Załącznik nr 2A

**I. URZĄDZENIE DO KONTROLI DOSTĘPU DO SIECI LAN ZAMAWIAJĄCEGO Z SYSTEMEM**

Producent: …………………………………………………………………………………………………………..

Nazwa oprogramowania : ……………………………………………………………………………………

|  |  |  |
| --- | --- | --- |
| **LP** | **Charakterystyka (wymagania minimalne)** | **Parametr oferowany** |
|  | Rozwiązanie na platformie sprzętowej dostarczone gotowe do użycia bez konieczności instalacji oprogramowania; | Spełnia : TAK / NIE\* |
|  | Platforma sprzętowa posiada co najmniej 2 interfejsy Gigabit w pełni konfigurowalne. System pozwala na konfigurację pracy urządzenia w co najmniej 15 sieciach VLAN; | Spełnia : TAK / NIE\* ………. interfejsy Gigabit  w pełni konfigurowalne. System pozwala na konfigurację pracy urządzenia w ……. sieciach VLAN |
|  | System pracuje w sieci co najmniej 85 hostów; | Spełnia : TAK / NIE\* praca w sieci ……….. hostów |
|  | Urządzenie zapewnia możliwość skanowania wszystkich urządzeń w infrastrukturze sieciowej.  Licencja rozwiązania na posiadane moduły bezpieczeństwa i kontroli dostępu do sieci nie jest ograniczona; | Spełnia : TAK / NIE\* |
|  | Produkt jest autoryzowanym produktem korzystającym z bazy CVE (zarówno bazy głównej jak i bazy kandydatów) oraz bazy NVD (NationalVulnerability Database); | Spełnia : TAK / NIE\* |
|  | Działanie badania podatności infrastruktury oparte na minimum trzech bazach  w tym bazy CVE i NVD ; | Spełnia : TAK / NIE\* |
|  | Możliwość wykrywania luk bezpieczeństwa w dowolnych systemach sieciowych bez instalowania dodatkowych aplikacji na tych systemach; | Spełnia : TAK / NIE\* |
|  | Możliwość weryfikacji bezpieczeństwa sieci w oparciu o normy bezpieczeństwa minimum: ISO27001/ISO17799, Sarbanes-Oxley, PCI-DSS; | Spełnia : TAK / NIE\* |
|  | Rozwiązanie posiada wbudowany system zarządzania zagrożeniami, przydzielania zleceń naprawy systemów wybranym pracownikom z możliwością nadzorowania postępu prac; | Spełnia : TAK / NIE\* |
|  | Urządzenie oferuje szczegółowe raporty zawierające opisy wykrytych luk bezpieczeństwa wraz z informacją o możliwości ich wyeliminowania z danego systemu; | Spełnia : TAK / NIE\* |
|  | System posiada wbudowany system raportowania z możliwością tworzenia podsumowań dla wskazanych systemów. System raportowania umożliwia tworzenie raportów dla administratorów, a także ogólnych raportów podsumowujących poziom bezpieczeństwa. Raporty są dostępne minimum  w formatach PDF oraz xml; | Spełnia : TAK / NIE\* |
|  | System posiada mechanizm wykrywania aktywnego malware oraz aktywacji linków phishingowych przez użytkowników sieci. Na bazie zintegrowanych mechanizmów system blokuje hosty zainfekowane malware lub aktywujące linki phishingowe; | Spełnia : TAK / NIE\* |
