OPIS PRZEDMIOTU ZAMÓWIENIA

Do postępowania pn.:

Dostawa sprzętu wraz z oprogramowaniem w celu podniesienia poziomu cyberbezpieczeństwa USK w Olsztynie

Dostarczenie systemu antywirusowego

1. Rozwiązanie typu zarządzalny antywirus wspierające następujące systemy:
   1.1. Microsoft Windows 7 z dodatkiem SP1
   1.2. Microsoft Windows 8.1
   1.3. Microsoft Windows 10
   1.4. Microsoft Windows 11
   1.5. Microsoft Windows Server 2008 R2
   1.6. Microsoft Windows Server 2012
   1.7. Microsoft Windows Server 2016
   1.8. Microsoft Windows Server 2019
   1.9. Microsoft Windows Server 2022
2. Oprogramowanie antywirusowe składa się z konsoli oraz aplikacji do ochrony stacji roboczych oraz serwerów.
3. Ochrona antywirusowa realizowana na wielu poziomach, tj.: monitora kontrolującego system w tle, modułu skanowania heurystycznego, modułu skanującego nośniki wymienne, monitora ruchu http oraz modułu wykrywającego rootkity.
4. Rozwiązanie posiada wbudowany mechanizm ochrony przed zagrożeniami typu ransomware.
5. Rozwiązanie wspiera technologię Antimalware Scan Interface (AMSI)
6. Rozwiązanie umożliwia wybór plików do skanowania – wszystkich plików lub tylko plików o określonych rozszerzeniach.
7. W momencie wykrycia infekcji rozwiązanie automatycznie stara się wyleczyć plik, a jeśli nie jest to możliwe - przenosi go do bezpiecznego folderu kwarantanny.
8. Rozwiązanie posiada możliwość ręcznej reakcji na wykryte zagrożenie, w takim przypadku pozwala na: wyleczenie pliku, usunięcie, przeniesienie do kwarantanny, zmiany nazwy, zablokowania.
9. Rozwiązanie chroni plik systemowy HOSTS przed nieautoryzowanymi zmianami.
10. Rozwiązanie posiada mechanizmy skanujące dyski sieciowe.
11. Skanowanie dysków sieciowych jest możliwe dla dowolnych operacji na takich zasobach lub tylko przy wykonywaniu znajdujących się tam plików.
12. Rozwiązanie posiada możliwość tworzenia wykluczeń dla mechanizmów ochrony w czasie rzeczywistym, w tym co najmniej dla: plików, folderów, procesów.
13. Rozwiązanie posiada mechanizm ochrony ruchu http chroniący użytkownika przed malware oraz phishingiem.
14. Istnieje możliwość stworzenia wykluczenia dla wskazanej aplikacji, tak aby nie skanowała ona ruchu http.
15. Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa jest zarówno aktualizacja automatyczna programu oraz na żądanie przez wywołanie funkcji w interfejsie lokalnym oprogramowania.
16. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.
17. Rozwiązanie posiada możliwość dystrybuowania aktualizacji baz definicji wirusów oraz aktualizacji oprogramowania zainstalowanego na stacji końcowej, za pomocą serwera pośredniczącego.
18. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej do nowej wersji, następuje w sposób automatyczny, niewidoczny dla użytkownika końcowego.

19. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej nie wymaga dodatkowych czynności konfiguracyjnych ze strony administratora systemu i następuje automatycznie w momencie udostępnienia takiej aktualizacji przez producenta.
20. Rozwiązanie posiada możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli zarządzania.
21. Rozwiązanie posiada możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej w określone dni i godziny tygodnia i miesiąca.
22. Rozwiązanie posiada możliwość wywołania skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli lub lokalnie przez określonego klienta.
23. Rozwiązanie posiada możliwość wywołania skanowania w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.
24. Rozwiązanie posiada możliwość wywołania procesu skanowania z niskim priorytetem, co pozwala na skanowanie z użyciem mniejszej ilości zasobów systemowych.
25. Rozwiązanie posiada możliwość wywołania skanowania uwzględnionych rozszerzeń a także ich wykluczanie.
26. Rozwiązanie posiada możliwość skanowania urządzeń przenośnych takich jak pendrive, dyski zewnętrzne itp.
27. Skanowanie dysków przenośnych może odbywać się w sposób automatyczny bez wiedzy użytkownika, automatycznie z wyświetleniem podsumowania skanowania użytkownikowi
28. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie.
29. Rozwiązanie posiada funkcję skanowania na żądanie pojedynczych plików, katalogów, napędów przy pomocy skrótu w menu kontekstowym
30. Mikrodefinicje wirusów – przyrostowe (inkrementalne) pobieranie są jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji).
31. Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.
32. Rozwiązanie posiada heurystyczną technologię do wykrywania nowych, nieznanych wirusów.
33. Umożliwia wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu spyware, adware, keylogger, dialer, trojan, rootkit.
34. Posiada mechanizm wykrywania nowych i nieznanych zagrożeń (0-day), bazujący na technologii chmurowej, analizującej podejrzane pliki wykonywalne (przez pliki wykonywalne rozumie się co najmniej: aplikacje, interpretowalną zawartość Flash, Sliverlight, skrypty oraz makra dokumentów pakietu Office).
35. Rozwiązanie posiada technologię wykrywania nowych i nieznanych zagrożeń typu 0-day, technologia ta powinna w głównej mierze bazować na metadanych na temat analizowanego pliku. Pliki sklasyfikowane jako bezpieczne, nie są wysyłane do analizy w infrastrukturze producenta.

36. Rozwiązanie posiada technologię wykrywania nowych i nieznanych zagrożeń, która w przypadku podejrzanych plików umożliwia automatyczne ładowanie ich do systemu sandbox, utrzymywanego w infrastrukturze dostawcy oprogramowania antywirusowego w celu przeprowadzenia dodatkowej strukturalnej i behawioralnej analizy podejrzanego pliku.
37. Rozwiązanie posiada możliwość wyłączenia mechanizmu automatycznego przesyłania podejrzanych plików do dodatkowej analizy przez producenta.
38. Rozwiązanie posiada możliwość umieszczenia oprogramowania typu spyware, adware, keylogger", dialer, trojan w kwarantannie.
39. Rozwiązanie posiada możliwość obsługi plików skompresowanych obejmującego najpopularniejsze formaty w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2 HQX.
40. Rozwiązanie posiada możliwość logowania historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów jest możliwy z poziomu GUI aplikacji jak i konsoli centralnego zarządzania.
41. Rozwiązanie automatycznie powiadamia użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem czy stacja robocza jest odpowiednio zabezpieczona.
42. Rozwiązanie posiada możliwość wyłączenia powiadomień dla użytkowników stacji końcowej o wykrytych zagrożeniach.
43. Rozwiązanie posiada możliwość wyłączenia interfejsu użytkownika oprogramowania zainstalowanego na stacji końcowej.
44. Rozwiązanie umożliwia blokowanie przez program na komputerze klienckim określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http.
45. Skanowanie http oraz blokowanie zawartości może być deaktywowane dla witryn określonych, jako zaufane przez system reputacyjny producenta.
46. Rozwiązanie posiada możliwość instalacji dodatku do przeglądarki internetowej (Google Chrome, Mozilla Firefox, MS Edge) pozwalającego na wyświetleniu graficznej informacji o reputacji witryny, która pojawia się w wynikach wyszukiwania w wyszukiwarkach internetowych.
47. Rozwiązanie jest wyposażone w mechanizm ochrony przeglądarki internetowej, w tym analizujący uruchamiane skrypty ActiveX i pobierane pliki.
48. Rozwiązanie posiada możliwość ochrony podczas przeglądania sieci Internet na podstawie badania reputacji witryn.
49. Rozwiązanie umożliwia blokowanie dostępu do kategorii witryn WWW skatalogowanych przez systemy producenta.
50. Oprogramowanie zapewnia co najmniej 30 kategorii klasyfikacji witryn WWW.
51. Użytkownik podczas próby przejścia na witrynę znajdująca się w zablokowanej przez Administratora kategorii, jest powiadomiony o nałożonej na niego blokadzie komunikatem w przeglądarce internetowej.
52. Rozwiązanie umożliwia blokowanie witryn na podstawie kategorii zarówno dla protokołu HTTP jak i HTTPS.
53. Rozwiązanie posiada wbudowany mechanizm zabezpieczenia połączenia do witryn skategoryzowanych przez producenta jako „bankowość elektroniczna" poprzez uniemożliwienie nawiązania nowych sesji do niezaufanych hostów na czas połączenia z bankiem.

54. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” rozwiązanie blokuje możliwość uruchamiania od strony chronionego hosta poleceń cmd oraz skryptów.
55. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” rozwiązanie automatycznie blokuje zdalny dostęp do hosta za pomocą takich narzędzi jak pulpit zdalny, TeamViewer, LogMein, VNC itp.
56. Kontrola połączenia umożliwia zabezpieczenie sesji do dowolnej witryny HTTPS wskazanej przez administratora – administrator ma możliwość tworzenia własnej listy takich witryn.
57. Rozwiązanie posiada wbudowaną funkcję, która po zakończeniu sesji z witrynami sklasyfikowanymi jako „bankowość elektroniczna” czyści zawartość schowka systemowego.
58. Rozwiązanie posiada funkcję zarządzania zaporą ogniową (tzw. personal firewall) wbudowaną w system Windows, z opcją definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup.
59. Profile bezpieczeństwa zapory ogniowej zawierają predefiniowane reguły zezwalające na bezproblemową komunikację w sieci lokalnej.
60. Rozwiązanie pozwala na tworzenie własnych reguł w oparciu co najmniej o: kierunek komunikacji sieciowej, protokół sieciowy, oraz możliwość wyboru akcji zezwolenia lub zablokowania wskazanej komunikacji.
61. Rozwiązanie posiada możliwość automatycznego przełączenia profilu bezpieczeństwa zapory ogniowej po spełnieniu określonych warunków (np. zmiana adresacji karty sieciowej na stacji roboczej).
62. Rozwiązanie umożliwia stworzenie zestawów reguł do natychmiastowego zastosowania, które zablokują komunikację sieciową w celu izolacji hosta na żądanie administratora.
63. Rozwiązanie jest wyposażone w mechanizm aktualizacji aplikacji (patch managment), umożliwiający instalację dostępnych poprawek dla systemu operacyjnego oraz aplikacji na nim zainstalowanych.
64. Mechanizm aktualizacji aplikacji (patch managment) nie wymaga instalowania dodatkowych agentów oprócz agenta AV.
65. Moduł aktualizacji aplikacji, okresowo skanuje aplikacje zainstalowane na stacji roboczej i umożliwia ich aktualizację do najnowszych wersji.
66. Moduł aktualizacji aplikacji pełni role mechanizmu łatającego podatności i instalującego aktualizacje oprogramowania, a nie jedynie pasywnego skanera luk w bezpieczeństwie aplikacji.
67. Administrator posiada możliwość określenia, kiedy i jakie aktualizacje mają zostać zainstalowane automatycznie.
68. Administrator posiada możliwość uruchomienia aktualizacji dla systemu operacyjnego jak i aplikacji znajdujących się na nim na żądanie dla wybranych lub wszystkich hostów.
69. Mechanizm aktualizacji aplikacji umożliwia automatyczne wyświetlenie komunikatu użytkownikowi od strony hosta o konieczności zamknięcia danej aplikacji, tak aby proces aktualizacji mógł się zakończyć.
70. W przypadku gdy instalacja aktualizacji dla systemu operacyjnego lub innej aplikacji wymaga restartu hosta w celu jej zastosowania, administrator posiada możliwość wymuszenia automatycznego restartu, wymuszenia restartu po określonej liczbie godzin, lub wyświetlenia komunikatu użytkownikowi o konieczności restartu.

71. Administrator konsoli zarządzającej ma możliwości zapoznania się z opisem danej podatności aplikacji uruchamiając aktywny link z konsoli zarządzającej z przekierowaniem na strony producenta aplikacji.
72. Mechanizm aktualizacji aplikacji (patch managment) nie wymaga uprawnień administratora lokalnego do instalacji poprawek i jest realizowany, jako dedykowany proces.
73. Administrator ma możliwość zdefiniowania aplikacji, które nie podlegają aktualizacji, poprzez wpisanie nazwy aplikacji na listę wykluczeń w konsoli zarządzającej.
74. Rozwiązanie umożliwia wyświetlenie w GUI od strony chronionego hosta informacji o brakujących poprawkach dla systemu lub aplikacji i umożliwienie, ich instalacji przez użytkownika końcowego.
75. System centralnego zarządzania prezentuje niezaktualizowane aplikacje występujące na wszystkich chronionych hostach lub listę nieaktualizowanego oprogramowania dla pojedynczej stacji końcowej.
76. Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.
77. Mechanizm kontroli urządzeń zewnętrznych wspiera m.in. urządzenia takie jak: pamięci masowe, napędy CD/DVD, modemy, porty COM i LTP, drukarki, czytniki kart pamięci, kamery, urządzenia bluetooth.
78. Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączania do stacji końcowej.
79. Lista urządzeń zaufanych jest tworzona co najmniej w oparciu o nazwę urządzenia i identyfikator sprzętowy.
80. Rozwiązanie posiada możliwość blokady zapisywania plików na zewnętrznych dyskach USB urządzenia takie są wówczas dostępne w trybie tylko do odczytu.
81. Mechanizm kontroli urządzeń umożliwia blokadę uruchamiania plików wykonywalnych z nośników pamięci. Blokada ta pozwala na korzystanie z pozostałych danych zapisanych na takich nośnikach.
82. Rozwiązanie posiada możliwość zabezpieczenia zmian w konfiguracji przez użytkownika końcowego przy wykorzystaniu hasła.
83. Zmiany w konfiguracji mogą być dokonywane przez użytkownika końcowego tylko dla poszczególnych funkcji aplikacji wskazanych przez administratora w profilu.
84. Rozwiązanie posiada możliwość przekazywania do konsoli administracji zdalnej kluczy odzyskiwania funkcji Bitlocker
85. Rozwiązanie jest wyposażone w dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware niezależnie od pozostałych modułów ochrony. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.
86. Moduł posiada możliwość pracy w trybie monitorowania (bez blokowania) przekazując administratorowi informacje dotyczące prób modyfikacji plików w chronionych folderach.
87. Administrator posiada możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.
88. Istnieje możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną antyransomware.

