Załącznik nr 2 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

Dotyczy: postępowania o udzielenie zamówienia publicznego prowadzonego w trybie podstawowym bez przeprowadzenia negocjacji o wartości poniżej 215 tys. euro

Zakup i wdrożenie systemów teleinformatycznych z zakresu „cyberbezpieczeństwa"
Nr sprawy: Sp/AZP/382/6/2022

Ogólny opis przedmiotu zamówienia:

Przedmiotem zamówienia jest rozbudowa infrastruktury informatycznej zamawiającego w ramach finansowania działań w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców.

Projekt będzie realizowany w oparciu o harmonogram przygotowany przez Wykonawcę i zatwierdzony przez Zamawiającego nie później niż 2 dni od daty podpisania umowy.

Asortyment:

LP.	Nazwa	Ilość
1	Oprogramowanie do Kopii Zapasowych	1
2	Serwer oraz Serwer NAS na redundantny, odmiejscowiony Backup	1
3	System Zarządzania Tożsamością i Uprawnieniami	1
4	Szkolenie z Cyberbezpieczeństwa	1
5	Przełączniki Sieciowe	5
6	Zapora Sieciowa UTM i System XDR	1
7	Oprogramowanie do monitorowania systemów klasy HIS	1
8	Oprogramowanie do monitorowania, gromadzenia, analizy zdarzeń	1
9	Opracowania podstawowego pakietu dokumentów z zakresu bezpieczeństwa systemów informatycznych	1

Termin realizacji przedmiotu zamówienia:

Termin realizacji przedmiotu zamówienia wynosi do 30 dni od daty zawarcia umowy.

Opis funkcjonalny wymagany przez Zamawiającego obejmuje:

1. Oprogramowanie do Kopii Zapasowych

Dostarczenie oprogramowania do kopii zapasowych.

Opis postępowania:
Przedmiotem zamówienia jest dostawa, instalacja, konfiguracja oraz uruchomienie przez Wykonawcę oprogramowania do wykonywania kopii zapasowych.

Wymagania minimalne

Oprogramowanie do kopii zapasowych
Ogólne
Rozwiązanie musi zapewniać wsparcie backupu dla następujących platform wirtualizacyjnych, środowisk chmurowych i maszyn fizycznych, przy czym obsługa poszczególnych z nich może być uwarunkowana wybranym typem licencji Microsoft Server z rolą Hyper-V min. w wersjach 2022, 2019, 2016, 2012R2, 2012 Vmware vSphere min. w wersjach v5.5-7.0.3 Nutanix AHV 5.10, 5.15, 5.20 (LTS) Maszyny fizyczne: Windows Server 2022, 2019, 2016, 2012R2, 2012, 2008R2 Microsoft 365 (Exchange online, One Drive for Business, Sharepoint) Oprogramowanie musi wspierać wszystkie systemy operacyjne gościa, które są obsługiwane przez natywny backup środowisk VMware vSphere, MS Hyper-V Oprogramowanie musi być niezależne sprzętowo i posiadać możliwość uruchomienia: na serwerze Windows lub Linux jako maszyna wirtualna Vmware jako maszyna wirtualna Amazon na serwerze NAS: ASUSTOR, NETGEAR, QNAP, Synology i Western Digital Oprogramowanie do backupu musi pozwalać na wykorzystanie dowolnego serwera oraz przestrzeni dyskowej (nie dedykowanych), za pośrednictwem protokołów CIFS lub NFS Oprogramowanie nie może wymagać instalacji dedykowanego agenta wewnątrz maszyny wirtualnej w celach backupu/przywracania Oprogramowanie nie może wymagać dodatkowej instalacji zewnętrznych aplikacji lub baz danych (jeżeli oprogramowanie wymaga bazy danych musi ona być instalowana automatycznie z paczki opracowanej przez producenta i nie wymagać dodatkowych licencji).
Licencjonowanie
Wszystkie funkcje i komponenty oprogramowania dla środowisk Vmware i Hyper-V powinny być licencjonowane per gniazdo procesora w hostach wirtualizacyjnych służących za źródło backupu lub replikacji. Licencjonowanie powinno być realizowane w wariancie wieczystym, w którym licencja nie ma terminu ważności Dopuszczalne jest dostarczenie oprogramowania w wersji umożliwiającej ograniczoną rozbudowę środowiska, wersja ta powinna jednak umożliwiać rozbudowę do nie mniej niż 6 gniazd procesorów w obrębie środowiska W ramach dostarczonej licencji na określoną ilość gniazd procesorów wymagane jest zapewnienie 1 roku wsparcia technicznego producenta, zapewniającego dostęp do aktualizacji i poprawek oprogramowania oraz umożliwiającego kontakt z działem technicznym producenta w zakresie oferowanego oprogramowania **W ramach dostawy wymagane jest dostarczenie licencji na ochronę 4 gniazd procesorów w hostach Vmware lub Hyper-V** Licencjonowanie innych środowisk może być realizowane na zasadzie wymagającej zakupu dedykowanej licencji dla środowiska

