od jednego producenta w celu zapewnienia kompatybilności wszystkich jego elementów oraz prawidłowego funkcjonowania. |
| Dostępność | 1. System musi zapewnić lokalne i zdalne zarządzanie za pomocą połączenia HTTPS przez przeglądarkę oraz poprzez protokół SSH. 2. System musi umożliwiać pracę w architekturze Master-Agent z możliwością przypisywania profili funkcjonalnych (filtrowania wiadomości, bazy kwarantanny, serwera logów) poszczególnym agentom. 3. System musi pracować jako brama SMTP i być niezależnym od rodzaju stosowanego, chronionego serwera poczty. |
| Filtrowanie poczty | 1. System musi umożliwiać filtrowanie poczty przychodzącej dla wskazanych domen oraz przesyłanie ruchu pocztowego na wskazany serwer pocztowy. 2. System musi umożliwiać filtrowanie poczty wychodzącej do wskazanych przez Administratora serwerów pocztowych. 3. System musi zapewnić możliwość zdefiniowania osobnych tras przesyłania poczty dla ruchu przychodzącego i wychodzącego w oparciu o statyczne wpisy adresów serwerów, smart hosta lub rekordy MX serwerów DNS. 4. System w momencie dostarczenia lub po odtworzeniu musi zawierać zestaw predefiniowanych reguł i polityk dla wszystkich modułów filtrujących: AV, antyspam, kontrola treści. 5. System musi umożliwiać automatyczne pobieranie oraz instalowanie aktualizacji modułów ochronnych oraz całego systemu 6. System musi posiadać lokalną kwarantannę dla zainfekowanych wiadomości. 7. System musi zapewniać użytkownikom końcowym możliwość zarządzania wiadomościami trafiającymi do ich personalnej kwarantanny. 8. System musi umożliwiać określanie poziomu dostępu i akcji możliwych do wykonania w obrębie kwarantanny dla różnych użytkowników/grup użytkowników. 9. Kwarantanna użytkownika oraz skrócone informacje o stanie kwarantanny dla użytkownika muszą być dostępne w języku polskim. 10. System musi zapewniać możliwość uwierzytelniania użytkownika w celu zmian parametrów własnego folderu kwarantanny. W tym celu, system musi wspierać mechanizmy uwierzytelnienia jednokrotnego (Single Sign-On) oparte o usługi federacyjne domeny Active Directory (ADFS) lub protokół SAML 2.0. 11. System musi zapewniać możliwość definiowania list zaufanych i blokowanych nadawców przez użytkowników końcowych. 12. System musi umożliwiać zmianę wyglądu portalu kwarantanny dla użytkownika końcowego, zarówno co do jej szaty graficznej (np. możliwość umieszczenia znaku firmowego) jak i treści komunikatów. 13. System musi umożliwiać definiowanie i przeglądanie wielu katalogów kwarantanny dla różnych reguł antywirusowych i antyspamowych. 14. Dla wszystkich stworzonych folderów kwarantanny system musi zapewniać możliwość ustawienia maksymalnego czasu przechowywania wiadomości a po jego upływie automatycznie je usunie. 15. System musi umożliwiać wyszukiwanie wiadomości w kwarantannie na podstawie nadawcy, odbiorcy, tematu wiadomości lub czasu od kiedy wiadomość znajduje się w kwarantannie. 16. System musi umożliwiać następujące operacje na wiadomościach przechowywanych w obszarze kwarantanny: usunięcie wiadomości, przesłanie do innego odbiorcy, przeniesienie do innego folderu, zwolnienie wiadomości, zwolnienie zaszyfrowanej wiadomości, ponowną ocenę wiadomości przez moduły filtrujące. 17. System musi zapewnić możliwość zgłoszenia przypadków złej klasyfikacji wiadomości do producenta systemu na poziomie kwarantanny administratora oraz personalnej kwarantanny użytkownika końcowego. 18. System musi umożliwiać stworzenie bazy użytkowników poczty elektronicznej w oparciu o zdefiniowanie lokalnych kont użytkowników, a także zapewniać możliwość synchronizacji bazy użytkowników z serwerów: Active Directory, Azure Active Directory, LDAP, MS Exchange lub za pomocą odpowiednio przygotowanych plików (tekstowych, csv). 19. System musi zapewniać możliwość ustawienia przez administratora harmonogramu synchronizacji bazy użytkowników. 