|  | System umożliwia wykrywanie i automatyczne blokowanie nieautoryzowanego dostępu do infrastruktury sieciowej w oparciu o zintegrowany, bezagentowy system Network Access Control; | Spełnia : TAK / NIE\* |
|  | System umożliwia wykrywanie i klasyfikowanie wszystkich urządzeń pracujących  w infrastrukturze; | Spełnia : TAK / NIE\* |
|  | Rozwiązanie posiada system wykrywania zmian w obrębie infrastruktury sieciowej i powiadamiania administratorów o każdej zanotowanej zmianie.  Powiadomienia nie są wysyłane później niż 30 sekund po zanotowaniu zdarzenia; | Spełnia : TAK / NIE\* |
|  | System posiada mechanizm automatycznego skanowania pod kątem występowania podatności i luk bezpieczeństwa zaufanych systemów podłączających się do infrastruktury sieciowej; | Spełnia : TAK / NIE\* |
|  | System wykrywa wszelkie anomalia sieciowe związane z MAC spoofing; | Spełnia : TAK / NIE\* |
|  | Możliwość integracji ze smartswitchami (co najmniej HP, 3COM, CISCO, Extreme Networks, D-Link, Dell, Alcatel oraz Juniper); | Spełnia : TAK / NIE\* |
|  | System umożliwia automatyczne przełączanie hostów niezaufanych do nowopowstałego VLANu (tzw. Blackhole) lub do wskazanego przez administratora VLAN o niskim priorytecie dostępu; | Spełnia : TAK / NIE\* |
|  | Rozwiązanie pozwala na tworzenie użytkowników mających dostęp do interfejsu webowego na trzech różnych poziomach – managera, pracownika IT i operatora NAC; | Spełnia : TAK / NIE\* |
|  | Możliwość wykrywania i powiadamiania o pojawieniu się w sieci hostów z danej puli adresów IP; | Spełnia : TAK / NIE\* |
|  | Możliwość monitorowania aktywności hostów i powiadamianie w przypadku braku łączności z monitorowanymi systemami/urządzeniami; | Spełnia : TAK / NIE\* |
|  | Zarządzanie przez interfejs webowy, bez konieczności używania maszyny Javy ani dodatkowego oprogramowania instalowanego na maszynie zarządzającej; | Spełnia : TAK / NIE\* |
|  | Praca urządzenia możliwa w sieciach z adresacją statyczną oraz w środowisku DHCP; | Spełnia : TAK / NIE\* |
|  | Urządzenie umożliwia określenie wykrytych luk bezpieczeństwa jako tzw. falsepositive oraz posiada możliwość generowania raportów podsumowujących,  a także zbiorczych raportów dla osób zarządzających; | Spełnia : TAK / NIE\* |
|  | Minimum 3 tryby audytowe: pełny, porównawczy oraz inkrementalny; | Spełnia : TAK / NIE\*  Posiadane tryby audytowe:  ……………………………………. |
|  | Minimum roczna subskrypcja aktualizacji baz zagrożeń oraz firmware i roczne wsparcie techniczne producenta. W ramach maintenance roczna gwarancja na urządzenie. | Spełnia : TAK / NIE\*  - ……………miesięcy gwarancji na urządzenie;  - ……………miesięcy na subskrypcję aktualizacji baz zagrożeń;  - ………….. miesięcy wsparcia technicznego. |