89. Rozwiązanie potrafi automatycznie wykryć zaufane aplikacje, dla których będzie zezwolony dostęp do plików w chronionych folderach, oraz daje możliwość wskazania zaufanych aplikacji przez administratora.
90. Rozwiązanie posiada funkcjonalność kontroli uruchamianych aplikacji.
91. Tryb kontroli aplikacji umożliwia uruchomienie wszystkich aplikacji, uruchomienie i monitorowanie wszystkich aplikacji, blokowanie niezaufanych aplikacji.
92. Istnieje możliwości blokowania, zezwolenia lub monitorowania aplikacji w oparciu, co najmniej o docelowy identyfikator SHA1,SHA256, lokalizację pliku, wersję pliku, nazwę aplikacji, wielkość pliku, wydawcę, ważność podpisu cyfrowego aplikacji.
93. Tworzone reguły dotyczyć mogą czynności: uruchomienia aplikacji, ładowania modułu, uruchomienia instalatora, dostępu do pliku.

Centralna administracja systemem antywirusowym

1. Portal zarządzający jest dostępny w języku polskim.
2. Komunikacja pomiędzy portalem centralnego zarządzania a stacjami roboczymi odbywa się w formie zaszyfrowanej.
3. W celu korzystania z centralnej administracji, od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli zarządzającej znajdującej się na serwerach producenta.
4. Interfejs zarządzania posiada funkcję wyświetlania monitów o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.
5. Interfejs jest wyposażony w panel kontrolny zawierający podsumowanie stanu bezpieczeństwa organizacji w postaci graficznych wykresów.
6. Wykresy są interaktywne, tzn. że po wybraniu interesującego elementu, następuje przekierowanie do zawierającego bardziej szczegółowe dane menu.
7. Rozwiązanie posiada dedykowaną zakładkę zawierającą informację o wszystkich hostach posiadających zainstalowane oprogramowanie do ochrony, w tym: ich nazwy, status ochrony, przypisany profil bezpieczeństwa.
8. Istnieje możliwość eksportu listy wszystkich hostów do pliku CSV.
9. Administrator ma możliwość wglądu w szczegóły zgłaszającego się hosta, w których zawarte są informacje dotyczące: ostatniego podłączenia do konsoli zarządzającej, wersji zainstalowanego produktu, systemu operacyjnego, stanu ochrony, akcji związanych z wykrytymi zagrożeniami i skanowaniami.
10. Administrator ma możliwość z poziomu szczegółów klienta, uruchomienia skanowania antywirusowego, instalacji aktualizacji dla aplikacji i systemu operacyjnego, przypisania profilu, usunięcia urządzenia, zmiany klucza subskrypcji, odizolowania hosta od sieci i pobrania pliku diagnostycznego.
11. Komputery nie nawiązujące komunikacji z konsolą zarządzającą mogą być automatycznie usuwane z listy po określonym przez administratora czasie - co najmniej 60 dni.
12. Rozwiązanie posiada dodatkową zakładkę zawierającą informacje dotyczącą brakujących aktualizacji dla zainstalowanych aplikacji i systemu operacyjnego.

13. Istnieje możliwość posortowania i filtrowania brakujących poprawek pod względem ich poziomu krytyczności.
14. Informacje dotyczące brakujących poprawek dla aplikacji i systemu operacyjnego zawierają liczbę i typ hostów na których został wykryty brak danej poprawki.
15. Po wskazaniu danej poprawki administrator posiada możliwość jej instalacji na wskazanych komputerach lub na wszystkich komputerach i serwerach, dla których dana poprawka została wydana.
16. Administrator ma możliwość wglądu w historię instalowanych poprawek na chronionych hostach.
17. Rozwiązanie posiada moduł raportujący w którym wyświetlane są informacje dotyczące stanu ochrony, infekcji malware, instalowanych aplikacji.
18. Raporty mogą być tworzone zgodnie z harmonogramem i wysyłane na wskazane adresy email.
19. Rozwiązanie posiada wbudowany mechanizm zarządzania subskrypcjami, z możliwością dodawania nowych kluczy licencyjnych.
20. Administrator widzi w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji.
21. Portal zarządzający umożliwia dodawanie kluczy licencyjnych dla innych produktów w celu aktywacji danej funkcjonalności, co najmniej dla systemu EDR, mechanizmów zarządzania podatnościami, ochrony usług Microsoft 365.
22. Dodanie klucza licencyjnego skutkuje pojawieniem się dedykowanej zakładki obsługującej dany produkt w portalu zarządzającym.
23. Rozwiązanie ma możliwość definiowania różnych profili ustawień dla chronionych urządzeń z poziomu portalu zarządzającego.
24. Profile mogą być przypisane do pojedynczych hostów lub do grup.
25. Istnieje możliwość porównania 2 profili konfiguracyjnych w celu wyświetlenia różnic pomiędzy nimi.
26. Rozwiązanie pozwala administratorowi podczas tworzenia profili wskazanie funkcjonalności, które mogą być zmieniane przez użytkownika od strony chronionego hosta – możliwość wprowadzanych zmian jest do określenia dla poszczególnych funkcji programu oraz całości konfiguracji.
27. Z poziomu portalu zarządzającego istnieje możliwość pobrania plików instalacyjnych, wykorzystywanych do instalacji agenta na objętych licencją hostach.
28. Pliki instalacyjne mają posiadać plików .EXE, .MSI, .MPKG, .DEB, .RPM w zależności od platformy i typu systemu na jakich ma zostać zainstalowany agent.
29. Tworzone profile muszą dają administratorowi możliwość blokowania ustawień konfiguracyjnych aplikacji zainstalowanych od strony stacji roboczych w celu uniemożliwienia ich modyfikacji przez lokalnego użytkownika.
30. Portal zarządzający pozwala na zarządzanie oprogramowaniem instalowanym na urządzeniach mobilnych (smartphony) w przypadku posiadania odpowiedniej licencji.
31. Konsola posiada możliwość definiowania wielu kont administratorów o różnych poziomach dostępu.
32. W ramach posiadanych licencji istnieje możliwość przenoszenia oprogramowania w ramach danego klucza subskrypcji z jednej stacji roboczej na inną.

