**Załącznik nr 7c Opis zamówienia ŁAGÓW**

1. **Zakup serwera do obsługi wdrażanych rozwiązań (1 sztuka) wraz z oprogramowaniem do serwera (1 sztuka) i 20 licencji dostępowych**

|  |  |
| --- | --- |
| **Lp.** | **Wymagane parametry minimalne** |
| 1 | Obudowa serwera typu Rack o wysokości maksymalnie 2U. Dostarczona wraz kompletem wysuwanych szyn i organizer okablowania, umożliwiającymi montaż w szafie rack i wysuwanie serwera do celów serwisowych. |
| 2 | Płyta główna – pozwalająca na zainstalowanie minimum dwóch procesorów zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |
| 3 | Chipset - dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych. |
| 4 | Procesory - zainstalowane dwa procesory maksimum 8-rdzeniowe klasy x86 uzyskujące w teście SPECrate2017\_int\_base dostępnym na stronie www.spec.org dla konfiguracji z dwoma procesorami wyniku minimum 72 punkty.  Maksymalna liczba rdzeni procesora ograniczona przez licencjonowanie objętego projektem oprogramowania. |
| 5 | Pamięć RAM – minimum 64GB DDR4 RDIMM. Płyta główna powinna obsługiwać do minimum 1TB pamięci RAM dla konfiguracji dwu-procesorowej.  Pojemność zastosowanych kości pamięci RAM min. 16 GB. |
| 6 | Zabezpieczenia pamięci RAM - Memory Rank Sparing, Memory Mirror, Lockstep lub równoważne |
| 7 | Gniazda PCI - minimum trzy sloty PCIe  x8, lub wydajniejsze |
| 8 | Interfejsy sieciowe:  minimum 2 porty typu Ethernet 1Gbps BaseT RJ45 zorganizowanych w dwóch kartach sieciowych. |
| 9 | Dyski twarde – dwa dyski o pojemności minimum 480GB SAS 6Gbps, pracujące w RAID1. |
| 10 | Sprzętowy kontroler RAID – kontroler RAID umożliwiający realizację RAID 1 i 5. |
| 11 | Wbudowane porty - minimum 2 porty USB 2.0 oraz 2 porty USB 3.0, 1 port RJ45 dedykowany do zarządzania, 2 porty VGA (1 na przednim panelu obudowy, drugi na tylnym), min. 1 port RS232. |
| 12 | Video - zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024 |
| 13 | Wentylatory - redundantne |
| 14 | Zasilacze - redundantne, Hot-Plug minimum 750W. |
| 15 | Karta Zarządzania - niezależna od zainstalowanego systemu operacyjnego, zintegrowana z płyta główną, posiadająca minimalną funkcjonalność :  - komunikacja poprzez interfejs RJ45,  - podstawowe zarzadzanie serwerem poprzez protokół IPMI 2.0, DCMI 1.5, SNMP, VLAN tagging,  - wbudowana diagnostyka,  - dostęp poprzez interfejs graficzny Web karty oraz z linii poleceń,  - monitorowanie temperatury oraz zużycia energii przez serwer w czasie rzeczywistym,  - lokalna oraz zdalna konfiguracja serwera,  - wsparcie dla IPv4 i IPv6,  - możliwość zdalnego dostępu do konsoli graficznej, zainstalowanego na serwerze systemu operacyjnego serwera. |
| 16 | Serwer musi być wyprodukowany zgodnie z normą  ISO-9001:2008 oraz ISO-14001 lub równoważnymi. Urządzenie musi być zgodne z normami UE i przeznaczone na rynek UE, musi posiadać certyfikat CE lub równoważny. |
| 17 | Dostarczone urządzenie musi być fabrycznie nowe, nieregenerowane i wyprodukowane najwcześniej w ciągu ostatnich 6 miesięcy przed dostawą, muszą pochodzić z oficjalnego kanału sprzedaży producenta na teren Polski |
| 18 | Licencje oprogramowania:  Licencja na oprogramowanie do serwera, obsługująca dostarczone procesory w serwerze – 1 szt.  Klienckie licencje dostępowe – 20 szt. |
| 19 | Oferowane urządzenie musi być objęte co najmniej 3-letnim wsparciem producenta  sprzętu w dni robocze, czas reakcji w miejscu instalacji sprzętu następny dzień roboczy. Pakiet serwisowy musi zawierać usługę pozostawiania bez opłat u Zamawiającego uszkodzonych dysków w okresie obowiązywania serwisu. |

1. **UPS do serwera (1 sztuka)**

|  |  |
| --- | --- |
| Lp. | **Wymagane parametry minimalne** |
|  | moc minimum: 1700VA/1350W 230V 50Hz |
|  | typ baterii: bateria wewnętrzna |
|  | port USB i RS232 |
|  | złącza minimum 8xIEC 320 C13 (10A) |
|  | wyłącznik awaryjny EPO |
|  | slot na kartę sieciową SNMP |
|  | wyświetlacz LCD |
|  | obudowa Rack |
|  | możliwość podłączenia dodatkowych baterii |
|  | moduł zarządzania UPS lub oprogramowanie umożliwiające nadzór i sterowanie w zakresie:  1) monitorowanie bieżących parametrów pracy urządzenia (napięcia wejściowe i wyjściowe, obciążenie, tryb pracy, temperatura)  2) dostęp do konsoli monitorowanie poprzez WWW z LAN.  3) zapisywanie historycznych danych,  4) wysyłanie mail odnośnie stanów alarmowych (zaniku napięcia, pracy na baterii, usunięciu alarmów) |
|  | karta komunikacyjna WEB/SNMP IPV4 do gniazda opcjonalnego. |
|  | Gwarancja 3 lata. |

