

**Część 4**

**PARAMETRY MINIMALNE:**

1. **Oprogramowanie Email Secure Gateway – 90 sztuk.**

Oprogramowanie do skanowania wiadomości e-mail  90 sztuk, na okres do 30.06.2026 r.

|  |  |
| --- | --- |
| Część składowa/ cechy podstawowe | Minimalne wymagane parametry |
| Funkcjonalność | Oprogramowanie realizujące co najmniej funkcje ochrony przed złośliwymi załącznikami w wiadomościach e-mail |
| Licencjonowanie | Usługa rozliczana w cyklu miesięcznym lub rocznym. Cena rozliczenia może ulec zmianie w przypadku, gdy zamawiający zmieni liczbę chronionych skrzynek  i/lub zrezygnuje lub dołączy dodatkowe funkcjonalności.  W czasie trwania usługi to dostawca jest odpowiedzialny za konfiguracje oraz zarządzanie usługą. |
| Opis właściwości oprogramowania | 1. Oprogramowanie musi wspierać co najmniej skrzynki pocztowe:  * Gmail * Microsoft 365  1. Oprogramowanie musi posiadać, co najmniej poniższe funkcjonalności:  * Ochrona antymalware, chroniąca przed otrzymaniem załącznika wiadomości e-mail, będącego malware. * Ochrona antyspam, skanująca wiadomości pod kątem spamu. * Skanowanie załączonych linków URL pod kątem spamu oraz szkodliwości * Analiza DMARC * Ochrona przed phishingiem * Ochrona przed podszywaniem się pod pracowników firmy. * Skanowanie załączników pod kątem wirusów * Możliwość automatycznego unieszkodliwienia podejrzanych załączników lub ich usunięcia, a następnie przesłanie wiadomości do adresata * Grafy, umożliwiające w łatwy sposób zweryfikowanie działanie systemu. Grafy obejmować powinny minimum ilość incydentów, sposoby ataku z podziałem na ostatni dzień, ostatni tydzień, ostatni miesiąc oraz inne, nietypowe przedziały czasowe * Możliwość wygenerowania raportów, celem analizy działania systemu i ilości alertów * Konsola powinna zawierać możliwość przesłania plików oraz adresów URL do analizy * Możliwość utworzenia tak zwanych użytkowników VIP, celem zaostrzenia ochrony przed podszywaniem się pod wyżej wymienionych użytkowników |

1. **Oprogramowanie do wykonywania kopii zapasowych – 1 sztuka.**

Oprogramowania do zabezpieczania danych poprzez mechanizm kopi zapasowych dedykowane dla środowisk wirtualizacyjnych.

1. Oprogramowanie musi wspierać co najmniej systemy operacyjne:
   * Dla hosta:
     + VMware ESX/ESX(i) 5.0, 5.1, 5.5, 6.0, 6.5, 6,7.
     + Hyper-V.
     + Citrix XenServer.
     + Red Hat Virtualization.
     + Linux KVM.
     + Oracle VM Server.
   * Dla maszyn wirtualnych:
     + Windows XP (SP3) i nowsze.
     + Windows Server 2003 i nowsze.
     + Windows SBS 2011/2008, 2003/2003R2.
     + Windows Storage Server 2012/2012R2, 2008R2/2008/2003.
     + Windows MultiPoint Server 2012/2011/2010.
     + Linux OS.
     + macOS.