Dostarczenie i instalacja UPS

1. Wykonawca dostarczy i zainstaluje UPS w serwerowni Zamawiającego.

2. Moc pozorna UPS: min. 10000 VA
3. Moc rzeczywista: 10000 W
4. Topologia (klasyfikacja IEC 62040-3)On-line z korekcją współczynnika mocy
5. Sprawność przy pracy normalnej (100% obc.) >95 %
6. Sprawność w trybie podwyższonej sprawności (100% obc.) >95 %
7. Współczynnik mocy min. 0,9
8. Czas przełączenia na baterię 0 ms
9. Możliwość pracy równoległej
10. Liczba, typ gniazd wyjściowych: Listwa zaciskowa + 4 szt. IEC-320-C19
11. Typ gniazda wejściowego: Listwa zaciskowa
12. Czas podtrzymania dla 100% obciążenia dla pf=0,9 10 min
13. Czas podtrzymania przy 50% obciążenia dla pf=0,9 25 min
14. Możliwość dodania min. 10 dodatkowych modułów baterii w celu wydłużenia czasu podtrzymania do 98 minut dla 100% obciążenia przy pf=0,9
15. Napięcie znamionowe200/208/220/230/240/250 V
16. Tolerancja napięcia prostownika 180V – 270 V (100-270V przy 40% obciążenia)
17. Częstotliwość znamionowa: 50/60 Hz autodetekcja
18. Tolerancja częstotliwości 40 – 70 Hz
19. Kształt napięcia sinusoidalny
20. Napięcie znamionowe wyjściowe 200/208/220/230/240V/250V (do wyboru przez użytkownika)
21. Zakres zmian napięcia przy pracy autonomicznej: +/-1% napięcia nominalnego
22. Częstotliwość wyjściowa przy pracy autonomicznej: 50/60 Hz +/-0,5%
23. Współczynnik szczytu 3:1
24. Dopuszczalny zakres współczynnika mocy obc. liniowego: 0,5 indukcyjny - 0,5 pojemnościowy.
25. Baterie mogą wymieniane przez użytkownika "na gorąco” bez zatrzymywania pracy urządzenia.
26. Posiada system ochrony przed przeładowaniem - ograniczenie prądu ładowarki, wyłączenie ładowarki oraz alarm.
27. Ochrona przed głębokim rozładowaniem.
28. Okresowy automatyczny test baterii.
29. System nieciągłego ładowania baterii. Do oferty dołączyć należy opis algorytmu ładowania nieciągłego baterii. W opisie znaleźć się muszą informacje nt. trwania okresów ładowania forsującego, konserwującego i okresu spoczynkowego (tzw. restingu). Okres spoczynkowy w jednym cyklu nie może być krótszy niż 14 dni. Opis powinien być materiałem firmowym producenta lub musi być przez niego zatwierdzony.
30. Zdolność zwarciowa 150A
31. Możliwość uruchomienia bez napięcia w sieci.
32. Akumulatory wewnętrzne o pojemności nie mniejszej niż 9Ah 12V, minimum 40 szt. (łącznie UPS i moduł bateryjny)
33. Czas ładowania akumulatorów do poziomu 90% (dla akumulatorów wewnętrznych 20 szt.) < 1,5 godz. do 90% pojemności użytkowej
34. Posiada interfejsy komunikacyjne:
    - 34.1. USB
    - 34.2. RS232
    - 34.3. Styki przekaźnikowe

34.4. Miniport
34.5. Karta SNMP/Ethernet

35. Posiada panel sterowania z wyświetlaczem który dostarcza informacji o: stanie pracy urządzenia, stanie obciążenia, pomiarach i ustawieniach. Funkcje ustawień i odczytów: lokalne, wyjścia (napięcie wyjściowe, częstotliwość wyjściowa), baterii (test baterii), pomiary i dane (numer seryjny, napięcie i częstotliwość wejściowa i wyjściowa, poziom obciążenia, pozostały czas podtrzymania, wydajność, zużycie energii w kWh).
36. Wskaźnik pokazujący kolorami tryby pracy: zasilany z sieci, tryb bateryjny, usterka/awaria.
37. Sygnalizator akustyczny dla stanów:
    37.1. Awaria
    37.2. Niski stan naładowania
    37.3. Przeciążenie
    37.4. Wezwij serwis
38. UPS jest w obudowie typu Tower/Rack
39. W zestawie znajdują się:
    39.1. instrukcja obsługi
    39.2. Instrukcja bezpieczeństwa
    39.3. Kabel szeregowy RS232
    39.4. Kabel komunikacyjny USB
    39.5. Karta sieciowa SNMP/Ethernet
40. Oprogramowanie producenta UPS-a, musi dostarczać narzędzia potrzebne do monitorowania i kontrolowania urządzeń zasilających w środowiskach fizycznych i wirtualnych. Umożliwiać łatwe określanie strategii ciągłości działania, aby zachować gotowość urządzeń IT do pracy podczas zdarzeń wpływających na zasilanie lub otoczenie.
41. Oprogramowanie, musi m.in.: umożliwiać:
    41.1. Zdalne monitorowanie i sterowanie wieloma urządzeniami zasilania gwarantowanego w sieci z jednego interfejsu,
    41.2. Możliwość zdalnego zarządzania parametrami zamykania maszyn fizycznych oraz wirtualnych,
    41.3. Wykonywać zaplanowane wyłączenia maszyn wirtualnych oraz hostów m.in.: VMware, HyperV, RedHat KVM i Xen, a także macierzy.
    41.4. Pełną integrację z systemem VMware vRealize Operations Manager,
    41.5. Podstawowe kontrolowanie oraz podgląd gniazd listew PDU.
42. Karta sieciowa musi spełniać następujące warunki:
    42.1. Typ: Ethernet /10Mbps - Half duplex - 10Mbps - Full duplex - 100Mbps - Half duplex - 100Mbps - Full duplex - 1.0 Gbps - Full duplex
    42.2. Protokoły: MQTT/RNDIS/LDAP/NVD/SSH/PKI
    42.3. Szyfrowanie pakietem szyfrów TLS 1.2 z minimum SHA256
    42.4. Nadawanie użytkownikowi dostępu za pomocą konta. Konto może wygasać po odpowiedniej, wprowadzonej liczbie dni (hasło przestaje być aktywne)
    42.5. Komunikacja Web/SNMP
    42.6. Kompatybilna z SNMP v1/v3 i IP v4/v6
    42.7. Adresowanie IP: DHCP/BootP/Manualne
    42.8. MIB II - Standard IETF UPS MIB (RFC 1628)

42.9. Systemy operacyjne obsługiwane przy zamykaniu systemu Microsoft Windows, UNIX i Linux
42.10. Konfiguracja e-mail: SMTP
42.11. Panel HMI
42.12. Kompatybilność z ICSIDPS/ SCADA

43. Wraz z UPS zostaną dostarczone listwy zasilające PDU (6 szt.):
43.1. Montaż za pomocą zaczepów guzikowych z tyłu i z boku oraz uniwersalny system montażu w szafie RACK
43.2. Długość przewodu min. 3 metry
43.3. Zabezpieczenie przed rozłączeniem wtyczek standardu IEC
43.4. Temperatura pracy do 60 st. C
43.5. Gwarancja producenta min. 36 miesięcy
43.6. Trzy sztuki listew będą posiadały gniazdo wejściowe IEC 60309 16A 1P
43.7. Trzy sztuki listew będą posiadały gniazdo wejściowe IEC-320-C20
43.8. Dostarczone listwy będą w pełni kompatybilne z dostarczonym UPS.
43.9. Listwy zapewnią następujące wyjścia: 8 szt. IEC-320-C19 + 40 szt. IEC-320-C13

44. Wraz z zasilaczami awaryjnymi UPS należy dostarczyć następujące niezbędne materiały w celu dostosowania sieci energetycznej serwerowni:
44.1. Kabel energetyczny YKY 5x16 mm2 - 23 metry
44.2. Kabel przemysłowy H07RN-F 3x10 mm2 - 15 metrów
44.3. Wyłącznik nadprądowy 2P 63A charakterystyka zwłoczna "D" - 2 szt.
44.4. Rozłącznik modułowy 4P 80A

Dostarczenie systemu backup

1. Wykonawca dostarczy i wdroży oprogramowanie do tworzenia kopii bezpieczeństwa (backup).
2. Oprogramowanie do backupu min. 20 systemów (fizycznych lub wirtualnych) ze wsparciem technicznym na min. 3 lata.
3. Zamawiający nie dopuszcza oprogramowania w formie subskrypcji - oprogramowanie może być wykorzystywane bezterminowo.
4. Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter.
5. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner: https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions i spełniać minimalne wymaganie : minimalna liczba referencji 150, minimalna ocena z referencji 4,5
6. Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 oraz Microsoft Hyper-V 2008R2SP1, 2012, 2012 R2 i 2019. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej.
7. Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.
8. Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manager, klastrami hostów oraz pojedynczymi hostami.

9. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.
10. Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej.
11. Oprogramowanie musi tworzyć samowystarczalne archiwa do odzyskania których nie jest wymagana osobna baza danych z metadanymi deduplikowanych bloków.
12. Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-inremental)
13. Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji.
14. Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
15. Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli.
16. Oprogramowanie musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację z Microsoft Azure Blob, Amazon S3 oraz z innymi kompatybilnymi z S3 macierzami obiektowymi. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych.
17. Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
18. Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota.
19. Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time)
20. Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu.
21. Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API.
22. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji.
23. Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji.
24. Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania.
25. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.

26. Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej.
27. Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
28. Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych
29. Oprogramowanie musi oferować ten mechanizm z dokładnością do pojedynczego datastore.
30. Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora.
31. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware i być dostępna dla następujących macierzy: HPE, Dell EMC, NetApp, Cisco, IBM, Lenovo, Fujitsu, INFINIDAT, Pure Storage.
32. Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.
33. Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn.
34. Oprogramowanie musi posiadać wsparcie dla NDMP.
35. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son).
36. Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
37. Oprogramowanie musi umieć korzystać z protokołu Catalyst (w tym Catalyst Copy) w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
38. Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 lub 2019 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.
39. Repozytoria oparte o XFS muszą pozwalać na zmienność danych przez określoną ilość czasu (tzw. Immutability)
40. Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.
41. Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
42. Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla

replikacji ciągłej musi być możliwości zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punktu w ramach ustalonego parametru RPO.

43. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
44. Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)
45. Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
46. Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.
47. Dodatkowo dla środowiska vSphere i Hyper-V powyższa funkcjonalność powinna umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
48. Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami
49. Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre
50. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
51. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2.
52. Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików
53. Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
54. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z następujących systemów plików:
    - 54.1. Linux: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs
    - 54.2. Windows: NTFS, FAT, FAT32, ReFS
55. Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.
56. Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
57. Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników oraz pozwalać na odtworzenie haseł.
58. Oprogramowanie musi wspierać granularne odtwarzanie dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA oraz elementów AD Sites.

59. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"),
60. Oprogramowanie musi wspierać przywracanie danych Exchange do oryginalnego środowiska
61. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowszych
62. Oprogramowanie musi wspierać odtworzenie point-in-time wraz z możliwością przywrócenia bazy do oryginalnego środowiska
63. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowszych
64. Oprogramowanie musi wspierać odtworzenia elementów, witryn, uprawnień dla witryn Sharepoint.
65. Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.
66. Oprogramowanie musi pozwalać na zaprezentowanie oraz migrację online baz MS SQL oraz Oracle bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego
67. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN.
68. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA.
69. Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN
70. Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu.
71. Dla VMware’a oprogramowanie musi pozwalać na uruchomienie takiego środowiska bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.
72. Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem
73. Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere
74. Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.
75. Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.

Szkolenie w zakresie zarządzania ryzykiem, dokumentacją i polityką bezpieczeństwa w jednostkach publicznych w świetle rozporządzenia Rady Ministrów z dn. 12.04.2012 r.

1. Czas trwania szkolenia to min. 6h
2. Dostarczone zostaną materiały szkoleniowe w postaci papierowej dla każdego uczestnika.
3. Ilość uczestników szkolenia to maksymalnie 15 osób.
4. Dopuszcza się szkolenie lokalne w siedzibie Zamawiającego oraz szkolenie on-line.
5. Szkolenie będzie prowadzone w dni robocze w godz. roboczych Zamawiającego (7:25 - 15:00)
6. Szkolenie obejmie:
    a. Krajowe Ramy Interoperacyjności - omówienie.
    b. Omówienie ustawy o KSC
    c. Przepisy o ochronie danych osobowych - RODO i UODO.
    d. Procesy zarządzania bezpieczeństwem informacji.
    e. Identyfikacja aktywów chronionych, klasyfikacja, identyfikacja systemów kluczowych.
    f. Metody identyfikacji ryzyka.
    g. Metody analizy ryzyka.
    h. Zasady oceny ryzyka.
    i. Kryteria akceptowalności ryzyka.
    j. Formułowanie planów postępowania z ryzykiem.
    k. Monitorowanie i audytowanie
        i. Dobór i pomiar wskaźników bezpieczeństwa.
        ii. Zasady prowadzenia audytu bezpieczeństwa informacji.
    l. Zarządzanie incydentami KRI i RODO.

Szkolenie w zakresie wykonywania kopii zapasowych oraz tworzenia polityki ciągłości działania

1. Czas trwania szkolenia to min. 12h
2. Dostarczone zostaną materiały szkoleniowe w postaci papierowej dla każdego uczestnika.
3. Ilość uczestników szkolenia to 4 osoby.
4. Dopuszcza się szkolenie lokalne w siedzibie Zamawiającego oraz szkolenie on-line.
5. Szkolenie będzie prowadzone w dni robocze w godz. roboczych Zamawiającego (7:25 - 15:00)
6. Szkolenie obejmie:
    6.1. Wprowadzenie do zarządzania ciągłością działania
        6.1.1. Wprowadzenie do zarządzania ciągłością działania
        6.1.2. Zarys zarządzania ciągłością działania.
        6.1.3. Wymagania prawne w obszarze zarządzania ciągłością działania.
        6.1.4. Standardy, normy i źródła dobrych praktyk.
        6.1.5. Zarządzanie ciągłością działania w teorii.
        6.1.6. Omówienie wymagań normy ISO 22301.
        6.1.7. Terminy i definicje.

6.2. Klasyczny cykl zarządzania ciągłością działania – wykład, ćwiczenia
- 6.2.1. Omówienie cyklu PDCA (Plan, Do, Check, Act (zaplanuj, wykonaj, sprawdź, działaj).
- 6.2.2. Opracowanie Polityki zarządzania ciągłością działania – cele, zakres.
- 6.2.3. Określenie roli i zadań najwyższego kierownictwa.
- 6.2.4. Kompetencje i zadania osób odpowiedzialnych za budowę i wdrożenie zarządzania ciągłością działania w organizacji.
- 6.2.5. Zasoby niezbędne od ustanowienia i wdrożenia BCMS.
- 6.2.6. Najważniejsze czynniki wdrożenia zarządzania ciągłością działania.

6.3. Zrozumienie organizacji
- 6.3.1. Analiza Wpływu na Biznes (Business Impact Analysis).
- 6.3.2. Organizowanie efektywnego zespołu BIA.
- 6.3.3. Identyfikacja krytycznych procesów, zasobów i usług dostarczanych przez dostawców i partnerów outsourcingowych – ćwiczenie.
- 6.3.4. Kluczowe wskaźniki wpływu zdarzenia na biznes (MTPoD,RTO,RPO).
- 6.3.5. Metody zbierania danych.
- 6.3.6. Budowa szablonów BIA.
- 6.3.7. Przygotowanie ankiety oceny analizy wpływu zdarzenia na biznes.
- 6.3.8. Minimalna akceptowalna konfiguracja.
- 6.3.9. Szacowanie ryzyka ukierunkowane na ciągłość działania.
- 6.3.10. Identyfikacja zagrożeń i sposoby postępowania z ryzykiem.
- 6.3.11. Prezentacja wyników analizy BIA dla kierownictwa.
- 6.3.12. Rezultaty biznesowe analizy wpływu zdarzenia na biznes.