1. **Zakup licencji do urządzenia UTM (1 sztuka)**

Zakup licencji Unified (UTM) Protection (8x5 FortiCare plus Application Control, IPS, AV, Web Filtering and Antispam, FortiSandbox Cloud) na 36 miesięcy dla urządzenia FortiGate 60D lub dostawa urządzenia o parametrach opisanych poniżej lub równoważnego:

|  |  |  |
| --- | --- | --- |
| Lp. | **Wymagane parametry minimalne** | |
|  | Producent rozwiązania musi posiadać udowodnioną pozycję lidera w zakresie bezpieczeństwa potwierdzone niezależnymi raportami. | |
|  | Producent rozwiązania musi posiadać dedykowaną szeroką gamę produktów dopasowanych do potrzeb klientów obejmujących małe biura po centra przetwarzania danych. | |
|  | Funkcjonalność bramy bezpieczeństwa | |
|  | Urządzenie powinno posiadać możliwość uruchomienia następujących funkcjonalności, dostarczonych przez jednego producenta: | Firewall |
|  | IPS |
|  | Zarządzanie identyfikacją użytkownika |
|  | System automatycznego wykrywania i klasyfikacji aplikacji wraz z filtrowaniem URL |
|  | Wykrywanie malware oraz komunikacji z serwerami C&C (wykrywanie działających botnetów) |
|  | Wykrywanie wiadomości SPAM |
|  | Brama IPSec VPN |
|  | Ochrona przed wyciekiem informacji (Data Loss Prevention) |
|  | Dostęp dla urządzeń mobilnych |
|  | Zarządzanie i konfiguracja |
|  | Rozwiązanie musi posiadać odpowiednie certyfikacje | Common Criteria |
|  | Urządzenie w formie appliance sprzętowego posiadające | LAN 10/100/1000Base-T Ports – 6 sztuk |
|  | DMZ 10/100/1000Base-T RJ-45 - 1 sztuka |
|  | WAN 10/100/1000Base-T RJ-45 port - 1 sztuka |
|  | Firewall | Rozwiązanie powinno posiadać inspekcję stanową opartą na granularnej analizie komunikacji oraz stanu aplikacji w celu poprawnego śledzenia i kontroli przepływu ruchu |
|  | Rozwiązanie powinno posiadać przepustowość firewalla nie mniejszą niż 1,95 Gb/s) |
|  | Urządzenie powinno pozwalać na kontrolę przynajmniej 150 predefiniowanych serwisów/protokołów |
|  | Urządzenie powinno posiadać możliwość zaraportowania ilości „trafień” wybranej polityki do aplikacji zarządzającej |
|  | Tworzenie reguł powinno pozwalać na ich konfiguracje w określonych interwałach czasowych wraz z podaniem daty lub godziny ich wygaśnięcia |
|  | Urządzenie musi posiadać możliwość konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika (Identity Firewall), integrując się ściśle z usługą katalogową Microsoft Active Directory |
|  | Powinno posiadać lokalną bazę użytkowników pozwalając na ich autentykację bez potrzeby korzystania z zewnętrznych rozwiązań |
|  | Urządzenie pracujące w klastrze musi umożliwiać pracę w trybie Transparent/Bridge |
|  | Rozwiązanie powinno wspierać wysoką dostępność (HA) wraz z dzieleniem obciążenia i synchronizacją stanu. |
|  | Urządzenie nie powinno posiadać ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej. |
|  | Rozwiązanie posiada możliwość komunikacji z serwerami uwierzytelnienia i autoryzacji za pośrednictwem protokołów RADIUS i TACACS+ |
|  | Powinno pozwalać na obsłużenie do 500000 jednoczesnych sesji/połączeń z prędkością zestawiania 19600 połączeń na sekundę |
|  | Wsparcie dla IPv6 | Rozwiązanie powinno pozwalać na obsługę IPv6 przez moduł Firewall, Kontroli Aplikacji, Antymalware, Filtrowania URL |
|  | Rozwiązanie powinno wspierać 6 do 4 NAT lub 6 do 4 tuneli |
|  | Powinna być zapewniona integracja z AD poprzez IPv6 |
|  | Urządzenie powinno nie mieć problemów z raportowaniem ruchu IPv6 oraz prezentacją tabel routingu dla IPv6 |
|  | Intrusion Prevention System (IPS) | Zapewniać skuteczność wykrywania zagrożeń i ataków na poziomie minimum 98% udokumentowany przez niezależne testy opublikowane w okresie ostatnich 18 miesięcy (np. niezależne testy NSS Labs) |
|  | Posiadać możliwość pracy w trybie in-line (wszystkie pakiety, które mają być poddane inspekcji muszą przechodzić przez system) |
|  | Posiadać możliwość pracy zarówno w trybie pasywnym (IDS) jak i aktywnym (z możliwością blokowania ruchu) |
|  | Posiadać możliwość wykrywania i uniemożliwiania szerokiej gamie zagrożeń (np.: złośliwe oprogramowanie, skanowanie sieci, ataki na usługi VoIP, próby przepełnienia bufora, ataki na aplikacje P2P, zagrożenia dnia zerowego, itp.) |