20. System musi umożliwiać konfigurację harmonogramu wysyłania powiadomień mailowych do użytkowników o np. nowych wiadomościach zatrzymanych w kwarantannie. 21. System musi posiadać graficzny interfejs administratora do śledzenia wiadomości na poziomie modułu MTA i modułach filtrujących na podstawie parametrów: odbiorca, nadawca, nazwa załącznika, temat wiadomości, sender hostname lub IP, nazwa reguły filtrującej, Message ID, nazwa wirusa, numer sesji. 22. System musi zapewniać możliwość tworzenia własnych reguł filtrowania treści w oparciu o: adresy IP nadawców odbiorców, adresy email, typ i rozmiar załącznika, ilość załączników, treść maila, pola nagłówka wiadomości, treść załączników. 23. System musi umożliwiać tworzenie własnych reguł filtrowania lub klonowania istniejących. 24. System musi umożliwiać tworzenie słowników słów kluczowych. 25. System musi zapewniać mechanizm weryfikacji poprawności nazwy odbiorcy na podstawie zapytań wysyłanych do serwera LDAP, SMTP lub lokalnego repozytorium użytkowników. 26. System musi zapewniać wsparcie dla standardu Sender Policy Framework (SPF). 27. System musi zapewniać wsparcie dla standardu Domain Keys Identified Mail (DKIM). 28. System musi zapewniać wsparcie dla standardu Domain-based Message Authentication Reporting & Conformance (DMARC). 29. Ochrona antywirusowa musi być realizowana poprzez silniki zasilane w sygnatury oraz filtr analizy heurystycznej wykrywający ataki typu zero hour. 30. System musi umożliwiać przegląd ostatnich infekcji oraz listę najczęstszych zagrożeń. 31. Aktualizacje sygnatur modułu antywirusowego muszą być dostępne nie rzadziej niż raz na dobę. 32. System musi zapewniać możliwość tworzenia wielu polityk ochrony antywirusowej przydzielanych w oparciu o: adresy IP serwera nadawcy, adres email nadawcy/odbiorcy wiadomości. 33. System musi zapewniać możliwość definiowania różnych sposobów postępowania z zainfekowanymi wiadomościami w zależności od rodzaju wykrytego wirusa. 34. System musi zapewniać możliwość określenia zasad postępowania z zabezpieczonymi wiadomościami (zawierającymi załączniki chronione hasłem, podpisanymi kluczem kryptograficznym lub zabezpieczonymi S/MIME, DKIM). 35. Moduł detekcji spamu musi bazować na metodzie zaawansowanej analizy heurystycznej, która wyklucza konieczność ręcznego tworzenia reguł w razie pojawienia się nowych technik omijania filtrów antyspamowych. 36. System musi umożliwiać korzystanie ze źródeł producenta, niepublicznych serwerów badania reputacji nadawców maila. 37. System musi zapewniać możliwość automatycznej oceny reputacji źródła przesyłanego maila (na podstawie weryfikacji ilości połączeń, procentowej ilości maili z wirusami, procentowej ilości wiadomości sklasyfikowanych jako spam) z możliwością limitowania ilości odbieranych wiadomości w określonej jednostce czasu od źródeł o niskiej reputacji. 38. System musi zapewniać możliwość definiowania reguł antyspamowych na poziomie całego systemu, grup użytkowników oraz pojedynczych użytkowników. 39. System musi zapewniać możliwość tworzenia systemowych list bezpiecznych i zablokowanych nadawców, odbiorców, hostów, domen lub adresów IP. 40. System musi zapewniać inteligentne rozpoznawanie typów analizowanych załączników. Zmiana rozszerzeń powinna być ignorowana przez system i nie powinna być metodą omijania tego typu filtra. 41. System musi zapewniać ochronę przeciwko atakom typu Odmowa dostępu do usługi (Denial Of Service) oraz wykrywać i blokować próby enumeracji kont użytkowników chronionej domeny pocztowej (Directory Harvesting Attack). 42. System musi posiadać mechanizm ochrony przed zjawiskiem wykorzystania wiadomości niedostarczonych (Fake NDR – Non-Delivery Receipt) za pomocą cyfrowego oznaczenia wiadomości wysyłanych z chronionych domen organizacji). 43. System musi zapewniać możliwość szyfrowania przesyłek za pomocą protokołu Transport Layer Security. |