6.4. Strategia zarządzania ciągłością działania
- 6.4.1. Definicja i cel strategii.
- 6.4.2. Budowa scenariuszy postępowania i określenie sposobów wznowienia krytycznych procesów i zasobów – ćwiczenie.
- 6.4.3. Scenariusze sytuacji kryzysowych i opracowanie strategii postępowania – ćwiczenie.
- 6.4.4. Strategie w obszarze biznesowym.
- 6.4.5. Strategie w obszarze IT.

6.5. Struktura zarządzania kryzysowego – wykład, ćwiczenia
- 6.5.1. Dlaczego potrzebujemy Planu Zarządzania Kryzysowego?
- 6.5.2. Zasady wyznaczenia osób w strukturze zarządzania kryzysowego.
- 6.5.3. Budowa graficznej struktury zarządzania kryzysowego w organizacji – ćwiczenie.
- 6.5.4. Określenie zadań , uprawnień i kompetencji dla zespołów kryzysowych.
- 6.5.5. Opracowanie reakcji w sytuacjach awaryjnych, kryzysowych.
- 6.5.6. Plan, zasoby, procedury i komunikacja w zarządzaniu kryzysowym.
- 6.5.7. Zasady współpracy ze służbami pracującymi w trybie ciągłym.
- 6.5.8. Zasady współpracy z lokalnymi Sztabami Zarządzania Kryzysowego (powiat, województwo)

6.6. Plan Ciągłości Działania – wykład, ćwiczenia
- 6.6.1. Dlaczego potrzebujemy Planu Ciągłości Działania (BCP)?
- 6.6.2. Cechy dobrego Planu Ciągłości Działania (BCP).
- 6.6.3. Cel i zakres Planów Ciągłości Działania.
- 6.6.4. Zasady opracowania struktury dokumentacji BCP – ćwiczenie.

6.6.5. Podstawowe procedury BCP.
6.6.6. Zasady uruchomienia BCP.
6.6.7. Zasady komunikacji i linie łączności.
6.6.8. Kluczowe zadania i odpowiedzialności osób i zespołów w ramach BCP.
6.6.9. Zasoby niezbędne do uruchomienia BCP.
6.6.10. Komunikacja zewnętrzna (media, pracownicy, interesariusze).
6.6.11. Proces wycofania Planów Ciągłości Działania.

6.7. Testowania utrzymanie i przegląd systemu zarządzania ciągłością działania (BCMS) – wykłady, ćwiczenia
6.7.1. Czemu służą testy?
6.7.2. Podstawowe zasady testowania.
6.7.3. Opracowanie planów i scenariuszy testów – ćwiczenie.
6.7.4. Ryzyka związane z realizacją testów.
6.7.5. Dokumentowanie testów.
6.7.6. Zasady przeglądu ustaleń związanych z BCMS.
6.7.7. Dane wejściowe do przeglądu.
6.7.8. Wyniki przeglądu.

6.8. Audyt i działania zapobiegawcze i korygujące – wykład
6.8.1. Zasady audytowania i opracowanie planów audytu.
6.8.2. Audyt wewnętrzny i zewnętrzny.
6.8.3. Częstotliwość i zakres audytu.
6.8.4. Działania zapobiegawcze.
6.8.5. Działania korygujące.

Konfiguracja StormShield SN910

1. Wykonawca skonfiguruje do pracy w sieci Zamawiającego klaster urządzeń SN910. Konfiguracja umożliwi przekierowanie całego ruchu sieciowego przez urządzenie brzegowe i obejmie następujące elementy:
    a. Konfiguracja interfejsów i routingów.
    b. Konfiguracja firewalla.
    c. Konfiguracja NAT.
    d. Konfiguracja IPS.
    e. Konfiguracja usług dodatkowych: DHCP, DNS Proxy.
    f. Integracja z ActiveDirectory.
    g. Konfiguracja transparentnej autoryzacji w ActiveDirectory.
    h. Konfiguracja VPN:
        i. IPSec Site-to-Site
        ii. IPSec Client-to-Site
    i. Konfiguracja i produkcyjne uruchomienie DMZ obejmujące do 10 maszyn wirtualnych.

Dostarczenie i instalacja macierzy

1. Wykonawca dostarczy, zainstaluje i uruchomi macierz w serwerowni Zamawiającego.

2. Istnieje możliwość zarządzania macierzą zarówno z poziomu interfejsu graficznego jak i z linii komend.
3. Dostępne jest stałe monitorowanie stanu macierzy (w tym monitorowanie wydajności) oraz możliwość konfigurowania jej zasobów. Macierz jest dostarczona z w/w funkcjonalnościami na zainstalowaną przestrzeń dyskową

1. Łączna zainstalowana pojemność surowej przestrzeni dyskowej minimum 140TB na dyskach NL-SAS 7200 RPM 3,5". Min 14 dysków o fizycznej pojemności nie mniejszej niż 10 TB.
4. Macierz umożliwia rozbudowę przestrzeni dyskowej do min 500 napędów dyskowych bez konieczności wymiany kontrolerów macierzowych (tylko poprzez dodawanie półek i dysków)
5. Macierz może zostać rozbudowana o dyski SSD, SAS, NLSAS z możliwością dowolnej konfiguracji i mieszania dysków w obrębie jednej macierzy.
6. Obudowa do montażu w szafie rack 19" za pomocą dostarczonych dedykowanych elementów
7. Macierz musi obsługiwać dyski 2,5" oraz 3,5". Wymagana obsługa dysków SSD, HDD SAS, HDD NL SAS.
8. Obudowa z kontrolerami umożliwiać instalację min. 12 dysków 3,5". Muszą być dostępne półki dyskowe w rozmiarze nie większym niż 2U obsługujące dyski 2,5" oraz półki dyskowe w rozmiarze nie większym niż 4U obsługujące dyski 3,5".
9. Kontrolery macierzy obsługują tryb pracy w układzie active-active. Macierz musi być dostarczona z zainstalowanymi minimum 2 kontrolerami.
10. Każdy z kontrolerów macierzy posiada po minimum 32 GB pamięci podręcznej Cache – zawartość pamięci Cache musi być identyczna dla wszystkich kontrolerów macierzy.
11. Macierz musi być wyposażona w zabezpieczenie stanu pamięci cache np. na wypadek awarii zasilania - pamięć cache zapisu mirrorowana między kontrolerami.
12. Kontrolery muszą posiadać możliwość ich wymiany (w przypadku awarii lub planowych zadań utrzymaniowych) bez konieczności wyłączania zasilania całego urządzenia.
13. Macierz musi obsługiwać wymianę kontrolera RAID bez utraty danych zapisanych na dyskach.
14. Macierz musi umożliwiać wymianę minimum 1 kontrolera bez konieczności wyłączania zasilania całego urządzenia.
15. Każdy z kontrolerów macierzy wyposażony co najmniej w procesor wykonany w technologii wielordzeniowej z minimum 12 rdzeniami.
16. Każdy kontroler macierzy pozwala na konfigurację interfejsów niezbędnych dla współpracy w sieci LAN, FC SAN oraz NAS.
17. Oferowana macierz musi mieć minimum 12 portów ETH minimum 10Gb/s (z wkładkami optycznymi) do dołączenia serwerów bezpośrednio lub do dołączenia do sieci SAN; minimum 8 portów ETH minimum 1Gb/s BASE-T.
18. Oferowana macierz musi mieć minimum 8 portów FC minimum 16Gb/s (z wkładkami optycznymi) do dołączenia serwerów bezpośrednio lub do dołączenia do sieci SAN.
19. Macierz musi zapewniać poziom zabezpieczenia danych na dyskach definiowany poziomami RAID: 0, 1, 10, 5, 50, 6.
20. Macierz musi być wyposażona w nadmiarowe mechanizmy badania integralności składowanych danych.