|  | Posiadać możliwość wykrywania modyfikacji znanych ataków jak i te nowo powstałe, które nie zostały jeszcze dogłębnie opisane, |
|  | Sposoby wykrywania zagrożeń – urządzenie musi posiadać | sygnatury ataków opartych na exploitach |
|  | reguły oparte na zagrożeniach |
|  | mechanizm wykrywania anomalii w protokołach |
|  | mieć możliwość inspekcji nie tylko warstwy sieciowej i informacji zawartych w nagłówkach pakietów, ale również szerokiego zakres protokołów na wszystkich warstwach modelu sieciowego włącznie z możliwością sprawdzania zawartości pakietu |
|  | posiadać mechanizm minimalizujący liczbę fałszywych alarmów jak i niewykrytych ataków (ang. false positives i false negatives) |
|  | mieć możliwość detekcji ataków/zagrożeń zgłoszonych z wielu elementów i korelacji wielu, pozornie niepowiązanych zdarzeń |
|  | posiadać wiele możliwości reakcji na zdarzenia takie jak: tylko monitorowanie, blokowanie ruchu zawierającego zagrożenia, zastąpienie zawartości pakietów oraz mieś możliwość zapisywania pakietów |
|  | posiadać możliwość pasywnego zbierania informacji o urządzeniach sieciowych oraz ich aktywności, takich jak systemy operacyjne, serwisy, otwarte porty, aplikacje oraz zagrożenia w celu wykorzystania tych informacji do analizy i korelacji ze zdarzeniami bezpieczeństwa, eliminowania fałszywych alarmów oraz tworzenia polityki zgodności |
|  | posiadać możliwość pasywnego gromadzenia informacji o przepływach ruchu sieciowego ze wszystkich monitorowanych hostów włączając w to czas początkowy i końcowy, porty, usługi oraz ilość przesłanych danych |
|  | zapewniać możliwość pasywnej detekcji predefiniowanych serwisów takich jak FTP, HTTP, POP3, Telnet, itp. |
|  | Posiadać możliwość automatycznej inspekcji i ochrony dla ruchu wysyłanego na niestandardowych portach używanych do komunikacji |
|  | Zapewniać możliwość obrony przed atakami skonstruowanym tak, aby uniknąć wykrycia przez IPS. W tym celu musi stosować najodpowiedniejszy mechanizm defragmentacji i składania strumienia danych w zależności od charakterystyki hosta docelowego |
|  | Zapewniać mechanizm bezpiecznej aktualizacji sygnatur. Zestawy sygnatur/reguł muszą byś pobierane z serwera w sposób uniemożliwiający ich modyfikację przez osoby postronne |
|  | zapewniać możliwość definiowania wyjątków dla sygnatur z określeniem adresów IP źródła, przeznaczenia lub obu jednoczenie być zarządzany tylko poprzez system centralnego zarzadzania za pomocą szyfrowanego połączenia |
|  | Zapewniać możliwość wykorzystanie informacji o sklasyfikowanych aplikacjach do tworzenia reguł IPS |
|  | zapewniać obsługę reguł Snort |
|  | mieć możliwość detekcji ataków i zagrożeń opartych na protokole IPv6 |
|  | mechanizm wykrywania anomalii w ogólnym zachowaniu ruchu sieciowego |
|  | Zapewniać mechanizmy automatyzacji co najmniej w zakresie wskazania hostów skompromitowanych |
|  | zapewniać mechanizmy automatyzacji w zakresie automatycznego dostrojenia polityk bezpieczeństwa |
|  | posiadać możliwość wykorzystania mechanizmów obsługi ruchu asymetrycznego firewalla dla uzyskania pełnej widoczności ruchu - w szczególności musi posiadać możliwość pracy w trybie failover firewalla oraz w trybie klastrowania |
|  |
|  | pozwalać na objęcie ochroną protokołów SCADA |
|  | pozwalać na ochronę protokołów VOIP |
|  | Identyfikacja użytkownika (User Identity) | Urządzenie musi w oparciu o zdarzenia być zdolne do identyfikacji użytkownika poprzez zadanie zapytań |
|  | Urządzenie musi pozwalać na identyfikację i autentykację użytkownika dla zasobów nie związanych z domeną |
|  | Urządzenie musi posiadać dedykowanego agenta instalowanego przez politykę pozwalającego na raportowanie i identyfikację użytkownika |
|  | Urządzenie musi wspierać środowiska terminalowe |
|  | Urządzenie musi integrować się z usługami katalogowymi, IF-MAP oraz RADIUS |
|  | Urządzenie musi powodować minimalny wpływ na kontrolery domeny |
|  | Urządzenie musi wspierać nagłówki pozwalającą na identyfikację użytkownika (np. X-forwarded) |
|  | System automatycznego wykrywania i klasyfikacji aplikacji wraz z filtrowaniem URL | Baza znanych aplikacji powinna zawierać nie mniej niż 7000 pozycji |