**II. OPROGRAMOWANIE DO BACKUP-U.  
1. Oprogramowania do zabezpieczania danych poprzez mechanizm kopii zapasowych dedykowane dla**

**środowisk wirtualizacyjnych.**

Producent: …………………………………………………………………………………………………………..

Nazwa oprogramowania : ……………………………………………………………………………………

|  |  |  |
| --- | --- | --- |
| **LP** | **Charakterystyka (wymagania minimalne)** | **Parametr oferowany** |
| 1. | 1. Wspierane systemy operacyjne   1). Dla hosta:   * + - VMware ESX/ESX(i) 5.0, 5.1, 5.5, 6.0, 6.5;     - Hyper-V;   2). Dla maszyn wirtualnych   * + - Windows 10,Windows 8/8.1/7/XP, Windows Vista;     - Windows Server 2016,Windows Server 2012/2012R2, Windows Server 2008/2008R2, Windows Server 2003/2003R2;     - Windows SBS 2011/2008, 2003/2003R2;     - Windows Storage Server 2012/2012R2, 2008R2/2008/2003;     - Windows MultiPoint Server 2012/2011/2010;     - Linux OS (wiele dystrybucji);     - macOS.  1. 2. Wymagania związane z zarządzaniem systemem kopii zapasowych i wymagania co do oczekiwanych funkcjonalności:  * Interfejs zarządzania oparty na przeglądarce WWW. Zgodność interfejsu  z większością popularnych przeglądarek www; * Interfejs zgodny z platformami mobilnymi (możliwość zarządzania system  z poziomu tabletu); * Zarządzanie procesem tworzenia kopii zapasowych dla wielu różnych podsieci, również w przypadku stosowania NAT; * Definiowanie planów wykonywania kopii zapasowych, ich replikacji  i zarządzaniem ich retencją (kasowaniem); * Zdalna instalacja agentów kopii zapasowych na maszynach z systemem operacyjnym Windows; * Zdalne uaktualniania agentów kopii zapasowych; * Zdalne zarządzanie procesem wykonywania kopii zapasowej i odzyskiwania danych.  1. Wymagane związane z wykonywaniem kopii zapasowych:  * 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 hostów Hyper-V i VMWare ESXi; * Zapis kopii zapasowych (plikowych i dyskowych) w magazynie chmurowym dostarczanym przez producenta systemu kopii zapasowych; * Zapis kopii zapasowych na udziały sieciowe; * Zapis kopii zapasowych na serwer SFTP ; * Zapis kopii zapasowych na dedykowaną ukrytą partycję na maszynie, której kopia zapasowa jest wykonywana; * Wyszukiwanie plików w kopiach zapasowych; * Szyfrowanie plików kopii zapasowych; * Wsparcie dla technologii VSS; * Kompresja plików kopii zapasowych; * Replikacja kopii zapasowych na kolejny nośnik (dysk, magazyn chmurowy) .  1. Wymagania związane z odtwarzaniem danych z kopii zapasowych:  * 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 całej maszyny wirtualnej; * Odtworzenie całego hosta (Hyper-V i VMWare ESXi) na takiej samej lub innej platformie sprzętowej; * Odtworzenie poszczególnych plików i folderów; * 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 ; * 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.  1. Dodatkowe wymagania związane ochroną danych:  * Ochrona systemów operacyjnych Windows przed złośliwym oprogramowaniem typu ransomware w oparciu o heurystyczne algorytmy identyfikacji i eliminacji zagrożeń . * Zapis kopii zapasowych na udziały sieciowe; * Zapis kopii zapasowych na serwer SFTP; * Zapis kopii zapasowych na dedykowaną ukrytą partycję na maszynie, której kopia zapasowa jest wykonywana; * Zapis kopii zapasowych na urządzenia taśmowe (pojedyncze napędy, biblioteki taśmowe, autoloadery); * Możliwość wyszukiwania plików w kopiach zapasowych; * Szyfrowanie plików kopii zapasowych; * Wsparcie dla technologii VSS; * Deduplikacja kopii zapasowych na poziomie bloków danych. Deduplikacja wykonywana na źródle w celu ograniczenia ilości danych przesyłanych przez sieć; * Kompresja plików kopii zapasowych; * Replikacja kopii zapasowych na kolejne nośniki (dyski, napędy taśmowe, magazyn chmurowy); * Możliwość zaplanowania zadań związanych weryfikacją, replikacją i retencją plików kopii zapasowych.   4. Wymagania związane z odtwarzaniem danych z kopi zapasowych:   * 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 zabootowaniu 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.   5.Dodatkowe wymagania związane ochroną danych:   * Ochrona systemów operacyjnych Windows przed złośliwym oprogramowaniem typu ransomware w oparciu o heurystyczne algorytmy identyfikacji i eliminacji zagrożeń.   6. Wymagania co do modelu licencjonowania rozwiązania:   * Możliwość wyboru przy zakupie licencji dożywotnich i subskrypcyjnych; * Model licencjonowania oparty na maszynach fizycznych i hostach – brak limitów na chronioną ilość danych, maszyn wirtualnych i aplikacji). | Spełnia : TAK / NIE \* |
| 2. | Wsparcie Producenta oraz uprawnienia do aktualizacji: minimum 12 miesięcy | Spełnia TAK / NIE\*  …………………… miesięcy wsparcia technicznego.  ……………………miesięcy uprawnień do aktualizacji. |

**2). Oprogramowania do zabezpieczania danych poprzez mechanizm kopii zapasowych dedykowane dla   
 środowisk serwerowych**

Producent: …………………………………………………………………………………………………………..