21. Prezentacja dysków logicznych o pojemności większej niż zajmowana przestrzeń dyskowa (Thin Provisioning). Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.
22. Macierz dostarcza funkcjonalność zwrotu wykasowanej przestrzeni dyskowej do puli zasobów wspólnych (Space Reclamation).
23. Migracja danych wolumenu logicznego pomiędzy różnymi technologiami dyskowymi (Tiering). Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.
24. Macierz umożliwia migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych (Tiering) na poziomie całych woluminów logicznych lub jego fragmentów bez konieczności rekonfiguracji po stronie serwerów korzystających z woluminów logicznych
25. Tworzenie na żądanie tzw. migawkowej kopii danych (ang. snapshot) w ramach macierzy. Wymagana jest minimalna ilość 1024 snapshot'ów. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.
26. Tworzenie na żądanie pełnej kopii danych (klon) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych bez przerywania dostępu do danych dla hostów. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.
27. Macierz dostarcza funkcjonalność podłączenia macierzy innych producentów do oferowanej macierzy i udostępnianie zasobów wirtualizowanego urządzenia jako własnego. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.
28. Macierz musi umożliwiać uruchomienie mechanizmów zdalnej replikacji danych z innymi macierzami (ten sam model/rodzina modeli) - w trybie synchronicznym i asynchronicznym. Funkcjonalność replikacji danych musi być zapewniona z poziomu oprogramowania wewnętrznego macierzy. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.
29. Macierz musi posiadać funkcjonalność zarządzania wydajnością, która dynamicznie przydziela zasoby macierzy w celu spełnienia określonych celów wydajnościowych aplikacji (QoS). Możliwość ustawiania priorytetów wydajności dla aplikacji w oparciu o zdefiniowane profile wolumenowe, dla wydajności w IOPS i przepustowości danych. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.
30. Model oferowanej macierzy musi wspierać rozwiązanie klastra „wysokiej dostępności" tj. zapewnienia wysokiej dostępności zasobów danych macierzy dla podłączonych platform software'owych i sprzętowych z wykorzystaniem synchronicznej replikacji danych po FC lub iSCSI pomiędzy minimum 2 macierzami. Pod użytym pojęciem „wysoka dostępność zasobów dyskowych" należy rozumieć zapewnienie bezprzerwowego działania środowiska (aplikacja/ system operacyjny/ serwer) podłączonego do macierzy (macierz podstawowa) w przypadku wystąpienia awarii logicznego połączenia z tą macierzą bądź awarii samej macierzy, powodujących dla danego środowiska brak dostępu do zasobów macierzy podstawowej.
31. Replikacja danych pomiędzy macierzami podstawową i zapasową, wykorzystanych w układzie „wysokiej dostępności", musi wspierać klastrowanie wybranych

woluminów bez konieczności stosowania lustrzanej konfiguracji grup dyskowych pomiędzy macierzami podstawową i główną. Musi być możliwość dodawania woluminów objętych zabezpieczeniem w klastrze bez konieczności zatrzymywania replikacji.

32. Funkcjonalność „wysokiej dostępności" musi pozwalać na automatyczne przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową w przypadku awarii macierzy podstawowej (tzw. automated failover).
33. Funkcjonalność „wysokiej dostępności" musi pozwalać na ręczne (zaplanowane) przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową (tzw. manual failover).
34. Funkcjonalność „wysokiej dostępności" musi pozwalać na minimum ręczne przełączanie obsługi środowisk produkcyjnych z macierzy zapasowej na podstawową po usunięciu awarii macierzy podstawowej (tzw. failback).
35. Funkcjonalność „wysokiej dostępności" musi wspierać konfiguracje z macierzą zapasową zainstalowaną w innej fizycznej lokalizacji o ile nadal spełnione są warunki dla realizacji synchronicznej replikacji danych pomiędzy lokalizacjami.
36. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane.
37. Macierz dyskowa musi zostać objęta minimum 5 letnim okresem gwarancji producenta 9x5xNBD (następnego dnia roboczego) . Producent macierzy musi umożliwiać skuteczne zgłaszanie usterek w trybie całodobowym.
38. Serwis gwarancyjny obejmuje dostęp do poprawek i nowych wersji firmware, które są elementem zamówienia przez cały okres obowiązywania gwarancji.
39. Oferowana macierz musi być fabrycznie nowa, Macierz pochodzi z legalnego kanału sprzedaży producenta. Nie dopuszcza się użycia macierzy odnawianych, demonstracyjnych lub powystawowych.
40. Urządzenie wykonane jest zgodnie z europejskimi normami.
41. Zamawiający wymaga dokumentacji w języku polskim lub angielskim.

Wymagany zakres prac

Wykonawca zobowiązany jest wdrożyć w pełnym zakresie dostarczone rozwiązanie i zintegrować je z istniejącą w Szpitalu infrastrukturą. W szczególności:

- dostarczony system backupu z posiadanym systemem wirtualizacji i serwerami NAS,
- dostarczonych UPS z systemem backupu i systemem wirtualizacji,
- dostarczony antywirus z dostarczoną macierzą i systemem wirtualizacji,
- dostarczonej macierzy z dostarczonym systemem backupu oraz systemem wirtualizacji i posiadaną macierzą,

Ponadto Wykonawca musi wdrożyć konfigurację posiadanych urządzeń UTM do prawidłowej pracy z dostarczoną infrastrukturą.

Szkolenia mają na celu również przygotowanie personelu do prawidłowej pracy z dostarczonymi elementami infrastruktury.

Uzasadnienie braku podziału zamówienia na części

W ramach postępowania dostarczony zostanie sprzęt i oprogramowanie systemowe pracujące wspólnie z istniejącą infrastrukturą. Ze względów technologicznych i wykonawczych (sprzęt i zainstalowane na nim oprogramowanie muszą być skonfigurowane łącznie – bez oprogramowania sprzęt nie spełni swojej roli i odwrotnie) postępowanie nie może być podzielone na części.