|  | Urządzenie musi pozwalać na kategoryzację adresów URL w liczbie przekraczającej 200000000 i pokrywać przynajmniej 85% adresów z listy top 1M serwisu Alexa |
|  | Urządzenie powinno pozwalać na musi umożliwiać tworzenie reguł zawierających wiele kategorii |
|  | Lokalny cache po 4 tygodniach powinien pozwalać na dostarczenie odpowiedzi na 99% zapytań |
|  | Filtrowanie URL powinno pozwalać na kategoryzację względem ryzyka danego adresu |
|  | Rozwiązanie powinno posiadać mechanizm ograniczenia użycia pasma |
|  | Rozwiązanie powinno posiadać mechanizm definiowania wyjątków na poziomie zdefiniowanego obiektu |
|  | Strona informująca o zablokowanym zasobie powinna być możliwa zdefiniowania, dodatkowo powinna umożliwiać na przekierowanie użytkownika na inna stronę. |
|  | Urządzenie powinno wspierać mechanizmy białych i czarnych list |
|  | Wykrywanie malware oraz komunikacji z serwerami C&C | Moduł wykrywający malware i botnety powinien być zintegrowaną z platformą aplikacją |
|  | System Anti-Bot powinien umożliwiać wykrycie oraz blokadę podejrzanego zachowania w chronionych segmentach sieci |
|  | Wykrycie zdarzenia powinno opierać na wielowarstwowej analizie (połączenie reputacji adresów URL, IP czy DNS połączonych z analizą cech charakterystycznych dla botnetów |
|  | Urządzenie powinno umożliwiać wykrycie malware typu „Cryptor” i „Ransomware” wraz z wariantami „Cryptolocker, CryptoWall…” itd. poprzez statyczną i dynamiczną analizę próbki |
|  | Urządzenie powinno umożliwiać wykrywania ataków typu „Waterhole” |
|  | Funkcjonalność powinna być zarządzana z centralnej konsoli |
|  | Funkcjonalność powinna posiadać możliwość:  a) inspekcji ruchu SSL  b) inspekcji plików skompresowanych  c) skanowania plików transmitowanych protokołem CIFS |
|  | Inspekcja SSL (ruch przychodzący / wychodzący) | Wsparcie dla Perfect Forward Secrecy (PFS, ECDHE) |
|  | Wsparcie dla AES-NI i AES-GCM |
|  | Integracja z sandboxem |
|  | Funkcjonalność powinna pozwalać na wykorzystanie przez administratora filtrowania URL |
|  | Brama IPSec VPN | Urządzenie powinno wspierać CA wewnętrzne oraz zewnętrzne |
|  | Wsparcie dla 3DES oraz AES-256 dla fazy IKE I i II oraz IKEv2 oraz „Suite-B-GCM-128” i „Suite-B-GCM-256” dla fazy II |
|  | Rozwiązanie powinno wspierać site-to-site VPN w następujących topologiach:  - każdy do każdego (full mesh)  - gwiazda  - połącznie poprzez huby |
|  | Urządzenie powinno wspierać użytkownika korzystającego z trybu klienta VPN (IPSec oraz SSL) oraz clientless SSL VPN, w zakresie obsługi haseł w systemie, bezpośrednio lub pośrednio, co najmniej dla obsługi sytuacji wygaśnięcia terminu ważności hasła w systemie, umożliwiając zmianę przeterminowanego hasła |
|  | Urządzenie powinno pozwalać na pracę z przepustowością 270 Mbps dla VPN AES-12 |
|  | Wsparcie dla urządzeń mobilnych | Zamawiający oczekuje zintegrowanej obsługi urządzeń mobilnych |
|  | Rozwiązanie powinno wspierać zarządzane i niezarządzane urządzenia dostępowe (polityka BYOD) |
|  | Zarządzanie i konfiguracja | Urządzenie posiada możliwość eksportu informacji przezsyslog |
|  |  | Urządzenie wspiera eksport zdarzeń opartych o przepływy za pomocą protokołu NetFlow lub analogiczny |
|  |  | Urządzenie posiada możliwość komunikacji z serwerami uwierzytelnienia i autoryzacji za pośrednictwem protokołów RADIUS i TACACS+ oraz obsługuje mechanizmy AAA (autentykacja, autoryzacja, accounting) |
|  |  | Urządzenie jest konfigurowalne przez CLI oraz interfejs graficzny |
|  |  | Dostęp do urządzenia jest możliwy przez SSH |
|  |  | Urządzenie obsługuje protokół SNMP 1/2/3 |
|  |  | Możliwa jest edycja pliku konfiguracyjnego urządzenia w trybie off-line. Tzn. istnieje możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej jest możliwe uruchomienie urządzenia z nową konfiguracją |
|  |  | Urządzenie umożliwia zrzucenie obecnego stanu programu (coredump) dla potrzeb diagnostycznych, |
|  |  | Urządzenie posiada wsparcie dla mechanizmu TCP Ping, który pozwala na wysyłanie wiadomości TCP dla rozwiązywania problemów związanych z łączności w sieciach IP |
|  | Licencje i gwarancja | na okres 36 miesięcy |