Nazwa oprogramowania : ……………………………………………………………………………………

|  |  |  |
| --- | --- | --- |
| **LP** | **Charakterystyka (wymagania minimalne)** | **Parametry oferowane** |
| 1. | 1. Wspierane systemy operacyjne:   * Windows 10, Windows 8/8.1/7/XP,Windows Vista; • Windows Server 2016, Windows Server 2012/2012R2, Windows Server   2008/2008R2, Windows Server 2003/2003R2;   * Windows SBS 2011/2008, 2003/2003R2; * Windows Storage Server 2012/2012R2, 2008R2/2008/2003; * Windows MultiPoint Server 2012/2011/2010; * Linux OS (wiele dystrybucji).   2. Wymagania związane z zarządzaniem systemem kopi zapasowych i wymagania co do oczekiwanych funkcjonalności:  • Interfejs zarządzania oparty na przeglądarce WWW. Zgodność interfejsu  z większością popularnych przeglądarek www;   * Interfejs musi być zgodny z platformami mobilnymi (możliwość zarządzania system z poziomu tabletu); * Zarządzanie procesem tworzenia kopii zapasowych dla wielu różnych podsieci, również w przypadku stosowania NAT;   • Definiowanie planów wykonywania kopii zapasowych, ich replikacji  i zarządzaniem ich retencją (kasowaniem);  • Zdalna instalacja agentów kopii zapasowych na maszynach z systemem operacyjnym Windows;  • Zdalne uaktualniania agentów kopii zapasowych;  • Zdalne zarządzanie procesem wykonywania kopii zapasowej i odzyskiwania danych.  3. Wymagane związane z wykonywaniem kopii zapasowych:  • Kopie zapasowe całych dysków i partycji;  • Kopie zapasowe wybranych plików i folderów;  • Kopie zapasowe aplikacji (Exchange, SQL, SharePoint, Active Directory);  • Zapis kopii zapasowych (plikowych i dyskowych) w magazynie chmurowym dostarczanym przez producenta systemu kopi zapasowych;  • Zapis kopii zapasowych na udziały sieciowe;  • Zapis kopii zapasowych na serwer SFTP;  • Zapis kopii zapasowych na dedykowaną ukrytą partycję na maszynie, której kopia zapasowa jest wykonywana;  • Wyszukiwanie plików w kopiach zapasowych;  • Szyfrowanie plików kopii zapasowych;  • Wsparcie dla technologii VSS;  • Kompresja plików kopii zapasowych;  • Replikacja kopii zapasowych na kolejny nośnik (dysk, magazyn chmurowy).  4. Wymagania związane z odtwarzaniem danych z kopii zapasowych:  • 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 całej maszyny wirtualnej;  • Odtworzenie poszczególnych plików i folderów;  • 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;  5. Dodatkowe wymagania związane ochroną danych:  • Ochrona systemów operacyjnych Windows przed złośliwym oprogramowaniem typu ransomware w oparciu o heurystyczne algorytmy identyfikacji i eliminacji zagrożeń. | Spełnia : TAK / NIE\* |
| 2. | Wsparcie techniczne oraz uprawnienia do aktualizacji min. 36 m-cy | Spełnia: TAK / NIE\*  …………………… miesięcy wsparcia technicznego.  ……………………miesięcy uprawnień do aktualizacji. |

**III. BEZPRZEWODOWY PUNKT DOSTĘPOWY.**

Producent: …………………………………………………………………………………………………………..

Nazwa oprogramowania : ……………………………………………………………………………………

|  |  |  |
| --- | --- | --- |
| **LP** | **Opis minimalnych parametrów** | **Parametry oferowane** |
|  | Urządzenie jest tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej. | Spełnia: TAK / NIE\* |
|  | Obudowa urządzenia wykonana z tworzywa sztucznego  i umożliwiać montaż na suficie wewnątrz budynku. | Spełnia: TAK / NIE\* |
|  | Urządzenie wyposażone w dwa niezależne moduły radiowe pracujące w pasmach i obsługiwać następujące standardy:  2.4 GHz b/g/n  5 GHz a/n/ac | Spełnia: TAK / NIE\* |
|  | Urządzenie pozwala na jednoczesne rozgłaszanie co najmniej 14 SSID | Spełnia: TAK / NIE\* |
|  | Liczba interfejsów Ethernet – 1 w standardzie 10/100/1000 Base-TX | Spełnia: TAK / NIE\* |
|  | Interfejs radiowy urządzenia wspiera następujące funkcje: MIMO – 2x2 | Spełnia: TAK / NIE\* |
|  | Maksymalna przepustowość interfejsu dla poszczególnych pasm:   1. 2.4GHz – 300Mbps 2. 5 GHz – 867 Mbps | Spełnia: TAK / NIE\* |
|  | Wymagana moc nadawania min. 19dBm | Spełnia: TAK / NIE\* |
|  | Wsparcie dla 802.11n 20/40Mhz HT | Spełnia: TAK / NIE\* |
|  | Wsparcie dla kanału 80 MHz dla 802.11ac | Spełnia: TAK / NIE\* |
|  | Anteny – 4 wbudowane o zysku min. 4dBi dla pasma 2.4GHz, 5dBi dla pasma 5GHz | Spełnia: TAK / NIE\* |
|  | Urządzenie zasilane poprzez interfejs ETH w standardzie 802.3at lub zewnętrzny zasilacz.  Wymagane jest dostarczenie przez dostawcę odpowiednich urządzeń zasilających. W przypadku zasilania poprzez port ETH wymagane jest dostarczenie modułów typu „powerinjector” w standardzie 802.3at wraz z odpowiednim zasilaczem. W przypadku zasilania urządzenia przez zewnętrzny zasilacz wymagane jest dostarczenie odpowiedniego zasilacza. | Producent: ………………………………………………..  Model:……………………………………………………….  Spełnia: TAK / NIE\* |
|  | Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres minimum 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 8 x 5. | Spełnia: TAK / NIE\*  - ……………miesięcy gwarancji na  urządzenie;  - ……………miesięcy uprawnień do  aktualizacji;  - ……………miesięcy wsparcia technicznego; |

\*- niepotrzebne skreślić

Wykonawca lub upoważniony

przedstawiciel wykonawcy

................................................

( podpis i pieczęć )

data:..................2018r