Podział zamówienia na części groziłby nadmiernymi trudnościami technicznymi w związku z potrzebą skoordynowania działań różnych wykonawców realizujących wspólnie poszczególne części zamówienia w celu realizacji całego projektu. W przypadku podziału na części wykonawca części programowej musiałby dostosowywać się (a przede wszystkim zakładać taką możliwość), że wdrożenie miałoby się odbywać na sprzęcie, którego nie będzie dostarczał i który może nie być skonfigurowany zgodnie z jego potrzebami a zmiana konfiguracji w najgorszym przypadku mogłaby wiązać się z utratą gwarancji producenta sprzętu. Tym samym instalacja, konfiguracja i parametryzacja sprzętu (a być może i konieczność poniesienia kosztów gwarancyjnych) również nie leżałaby po jego stronie. W takim przypadku wykonawca części softwarowej może mieć uzasadnione obawy co do przebiegu swojego wdrożenia, co zapewne uwzględni w ofercie cenowej – skalkulowane w ofercie ryzyko związane z wdrożeniem jest większe, zatem cena również musi zostać odpowiednio podwyższona. Wdrożenia oprogramowania nie da się oddzielić od wdrożenia części sprzętowej, ponieważ przy wdrażaniu kompleksowego systemu informatycznego zawsze jest tak, że poprawna praca oprogramowania wymaga odpowiednich konfiguracji sprzętowych. Ze względów różnic technologicznych pomiędzy starą infrastrukturą a nowo wdrażaną (głównie z powodu różnicy w architekturze) oraz ograniczeń pojemności starej infrastruktury Zamawiającego, nie ma możliwości uruchomienia usług na starym sprzęcie i dokonania ich migracji na nowy w momencie kiedy ten będzie już dostarczony przez Wykonawcę części sprzętowej – o ile w ogóle będzie. W przypadku podziału takiego zamówienia na części, na etapie wdrożenia występowałyby problemy przy zmianach konfiguracyjnych sprzętu, ponieważ konfiguracja leżałaby po stronie dostawcy sprzętu. Rodzi to też ryzyko podwójnej zapłaty za te same czynności, ponieważ i jeden i drugi wykonawca w ofercie musiałby w praktyce wycenić zakres konfiguracji i parametryzacji sprzętu. Istnieje również ryzyko, że wykonawca wybrany do części programowej nie będzie miał uprawnień i/lub kompetencji do zmian konfiguracyjnych sprzętu dostarczonego przez wykonawcę części sprzętowej. Wykonawca części programowej niekonieczne musi mieć bowiem kompetencje właściwe do konfiguracji wszystkich dostępnych na rynku urządzeń. Z drugiej strony Wykonawca części sprzętowej nie będzie miał pojęcia jaki dokładnie sprzęt będzie najodpowiedniejszy dla dostarczanego oprogramowania i nie będzie mógł zaoferować rozwiązania skrojonego dokładnie na potrzeby Zamawiającego i umożliwiające uruchomienie zaoferowanego oprogramowania.

Zamawiający dokonując opisu przedmiotu zamówienia, dla tak obszernego projektu, gdzie wiele aspektów technicznych sprzętu zależy od konkretnej technologii użytej w dostarczonym oprogramowaniu (*np. interfejs przeglądarkowy czy aplikacja desktopowa, aplikacje windowsowe czy linuxowe, aplikacje pisane w Javie czy w PHP, itd…*) zmuszony jest opisać niektóre jego elementy w sposób bardzo ogólny (*w celu uniknięcia zarzutu ograniczenia konkurencji)* i precyzować jedynie niektóre minimalne parametry techniczne, które w konfrontacji z szczególnym sprzętem dostarczonym przez Wykonawcę części

sprzętowej może nie odpowiadać dostarczonemu oprogramowaniu. W konsekwencji Zamawiający może otrzymać sprzęt spełniający wszystkie minimalne parametry opisane w SWZ jednakże niedostosowane do potrzeb oprogramowania (np. procesor cztero-rdzeniowy w macierzy i licencję na oprogramowanie na dwa procesory). Z uwagi, na to że nie można wymusić na Wykonawcy jednej części zamówienia aby jego rozwiązanie było kompatybilne w 100% i dostosowane do konkretnej technologii opisanej w innej części zamówienia, otrzymanie niekompatybilnej lub nieodpowiednio dobranej infrastruktury jest bardzo realnym zagrożeniem. Rozwiązanie techniczne, realizowane w ramach projektu stanowi integralną całość realizacyjną. Przedmiotem zamówienia w tym przypadku jest system informatyczny jako całość. Nie jest to dostawa oprogramowania i sprzętu, który będzie używany do różnych celów. Zamawiany sprzęt ma stworzyć środowisko teleinformatyczne, które razem z oprogramowaniem tworzyć będzie jednolity system informatyczny.

Wykonywanie całego zamówienia przez jeden podmiot niewątpliwie wpłynie pozytywnie na szybkość i sprawność realizacji całego projektu. Wykonawca odpowiedzialny za całość realizacji nie będzie mógł doszukiwać się przeszkód realizacyjnych leżących np. po stronie dostawcy sprzętu (nie działający sprzęt, zła konfiguracja, uniemożliwiająca wdrożenie oprogramowania, itp.) jednocześnie w przypadku wystąpienia problemu sprzętowego będzie mógł dokładnie przeorganizować harmonogram, tak aby mógł się skupić na innej części wdrożenia w oczekiwaniu na rozwiązanie problemu bez zbędnej zwłoki. Uniknięcie „rozmycia się" odpowiedzialności gwaranta za nienależyte wykonanie zamówienia z pewnością jest ważnym aspektem w przypadku projektów objętych pewnymi sztywnymi ramami czasowymi. W przypadku niepowodzenia wdrożenia systemu, wykonawca części softwarowej zawsze będzie bronił się tym, że sprzęt był niewłaściwy, nie dostarczony na czas, źle podłączony, źle skonfigurowany, itd. W przypadku braku podziału na części takich argumentów nie będzie mógł podnieść, ponieważ to on będzie odpowiedzialny za całość wdrożenia.

Ponadto w przypadku podzielenia zamówienia na części istnieje realne ryzyko niewykonania części zamówienia (czy to programowej czy to sprzętowej) co groziłoby niewykonaniem całego projektu lub zakup elementów niekompatybilnych lub nie użytecznych w 100%. Ważnym czynnikiem determinującym przeprowadzenie postępowania w jednej części jest również czas, czas potrzebny na przeprowadzenie postępowania, czas potrzebny na wdrożenie systemów. Wszystkie te elementy muszą być skoordynowane w czasie i niedotrzymanie terminu przez jeden element powoduje przesunięcie wszystkich pozostałych elementów. Alternatywna realizacja projektu w etapach polegających na dostarczeniu sprzętu a potem (*mając już pewność co do terminu dostawy sprzętu*) ogłoszeniu odrębnego postępowania na oprogramowanie, jest czasowo i funkcjonalnie nieuzasadniona. Konieczność koordynowania działań wykonawców nastręczałaby w przypadku podziału zamówienia tak wiele kłopotów, że w praktyce mogłaby spowodować paraliż organizacyjny Zamawiającego.

Kryterium parametry jakościowe - techniczne

Kryteria dot. UPS

Sprawność w trybie podwyższonej sprawności (100% obc.):

- 95% - 0 pkt
- 98% - 10 pkt

Moc pozorna UPS:

- 10000 VA - 0 pkt
- 11000 VA - 10 pkt

Kryteria dla macierzy

Obsługiwana ilość snapshot'ów:

- 1024 - 0 pkt
- 2048 - 5 pkt

Procesory kontrolerów macierzy:

- 12 rdzeni - 0 pkt
- 16 rdzeni - 5 pkt

Ilość pamięci CACHE:

- 32 GB / kontroler - 0 pkt
- 64 GB / kontroler - 10 pkt