1. **Zakup sprzętu do backupu danych z dyskami (1 szt.)**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Parametr** | **Wymagania minimalne** |
|  | Procesor CPU | Czterordzeniowy procesor o taktowaniu 3,6 GHz |
|  | Pamięć (RAM) | 4 GB UDIMM DDR4 (1 x 4 GB) |
|  | Flash | 4GB eMMC |
|  | Liczba gniazd pamięci RAM | 64 GB (4 x 16 GB) DDR4 long DIMM |
|  | Maks. liczba dysków HDD i SSD | 8 dysków 3,5-calowe |
|  | Kieszeń na dysk twardy wymieniany podczas pracy | TAK |
|  | Kompatybilność dysków | 3,5-calowe wnęki:  3,5-calowe dyski twarde SATA  2,5-calowe dyski twarde SATA  2,5-calowe dyski SSD SATA |
|  | Obsługa przyśpieszenia pamięci podręcznej SSD | TAK |
|  | Porty gigabitowej sieci LAN | 4 |
|  | Ramka Jumbo (GbE) | TAK |
|  | 10 GbE | 2 porty 10GbE SFP+ SmartNIC |
|  | Gniazdo rozszerzeń (PCle) | Gniazdo 1: PCIe Gen2 x4 (PCH)  Gniazdo 2: PCIe Gen3 x8 (procesor)  Gniazdo 3: PCIe Gen3 x4 (procesor)  Gniazdo 4: PCIe Gen3 x4 (procesor) |
|  | USB 3.1 10Gbps | 2 gniazda typu C USB 3.1 Gen2 5V/3A 10 Gb/s  4 gniazda typu A USB 3.1 Gen2 5V/1A 10 Gb/s |
|
|
|  | HDMI | 1, HDMI 2.0 (rozdzielczość do 3840 x 2160 przy częstotliwości 60 Hz) |
|  | Wskaźniki LED | HDD 1–8, stan, LAN, stan gniazda rozszerzenia pamięci masowej |
|  | Przyciski | Zasilanie, Reset |
|  | Format2 | 2U, do montażu stelażowego |
|  | Temperatura | 0 - 40 °C |
|  | Specyfikacja zasilania | 300 W(x2), 100–240 V |
|  | Pobór mocy: Tryb pracy, typowe (W) | 90,2W |
|  | Natężenie dźwięku dB(A) | 52,1 db(A) |
|  | Ostrzeżenie systemowe | Brzęczyk |
|  | Złącze bezpieczeństwa Kensington | TAK |
|  | System plików: wewnętrzny dysk twardy | EXT4 |
|  | System plików: zewnętrzny dysk twardy | EXT3, EXT4, NTFS, FAT32, HFS+ |
|  | Port Trunking / agregacja łączy | TAK |
|  | Wykrywanie usługi sieciowej (UPnP i Bonjour) | TAK |
|  | Wirtualne sieci LAN (VLAN) | TAK |
|  | Wiązanie usług na podstawie interfejsów sieciowych | TAK |
|  | 256-bitowe szyfrowanie AES na podstawie wolumenów | TAK |
|  | 256-bitowe szyfrowanie AES folderów | TAK |
|  | Szyfrowanie dysków zewnętrznych | TAK |
|  | Migawka | TAK |
|  | Przywracanie RAID | TAK |
|  | Powiększanie pojemności RAID online | TAK |
|  | Migracja poziomów RAID online | TAK |
|  | RAID 50/60 | TAK |
|  | RAID10+ hot spare | TAK |
|  | RAID10 | TAK |
|  | RAID6+ hot spare | TAK |
|  | RAID 6 | TAK |
|  | RAID 5+ dysk zapasowy | TAK |
|  | RAID 5 | TAK |
|  | RAID 1 | TAK |
|  | RAID 0 | TAK |
|  | JBOD | TAK |
|  | Pojedynczy dysk | TAK |
|  | Globalny dysk Hot Spare | TAK |
|  | Pula pamięci masowej | TAK |
|  | Buforowanie SSD | TAK |
|  | Obiekt docelowy iSCSI | TAK |
|  | Migawka/kopia zapasowa jednostek iSCSI LUN | TAK |
|  | Kontroler domeny i serwer NTP | TAK |
|  | Wolumin z elastycznym alokowaniem | TAK |
|  | Container Station | TAK |
|  | Virtualization Station | TAK |
|  | Linus Station (pamięć RAM serwera NAS>=4GB) | TAK |
|  | Obsługa VMware® | TAK |
|  | Citrix Ready | TAK |
|  | Zgodność z Microsoft Hyper-V | TAK |
|  | Jednostki iSCSI LUN oparte na blokach | TAK |
|  | Odzyskiwanie miejsca | TAK |
|  | Funkcja Storage Plug & Connect (iSCSI i CIFS) | TAK |
|  | Kontroler domeny | TAK |
|  | Obsługa ACL na poziomie folderów współdzielonych | TAK |
|  | Lista ACS systemu operacyjnego | TAK |
|  | Zaawansowane uprawnienia do folderów z obsługą ACL na poziomie podfolderów w protokołach i usługach CIFS/SMB, AFP, FTP oraz Menadżerze plików w przeglądarce | TAK |
|  | Uwierzytelnianie Microsoft Active Directory (AD) | TAK |
|  | Serwer i klient LDAP | TAK |
|  | Replikacja zdalna w czasie rzeczywistym (Real-time Remote Replication, RTRR) | TAK |
|  | Maks. liczba zadań RTRR | 400 |
|  | Replikacja zdalna (rsync) | TAK |
|  | Obsługa etykiet woluminu na dyskach zewnętrznych | NTFS |
|  | Obsługa programu Apple Time Machine | TAK |
|  | Powiadomienia (e-mail, SMS) | TAK |
|  | Kosz sieciowy do usuwania plików przez CIFS/SMB i AFP z czasem zachowywania i filtrem typów plików | TAK |
|  | Wake on LAN (WOL) | TAK |
|  | Zaplanowane włączanie i wyłączanie (15 ustawień) | TAK |
|  | Qtier | TAK |
|  | Przełącznik wirtualny | TAK |
|  | Maks. Wersja SMB | 3 |
|  | SNMP (Wersja 2 i 3) | TAK |
|  | Drukarki USB (maks. 3) | TAK |
|  | Logowanie przez Telnet i SSH (tylko dla administratora) | TAK |
|  | Qsirch (pamięć RAM serwera NAS >= 2 GB) | TAK |
|  | Serwer i klient Syslog | TAK |
|  | Serwer VPN (PPTP + OpenVPN + L2TP) | TAK (maksymalna liczba klientów: 15 + 15 + 15) |
|  | Pamięć w chmurze usługodawców | Amazon S3/Glacier, ElephantDrive, Google Drive, Microsoft Azure lub innch i równoważnych |
|  | Serwer iTunes | TAK |
|  | Serwer multimediów DLNA, AirPlay, Chromecast | TAK |
|  | Download Station (pobieranie przez BT, Magnet Link, HTTP, FTP) | TAK |
|  | QVR Pro | TAK |
|  | Maks. liczba kamer (QVR Pro) | Domyślnie: 8, maks.: 128 (możliwość zakupu licencji) |
|  | Surveillance Station | TAK |
|  | Maks. liczba kamer (monitoring) | Domyślnie: 8, maks.: 80 (możliwość zakupu licencji) |
|  | Maks. liczba użytkowników | 4096 |
|  | Maks. liczba grup użytkowników | 512 |
|  | Maks. liczba folderów współdzielonych | 512 |
|  | Maks. liczba jednoczesnych połączeń (CIFS) | 700 |
| Dyski 4 sztuki | | |
|  | Pojemność | 4TB |
|  | Interfejs | SATA 6 Gb/s |
|  | Format obudowy | 3.5" |
|  | Klasa obr./min | 5400 |
|  | Pamięć podręczna | 64MB |