| Ochrona przed atakami ukierunkowanymi | 1. System musi zapewniać mechanizmy ochrony przed zaawansowanymi lub nieznanymi atakami ukierunkowanymi, które wykorzystują załączniki lub hiperłącza (adresy URL) w celu zainstalowania na urządzeniu użytkownika szkodliwego oprogramowania lub skłonienia użytkownika do ujawniania haseł lub innych poufnych danych. 2. Moduł ochrony przed zaawansowanymi lub nieznanymi atakami ukierunkowanymi musi stanowić integralną część systemu i nie może wymagać zastosowania dodatkowej maszyny wirtualnej lub urządzenia fizycznego. 3. Moduł ochrony przed zaawansowanymi lub nieznanymi atakami ukierunkowanymi musi zapewniać przynajmniej mechanizmy ochrony przed:    1. Niebezpiecznymi załącznikami.    2. Niebezpiecznymi hiperłączami (adresami URL prowadzącymi do niebezpiecznych stron WWW typu phishing lub malware). 4. Moduł ochrony przed zaawansowanymi lub nieznanymi atakami ukierunkowanymi musi umożliwiać zatrzymanie analizowanej wiadomości w systemowej kolejce do momentu otrzymania werdyktu o zagrożeniu w analizowanym załączniku lub łączu URL wiadomości. 5. System musi zapewniać możliwość wyboru trybu analizy załączników przez moduł ochrony przed zaawansowanymi lub nieznanymi atakami ukierunkowanymi przynajmniej w zakresie:    1. sprawdzenia wyłącznie reputacji pliku poprzez porównaniu jego skrótu z bazą skrótów znanych zagrożeń.    2. wieloetapowej analizy dynamicznej, obejmującej uruchomienie pliku w izolowanym środowisku typu sandbox. 6. Środowisko analizy dynamicznej typu sandbox powinno być elementem modułu ochrony przed zaawansowanymi lub nieznanymi atakami ukierunkowanymi. 7. W celu zapewnienia wysokiej dostępności, wydajności i skalowalności systemu, środowisko analizy dynamicznej typu sandbox musi pochodzić od tego samego producenta co oferowany system ochrony poczty elektronicznej i być dostarczane w modelu oprogramowanie jako usługa (SaaS). 8. Zbiór analizowanych typów plików przez moduł ochrony przed zaawansowanymi lub nieznanymi atakami ukierunkowanymi powinien obejmować przynajmniej:    1. MS Office (Word, Excel, Power Point).    2. PDF.    3. Adobe Flash.    4. HTML, TXT, RTF.    5. EML.    6. Pliki skompresowane (ZIP, TAR, RAR, GZIP, 7ZIP). 9. W przypadku analizy plików zabezpieczonych hasłem (zaszyfrowanych), system powinien podjąć próbę odszyfrowania tych plików wykorzystując słowa lub ciągi słów, wybrane metodą heurystyczną, z treści analizowanej wiadomości. 10. System musi umożliwiać określenie maksymalnego dopuszczalnego czasu analizy załączników przez moduł ochrony przed nieznanymi zagrożeniami i atakami ukierunkowanymi oraz wybór odpowiedniej dyspozycji na wiadomości (prześlij dalej / zablokuj / zatrzymaj w kwarantannie) w przypadku przekroczenia tego czasu. 11. Moduł ochrony przed niebezpiecznymi hiperłączami (adresami URL prowadzącymi do stron typu phishing lub malware) musi wykorzystywać mechanizmy analizy predykcyjnej w celu identyfikacji podejrzanych hiperłączy i wiadomości, zanim wiadomości zostaną dostarczone na skrzynki odbiorcze użytkowników. Proces wyszukiwania podejrzanych hiperłączy oraz analiza dynamiczna stron internetowych, do których te łącza prowadzą, musi być realizowany przez producenta systemu na zbiorze przynajmniej 50 milionów unikalnych adresów URL na minutę i być niezależny od wiadomości dostarczanych do organizacji Zamawiającego. 12. Ochrona przed niebezpiecznymi hiperłączami musi polegać na przepisywaniu adresów URL zawartych w treści wiadomości lub w jej załącznikach do formatu umożliwiającego śledzenie kliknięć użytkowników i zablokowania prób wejścia użytkowników na niebezpieczne strony WWW. 13. Po kliknięciu przez użytkownika w hiperłącze poddane analizie predykcyjnej, w oknie przeglądarki internetowej użytkownika musi zostać wyświetlony:     1. komunikat o wykrytym zagrożeniu i zablokowaniu wejścia na żądaną stronę.     