Ochrona danych

Oprogramowanie musi posiadać funkcje backupu i replikacji:

- Backup maszyn wirtualnych Vmware
- Replikacja maszyn wirtualnych Vmware (tworzenie I aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu
- Backup maszyn wirtualnych Hyper-V
- Replikacja maszyn wirtualnych Hyper-V (tworzenie I aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu
- Możliwość przesłania pierwszych kopii za pośrednictwem dysków zewnętrznych do lokalizacji docelowej oraz późniejsze wznowienie ochrony maszyn wirtualnych
- Możliwość określania pasma wykorzystywanego przez oprogramowanie do backupu globalnie lub per zadanie
- Możliwość tworzenia do 1000 punktów przywracania dla każdej z maszyn wirtualnych w ramach zadania backupu
- Obsługa retencji zgodnie z zasadą Grandfather-father-son – oprogramowanie musi pozwalać na rotację punktów przywracania w trybie dziennym, tygodniowym, miesięcznym oraz rocznym
- "Kopia backupu (replikacja) do innych repozytoriów backupu lokalnych oraz zdalnych
- Oprogramowanie musi pozwalać na utworzenie kopii źródłowego repozytorium backupu oraz tylko wybranych backupów. Kopia tworzona jest zgodnie z określonym harmonogramem"
- Oprogramowanie musi pozwalać na określenie kolejności, w jakiej są backupowane lub replikowane maszyny wirtualne w ramach zadania
- Oprogramowanie musi umożliwiać tworzenie scenariuszy odtwarzania w środowiskach wirtualnych składających się z wielu etapów np. wyłączenia/włączenia maszyny, odczekania określonego czasu, wykonania jednego lub wielu wcześniej utworzonych zadań backupu lub replikacji
- Oprogramowanie musi udostępniać widok kalendarza z naniesionymi zadaniami backupu/replikacji w celu łatwiejszego zarządzania zadaniami w bardziej złożonych środowiskach

Optymalizacja wykorzystania miejsca na dane

Oprogramowanie musi posiadać poniższe funkcje pozwalające na ograniczenie wielkości backupowanych danych:

- Deduplikacja backupu, która działa w ramach całego repozytorium backupu oraz obejmuje wszystkie dane, które są w tym repozytorium przechowywane
- Kompresja backupu, w tym konfigurowalny stopień kompresji
- Automatyczne pomijanie plików i partycji wymiany w systemach Windows i Linux działających jako maszyny wirtualne

Spójność Danych

Oprogramowanie musi posiadać poniższe funkcje, gwarantujące spójność danych:

- Spójny backup i replikacja maszyn wirtualnych z systemami Windows i Linux
- Oprogramowanie musi umożliwiać wykonywanie własnych skryptów przed wykonaniem backupu oraz po jego wykonaniu
- Automatyczne usuwanie (trunking) logów transakcyjnych z poniższych aplikacji:
- Microsoft Exchange 2013, 2016, 2019
- Microsoft SQL 2008, 2008R2, 2012, 2014, 2016, 2017, 2019

- Automatyczna weryfikacja utworzonych backupów oraz replik ze środowiska Vmware poprzez uruchamianie maszyny wirtualnej bezpośrednio z backupu lub uruchamianie repliki
- Oprogramowanie pozwala na generowanie oraz automatyczne wysyłanie raportów ze zrzutami ekranu testowanych maszyn wirtualnych Vmware i Hyper-V
- Pełna weryfikacja wszystkich danych przechowywanych w repozytorium backupu na żądanie, ze wskazaniem niespójnych punktów przywracania
- Szyfrowanie danych przesyłanych przez sieć do zdalnego repozytorium backupu i/lub repozytorium replikacji

Przywracanie danych

Oprogramowanie musi posiadać poniższe funkcje:

- Przywracanie pełnych maszyn wirtualnych z backupu do oryginalnego lub innego serwera wirtualizacji
- Uruchomienie maszyny wirtualnej bezpośrednio z plików backupu w środowisku VMware (bez wcześniejszego przywracania maszyny wirtualnej)
- Przywracanie pojedynczych plików czy folderów bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej)
- Przywracanie pojedynczych obiektów z poniższych aplikacji, bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej z backupu czy rozpakowywania plików backupu):
- Microsoft Exchange
- MS Active Directory
- MS SQL
- Migracja dysków maszyn wirtualnych pomiędzy środowiskami wirtualizacji Vmware i Hyper-V i odwrotnie.

Wydajność i Zarządzanie

Oprogramowanie do backupu musi pozwalać na:

- Tworzenie backupu I replik przyrostowo przy wykorzystaniu VMware CBT oraz Hyper-V RCT
- Wykonywanie backupów przyrostowych bez wymogu okresowego tworzenia kopii pełnych
- Backup z pominięciem sieci lan dzięki opcjom dostępu bezpośredniego w sieciach SAN
- Akceleracją sieciową umożliwiającą redukcję ilości danych przesyłanych w sieci
- Wsparcie dla urządzeń oferujących dodatkową deduplikację danych

Oprogramowanie musi pozwalać na następujące formy zarządzania:

- Być wyposażone w interfejs web do zarządzania wszystkimi aspektami związanymi z backupem i przywracaniem danych
- Umożliwiać wysyłanie powiadomień w formie email dotyczących wykonywanych zadań backupu, błędów, cyklicznych raportów oraz wiadomości email z załącznikami potwierdzającymi poprawność odtworzenia maszyn wirtualnych dla wybranych zadań w formie zrzutów ekranu z uruchomionej z backupu maszyny wirtualnej
- Zadanie backupu musi mieć możliwość uruchamiania zgodnie z harmonogramem, z opcją dodawania wielu harmonogramów dla pojedynczego zadania
- Pliki backupu muszą mieć możliwość eksportu z opcją wyboru rodzaju dysków do których będzie robiony eksport.
- Oprogramowanie musi pozwalać na eksportowanie oraz importowanie konfiguracji na cele reinstalacji czy migracji
- Oprogramowanie musi umożliwiać integrację z Active Directory

• Oprogramowanie musi wspierać tzw. tryb multi tenant, umożliwiający podzielenie oprogramowania do backupu na kilka podinstancji zarządzanych z odrębnych interfejsów w celu rozłożenia zarządzania w złożonych środowiskach

Wymagania dodatkowe

- Instalacja sprzętu/oprogramowania w miejscu wskazanym przez Zamawiającego.
- Uruchomienie, przetestowanie, parametryzację i wstępną konfigurację zgodnie z wytycznymi Zamawiającego
- Konfiguracja kopii zapasowych systemów wskazanych przez Zamawiającego oraz według ustalonego z Zamawiającym harmonogramu

2. Serwer oraz Serwer NAS na redundantny, odmiejscowiony Backup

Dostarczenie Serwera oraz Serwera NAS o minimalnych parametrach

Opis postępowania:
Przedmiotem zamówienia jest dostawa, instalacja, konfiguracja oraz uruchomienie przez Wykonawcę Serwera oraz Serwera NAS.