1. **Zakup oprogramowania do backupu danych (1 szt.)**

|  |  |
| --- | --- |
| Lp. | Wymagania minimalne |
|  | Możliwość backupu do 50 komputerów , 3 serwerów, 1 hosta ESX(i)/Hyper-V |
|  | Wsparcie techniczne producenta – 24 miesiące |
|  | Oprogramowanie działające w architekturze klient-serwer w oparciu o protokół TCP/IP, z centralnym modułem sterowania wykonywaniem kopii zapasowych z dysków komputerów klienckich |
|  | Program serwerowy kompatybilny z systemami: Microsoft Windows 2000, XP, Vista, Windows 7, Windows 8, Windows 10; Microsoft Windows Server 2000, 2003, 2008, 2012, 2016, Linux, BSD, Mac OS X, QNAP, Synology lub równoważnymi systemami |
|  | Program kliencki kompatybilny z systemami: Microsoft Windows 2000, XP, Vista, Windows 7, Windows 8, Windows 10; Microsoft Windows Server 2000, 2003, 2008, 2012, 2016, Linux, BSD, Mac OS X, QNAP, Synology lub równoważnymi systemami |
|  | Możliwość archiwizacji pełnej, przyrostowej/różnicowej i delta (różnica na poziomie fragmentów plików) |
|  | Możliwość archiwizacji otwartych i zablokowanych plików bez korzystania z usługi Volume Shadow Copy Service (VSS) |
|  | Automatyczny backup przy wyłączaniu komputera |
|  | Możliwość wybrania do archiwizacji lub wykluczenia z archiwizacji określonych woluminów, katalogów, plików za pomocą symboli wieloznacznych np.: \* i ? |
|  | Backup całego systemu operacyjnego i zainstalowanych programów |
|  | Backup baz danych i plików poczty w trybie online i offline |
|  | Kopie rotacyjne (wersjonowanie) |
|  | Zapis archiwów w otwartym formacie (ZIP 64-bit) |
|  | Odzyskiwanie systemu operacyjnego na czystym dysku twardym bez konieczności ponownej instalacji (bare metal restore) |
|  | Bezpośrednie odzyskiwanie plików do lokalizacji oryginalnej |
|  | Odzyskiwanie z kopii różnicowych i delta tak jak z kopii pełnych |
|  | Szyfrowanie archiwów i transferu zapewniających bezpieczeństwo sieci i informacji wymaganych przez RODO |
|  | Kompresja po stronie stacji roboczej |
|  | Replikacja archiwów na dodatkowy dysk twardy, NAS, serwer FTP, |
|  | Replikcacja na napęd optyczny: CD, DVD, Blu-Ray, HD-DVD i napęd taśmowy: DDS, DLT, LTO, AIT |
|  | Centralne sterowanie całym Systemem z jednego miejsca |
|  | Transparentna archiwizacja wykonywana w tle, która nie jest odczuwalna przez pracowników |
|  | Możliwość równoległej archiwizacji wszystkich komputerów podłączonych do sieci LAN/WAN |
|  | Wysyłanie Alertów administracyjnych na e-mail |
|  | Możliwość uruchamiania zewnętrznych programów, skryptów i plików wsadowych na serwerze backupu i na komputerach zdalnych |
|  | Raporty podsumowujące przebieg archiwizacji, zawierające informacje na temat zaległych zadań archiwizacji oraz statystyki |
|  | Automatyczna aktualizacja oprogramowania na komputerach zdalnych |
|  | Bezterminowa licencja - licencja nie może być ograniczona czasowo |
|  | Interfejs, instrukcja i pomoc techniczna w języku polskim |
|  | Możliwość instalacji klienta przez GPO |