1. Zarządzanie systemem kopii zapasowych musi posiadać, co najmniej poniższe funkcjonalności:
   * Interfejs zarządzania oparty na przeglądarce WWW. Zgodność interfejsu z większością popularnych przeglądarek www.
   * Interfejs musi być zgodny z platformami mobilnymi (możliwość zarządzania systemem z poziomu urządzenia mobilnego).
   * Interfejs musi oferować możliwość prezentacji najważniejszych danych dotyczących stanu systemu i zadań przez niego realizowanych w przejrzystej formie graficznej z możliwością dostosowania zawartości, treści i formy prezentacji poszczególnych danych.
   * Moduł raportujący z możliwością zdefiniowania zawartości, formy i częstotliwości generowania raportów oraz metody ich dostarczania (wysyłanie na podany adres email lub zapisywanie do wskazanego folderu).
   * Definiowanie uprawnień dla administratorów system kopi zapasowych na poziomie dostępu do poszczególnych obiektów (maszyn, hostów, lokalizacji, modułów, itp.).
   * Integracja z MS Active Directory na poziomie zarządzania dostępem i administratorami.
   * Wsparcie dla Single Sign On dla logowania do systemu.
   * Zarządzanie procesem tworzenia kopi zapasowych dla wielu różnych podsieci, również w przypadku stosowania NAT.
   * Definiowanie planów wykonywania kopii zapasowych, ich replikacji i zarządzaniem ich retencją (kasowaniem).
   * Tworzenie zcentralizowanych (obejmujących swym zasięgiem wiele maszyn lub ich grupy) planów wykonywania kopi zapasowych.
   * Zdalna instalacja agentów kopi zapasowych na maszynach z systemem operacyjnym Windows.
   * Zdalne uaktualniania agentów kopi zapasowych.
   * Zdalne zarządzanie procesem wykonywania kopii zapasowej i odzyskiwania danych.
   * Możliwość zdefiniowania dedykowanej maszyny, której agent kopi zapasowej wykonywał będzie czynności zarządzania i replikacji kopii zapasowych z wielu innych maszyn (zadania kopiowania, przenoszenia, konsolidacji plików kopi zapasowej).
   * Możliwość zastosowania zcentralizowanych modułów do zarządzania przechowywaniem plików kopii zapasowych.
   * Centralny katalog wszystkich danych zapisanych w kopiach zapasowych
   * Wbudowany serwer PXE umożliwiający bootowanie maszyn przez sieć LAN z przygotowanego nośnika startowego.
2. Wykonywanie kopii zapasowych musi posiadać, co najmniej poniższe funkcjonalności:
   * Kopie zapasowe całych dysków i partycji.
   * Kopie zapasowe wybranych plików i folderów.
   * Technologia bezagentowego wykonywania kopii zapasowej dla maszyn wirtualnych (dotyczy Hyper-V i VMWare ESXi).
   * Kopie zapasowe aplikacji (Exchange, SQL, SharePoint, Active Directory)
   * Kopie zapasowe baz danych Oracle.
   * Kopie zapasowe hostów Hyper-V i VMWare ESXi.
   * Zapis kopi zapasowych (plikowych i dyskowych) w magazynie chmurowym dostarczanym przez producenta systemu kopi zapasowych.
   * Zapis kopi zapasowych na udziały sieciowe.
   * Zapis kopi zapasowych na serwer SFTP..
   * Zapis kopi zapasowych na dedykowaną ukrytą partycję na maszynie, której kopia zapasowa jest wykonywana.
   * Zapis kopi zapasowych na urządzenia taśmowe (pojedyncze napędy, biblioteki taśmowe, autoloadery).
   * Możliwość wyszukiwania plików w kopiach zapasowych.
   * Szyfrowanie plików kopi zapasowych.
   * Wsparcie dla technologii VSS.
   * Deduplikacjia kopi zapasowych na poziomie bloków danych. Deduplikacja wykonywana na źródle w celu ograniczenia ilości danych przesyłanych przez sieć.
   * Kompresja plików kopi zapasowych.
   * Replikacja kopi zapasowych na kolejne nośniki (dyski, napędy taśmowe, magazyn chmurowy).
   * Możliwość zaplanowania zadań związanych weryfikacją, replikacją i retencją plików kopi zapasowych.
3. Oprogramowanie musi umożliwiać odtwarzanie kopii zapasowych w oparciu o co najmniej:
   * Odtworzenie całej maszyny (Windows, Linux, Mac) – tzw. Bare Metal Restore
   * Odtworzenie całej maszyny (Windows, Linux, Mac) na innej platformie sprzętowej niż ta, z której wykonano kopię zapasową.
   * Odtworzenie całego hosta (Hyper-V i VMWare ESXi) na takiej samej lub innej platformie sprzętowej.
   * Odtworzenie poszczególnych plików i folderów.
   * Automatyzacja procesu odtwarzania całych maszyn – np.: po zabootowania maszyny z przygotowanego wcześniej nośnika, powinna zostać odtworzona ostatnia wykonany kopia zapasowa automatycznie, bez konieczności jej wyszukiwania i wskazywania).
   * Granularne odtwarzanie baz danych Microsoft Exchange.
   * Granularne odtwarzanie skrzynek pocztowych i poszczególnych wiadomości email z Microsoft Exchange.
   * Wyszukiwanie i podgląd odtwarzanych wiadomości email.
   * Granularne odtwarzanie baz danych Microsoft SQL.
   * Granularne odtwarzanie witryn i plików Microsoft SharePoint.
   * Odtwarzanie kontrolerów domeny Microsoft Active Directory.
   * Granularne odtwarzanie baz danych Oracle.
   * Dla hostów VMware ESXi i Hyper-V – uruchomienie maszyny wirtualnej bezpośrednio z pliku kopii zapasowej bez konieczności odtwarzania całej maszyny na hoście. Możliwość docelowego odtworzenia uruchomionej maszyny z pliku kopii zapasowej na wybranym hoście bez przerywania jej pracy.
4. Dodatkowe wymagania związane ochroną danych:
   * Ochrona systemów operacyjnych Windows przed złośliwym oprogramowaniem typu ransomware w oparciu o heurystyczne algorytmy identyfikacji i eliminacji zagrożeń
5. Wymagania co do modelu licencjonowania rozwiązania:
   * Możliwość zakupu licencji subskrypcyjnych w okresie 1/3/5 lat
   * Model licencjonowania oparty na maszynach fizycznych i hostach – brak limitów na chronioną ilość danych, maszyn wirtualnych i aplikacji)