2. oryginalna strona WWW – jeśli w wyniku przeprowadzonej analizy nie znaleziono zagrożenia. 14. W przypadku kliknięcia przez użytkownika w hiperłącze nieobjęte analizą predykcyjną, w oknie przeglądarki internetowej użytkownika musi zostać wyświetlona oryginalna strona WWW, a system musi rozpocząć analizę tej strony w środowisku sandbox. Proces analizy dynamicznej musi być transparentny dla użytkownika. W przypadku wykrycia zagrożenia, system musi wygenerować alarm o odpowiednim poziomie krytyczności (Major lub Critical), wysłać mailowe powiadomienie do administratorów o zaistniałym zdarzeniu oraz przekazać w sposób automatyczny alarm, wraz z informacjami o zaistniałym zdarzeniu, do systemu klasy SOAR, który podejmie w sposób automatyczny odpowiednie reakcje naprawcze. 15. Wraz z modułem ochrony przed nieznanymi zagrożeniami i atakami ukierunkowanymi, producent systemu musi zapewnić dostęp do portalu WWW prezentującego informacje o wykrytych zagrożeniach, w zakresie min.: wektor ataku (załącznik / hiperłącze), źródło i cel ataku, atrybuty wiadomości będącej nośnikiem ataku, wykorzystana technika ataku, poziom krytyczności wykrytego zagrożenia, globalny zasięg ataku oraz dostarczać materiały dowodowe (forensics) w postaci min. list adresów URL, IP lub DNS powiązanych z wykrytymi zagrożeniami. 16. Portal WWW musi dostarczać sumaryczne raporty efektywności modułu ochrony przed nieznanymi zagrożeniami i atakami ukierunkowanymi, identyfikować użytkowników, którzy weszli w bezpośrednią interakcję z wykrytymi przez system zagrożeniami (kliknęli w hiperłącze prowadzące do niebezpiecznej strony malware bądź phishing lub otrzymali wiadomość z niebezpiecznym załącznikiem) oraz tworzyć i stale utrzymywać dynamiczną listę najczęściej atakowanych osób w organizacji Zamawiającego. Lista musi zawierać min. adresy email atakowanych użytkowników oraz wskazywać typy wykrytych ataków (credential phishing / corporate credential phishing / malware / ransomware, RAT, etc.) wraz z ich rozkładem procentowym w rozbiciu na każdego użytkownika ujętego na liście. 17. Dla kont pocztowych z listy najczęściej atakowanych użytkowników system musi posiadać dodatkowe zabezpieczenie w formie izolowanej przeglądarki internetowej, tak aby uniemożliwić ściąganie złośliwego kodu przy użyciu adresów URL zawartych w poczcie kierowanej do tej grupy pracowników. |
| Informacje dodatkowe | 1. Administrator musi mieć możliwość zapisu konfiguracji na zewnętrzny nośnik i odtworzenia zapisanej wcześniej konfiguracji. 2. System musi umożliwiać automatyczne wykonywanie kopii zapasowej konfiguracji zgodnie z ustalonym harmonogramem. 3. Wszystkie aktualizacje muszą być pobierane z jednego miejsca a system komunikować się ze źródłem aktualizacji z częstotliwością narzuconą przez administratora systemu. 4. System musi zapewnić śledzenie historii wykonywania aktualizacji. 5. System musi umożliwiać tworzenie wielu administratorów oraz przypisanie im odpowiednich uprawnień dostępowych do modułów ochronnych. 6. System musi zapewniać rozbudowany system raportowania zapewniający dostęp do minimum 65 różnych rodzajów graficznych raportów oraz możliwość tworzenia własnych. 7. System w momencie dostarczenia lub po odtworzeniu musi zawierać zestaw predefiniowanych raportów. 8. Administrator musi mieć możliwość okresowej publikacji wybranych raportów jako strony WWW lub przy pomocy wysyłanych automatycznie wiadomości email. 9. System musi umożliwiać eksport logów do formatu CSV oraz XML. 10. System musi umożliwiać logowanie na lokalnym dysku twardym lub zewnętrznym serwerze. System musi mieć możliwość przechowywania logów Syslog, zdarzeń podejmowanych przez filtry oraz zdarzeń dotyczących komunikacji SMTP przez minimum 365 dni. |