1. **Streamer do kopii**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Parametr** | **Wymagania minimalne** |
|  | Certyfikaty | UL 60950, CSA C22.2 No. 60950, IEC 60950/ EN60950\nFCC 47CFR, part 15, class B, CISPR22, class B, EN55022, class B, EN61000-3-2, EN61000-3-3, CISPR24, EN55024, ICES-003, class B, VCCI, CE, C-Tick  lub równoważne |
|  | Zakres temperatur (eksploatacja) | 10 - 40  °C |
|  | Zakres temperatur (przechowywanie) | -40 - 65  °C |
|  | Zakres wilgotności względnej | 20 - 80  % |
|  | Dopuszczalna wilgotność względna | 8 - 90  % |
|  | Dopuszczalna wysokość podczas eksploatacji (n.p.m.) | -15 - 3048  m |
|  | Waga produktu | 615  g |
|  | Typ napędu | HDD |
|  | Pojemność | 4TB |

1. **Zakup stacji roboczych do obsługi wdrażanych rozwiązań (9 szt.)**

|  |  |  |
| --- | --- | --- |
| Lp. | Parametr | Wymagania minimalne |
|  | Taktowanie procesora | 3.6 GHz |
|  | Zainstalowana pamięć RAM | 4 GB |
|  | Maks. wielkość pamięci | 32 GB |
|  | Liczba obsadzonych gniazd pamięci | 1 |
|  | Liczba wolnych gniazd pamięci | 1 |
|  | Rodzaj pamięci | DDR4 |
|  | Częstotliwość szyny pamięci | 2400 MHz |
|  | Typ dysku | SSD |
|  | Pojemność SSD | 128 GB |
|  | Porty wideo | 1 x VGA (15 pin D-Sub)  1 x HDMI |
|  | Interfejs sieciowy | 1 x 10/100/1000 Mbit/s  WiFi 802.11b/g/n  Bluetooth |
|  | Napęd optyczny | DVD-RW |
|  | Czytnik kart pamięci | Tak |
|  | Porty USB | 4 x USB 2.0 Type-A  2 x USB 3.0 Type-A |
|  | Pozostałe porty we/wy | 2 x Audio (Line-in)  1 x Audio (Line-out)  1 x Audio (Combo)  1 x RJ-45 |
|  | Obudowa | Small Form Factor |
|  | Wysokość | Max 295 mm |
|  | Szerokość | Max 96 mm |
|  | Głębokość | Max 300 mm |
|  | System operacyjny | System operacyjny 64-bit |
|  | Akcesoria w zestawie | 1. Dokumentacja  2. Klawiatura  3. Mysz optyczna  4. Europejski przewód zasilający |
|  | Informacje o gwarancji | 3 lata NBD |
| Monitor | | |
|  | Proporcje obrazu | 16:09 |
|  | Przekątna ekranu | 21.5" |
|  | Typ matrycy | TFT IPS |
|  | Powierzchnia matrycy | Matowa |
|  | Technologia podświetlania | Diody LED |
|  | Plamka matrycy | 0.24795 mm |
|  | Rozdzielczość | 1920 x 1080 (FHD 1080) |
|  | Czas reakcji | 5 ms |
|  | Jasność | 250 cd/m² |
|  | Kontrast statyczny | 1 000:1 |
|  | Gniazda we/wy | 1 x 15-pin D-Sub  1 x HDMI |
|  | Certyfikaty | RoHS  TCO |
|  | Kolor | Czarny |

1. **Zakup oprogramowania biurowego do komputerów (11 szt.)**

Oprogramowanie biurowe (najnowsza aktualna wersja oferowana przez producenta na dzień składania ofert) instalowana na stacjach roboczych w niewyłącznej i nieograniczonej czasowo licencji. Pakiet biurowy powinien zawierać co najmniej: edytor tekstu, arkusz kalkulacyjny, program do tworzenia prezentacji multimedialnych, program do obsługi poczty elektronicznej i kalendarza oraz powinien spełniać następujące kryteria minimalne:

Wymagania odnośnie interfejsu użytkownika:

* pełna polska wersja językowa interfejsu użytkownika z możliwością przełączania wersji językowej interfejsu na język angielski;
* możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory);
* użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się;
  1. wykorzystanie tej samej licencji na komputerze stacjonarnym oraz na komputerze przenośnym Zamawiającego;
  2. możliwość automatycznej instalacji komponentów (przy użyciu instalatora systemowego);
  3. możliwość zdalnej instalacji pakietu poprzez zasady grup (GPO);
  4. całkowicie zlokalizowany w języku polskim system komunikatów i podręcznej pomocy technicznej w pakiecie;
  5. prawo do (w okresie przynajmniej 5 lat) instalacji udostępnianych przez producenta poprawek w ramach wynagrodzenia;
  6. wsparcie dla formatu XML;
  7. możliwość nadawania uprawnień do modyfikacji dokumentów tworzonych za pomocą aplikacji wchodzących w skład pakietów;
  8. automatyczne wypisywanie hiperłącz;
  9. możliwość automatycznego odświeżania danych pochodzących z Internetu w arkuszach kalkulacyjnych;
  10. możliwość dodawania do dokumentów i arkuszy kalkulacyjnych podpisów cyfrowych, pozwalających na stwierdzenie czy dany dokument/arkusz pochodzi z bezpiecznego źródła i nie został w żaden sposób zmieniony;
  11. możliwość automatycznego odzyskiwania dokumentów i arkuszy kalkulacyjnych: w wypadku nieoczekiwanego zamknięcia aplikacji spowodowanego zanikiem prądu;
  12. prawidłowe odczytywanie i zapisywanie danych w dokumentach w formatach: .DOC, .DOCX, XLS, .XLSX, .PPT, .PPTX, w tym obsługa formatowania, makr, formuł, formularzy w plikach wytworzonych;
  13. tworzenie i edycja dokumentów elektronicznych w formacie, który spełnia następujące warunki:
* posiada kompletny i publicznie dostępny opis formatu;
* ma zdefiniowany układ informacji w postaci XML zgodnie z Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych *(Dz. U. 2012 nr 0 poz. 526);*
* umożliwia wykorzystanie schematów XML;
* wspiera w swojej specyfikacji podpis elektroniczny zgodnie z Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych *(Dz. U. 2012 poz. 526) wraz z późniejszymi zmianami;*
  1. zawiera narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy);
  2. umożliwia tworzenie drukowanych materiałów informacyjnych poprzez:
* tworzenie i edycję drukowanych materiałów informacyjnych;
* tworzenie materiałów przy użyciu dostępnych z narzędziem szablonów: broszur, biuletynów, katalogów;
* edycję poszczególnych stron materiałów;
* podział treści na kolumny;
* umieszczanie elementów graficznych;
* wykorzystanie mechanizmu korespondencji seryjnej;
* płynne przesuwanie elementów po całej stronie publikacji;
* eksport publikacji do formatu PDF oraz TIFF;
* wydruk publikacji;
* możliwość przygotowywania materiałów do wydruku w standardzie CMYK.
  1. edytor tekstów musi umożliwiać:
* edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty;
* wstawianie oraz formatowanie tabel;
* wstawianie oraz formatowanie obiektów graficznych;
* wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne);
* automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków;
* automatyczne tworzenie spisów treści;
* formatowanie nagłówków i stopek stron;
* śledzenie zmian wprowadzonych przez użytkowników;
* nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności;
* określenie układu strony (pionowa/pozioma);
* wydruk dokumentów;
* wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących   
  z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną;
* pracę na dokumentach z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu;
* zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji;
* wymagana jest dostępność do oferowanego edytora tekstu narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze i pozwalające zapisać plik wynikowy w zgodzie z Rozporządzeniem o Aktach Normatywnych i Prawnych;
* wymagana jest zgodność z szablonami udostępnianymi przez Rządowe Centrum Legislacji, zawierającymi zestaw stylów wykorzystywanych do formatowania projektów aktów prawnych oraz makroinstrukcji służących w szczególności automatyzacji stosowania stylów, jak również weryfikacji niektórych nieprawidłowości przy redagowaniu aktu prawnego.
  1. arkusz kalkulacyjny musi umożliwiać:
  + tworzenie raportów tabelarycznych;
* tworzenie wykresów liniowych (wraz z linią trendu), słupkowych, kołowych;
* tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu;
* tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice);
* obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych;
* tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych;
* wyszukiwanie i zamianę danych;
* wykonywanie analiz danych przy użyciu formatowania warunkowego;
* nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie: nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności;
* formatowanie czasu, daty i wartości finansowych z polskim formatem;
* zapis wielu arkuszy kalkulacyjnych w jednym pliku;
* zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń;
* zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
  1. Narzędzie do przygotowywania i prowadzenia prezentacji multimedialnych umożliwiających:
* drukowanie w formacie umożliwiającym robienie notatek;
* zapisanie jako prezentacja tylko do odczytu;
* nagrywanie narracji i dołączanie jej do prezentacji;
* opatrywanie slajdów notatkami dla prezentera;
* umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych   
  i wideo;
* umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego;
* odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym;
* możliwość tworzenia animacji obiektów i całych slajdów;
* prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera;
  1. Oprogramowanie równoważne musi w pełni współpracować z Lokalnym Systemem Informatycznym, systemem Quorum i Elektronicznym Systemem obiegu Dokumentów eksploatowanymi u Zamawiającego.
  2. Oprogramowanie równoważne nie pogorszy funkcjonalności i współpracy z innymi systemami eksploatowanymi u Zamawiającego, a jego zastosowanie nie będzie wymagało żadnych nakładów związanych z dostosowaniem aktualnie działającej infrastruktury IT Zamawiającego.
  3. W przypadku, gdy zaoferowane przez Wykonawcę oprogramowanie równoważne nie będzie właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego lub spowoduje zakłócenia w funkcjonowaniu pracy środowiska sprzętowo-programowego u Zamawiającego, Wykonawca pokryje wszystkie koszty związane z przywróceniem i sprawnym działaniem infrastruktury sprzętowo-programowej Zamawiającego oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie środowiska sprzętowo-programowego Zamawiającego również po odinstalowaniu oprogramowania.