Wymagania minimalne:

Wymagania Serwer na redundantny, odizolowany Backup
Obudowa
Typu Rack, wysokość maksimum 2U; Dostarczona wraz z szynami umożliwiającymi pełne wysunięcie serwera z szafy rack Możliwość instalacji minimum 8 dysków 2.5” typu Hot-Plug.
Płyta główna
Wieloprocesorowa wyprodukowana i zaprojektowana przez producenta serwera, możliwość instalacji procesorów 28-rdzeniowych; Wyposażona w minimum 32 gniazda pamięci RAM DDR4, obsługa minimum 4TB pamięci RAM DDR4 3200 MHz. Możliwość rozbudowy do minimum 1024GB pamięci RAM bez konieczności wymiany zaoferowanych modułów DDR4; Obsługa pamięci nieulotnej instalowanej w gniazdach pamięci (przez pamięć nieulotną rozumie się moduły pamięci zachowujące swój stan np. w przypadku nagłej awarii zasilania, nie dopuszcza się podtrzymania bateryjnego stanu pamięci); Możliwość rozbudowy do minimum 3 złącz PCI Express generacji 4 x16. Mozliwość instalacji 2 slotów dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) nie zajmujące klatek dla dysków hot-plug; dyski M.2 muszą być chronione poziomem RAID1.
Procesory
Zainstalowany min. jeden procesor min 16-rdzeniowy, 32 wątkowy o minimalnym taktowaniu 2.4 GHz w architekturze x86 osiągający w testach wydajności cpubenchmark.net wynik minimum 30040.
Pamięć RAM
System posiada minimum 128 GB pamięci RAM typu DDR4 Registered, 3200 MHz Wsparcie dla technologii zabezpieczania pamięci ECC, Memory Mirroring, Memory Single Device Data Correction (SDDC), Failed DIMM Isolation, Memory Thermal Throttling, Command/Address Parity Check and Retry, Memory Demand/Patrol Scrubbing, Memory Data Scrambling, Memory Multi Rank Sparing

Kontrolery dyskowe, I/O
Zainstalowany dedykowany sprzętowy kontroler SAS 3.0 ze wsparciem dla poziomów RAID: 0, 1, 10
Dyski twarde
Dyski typu SSD o łącznej pojemności minimum 3,8 TB Dyski SAS 12Gb/s 7,2 tys o łącznej pojemności minimum 16 TB
Interfejsy sieciowe
System posiada min. 2 porty 10 Gigabit Ethernet optyczne z wkładkami SFP+ MM lub BaseT oraz min 2 porty 1 Gigabit Ethernet RJ45
Zasilanie, chłodzenie
Podwójny nadmiarowy zasilacz z możliwością wymiany bez wyłączania systemu (1+1), 600-900W
Zarządzanie
Wbudowany na froncie obudowy wyświetlacz informujący o stanie serwera w tym awarii: procesora, pamięci, temperaturze, zasilacza, wentylatora, płyty głównej, dysk - Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: • Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera; • Dedykowana karta LAN 1 Gb/s (dedykowane złącze RJ-45 z tyłu obudowy) do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; • Dostęp poprzez przeglądarkę Web (także SSL, SSH); • Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii; • Zarządzanie alarmami (zdarzenia poprzez SNMP); • Możliwość przejęcia konsoli tekstowej; • Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM); • Sprzętowy monitoring serwera w tym stanu dysków twardych i kontrolera RAID (bez pośrednictwa agentów systemowych); • Możliwość zapisu i przechowywania informacji i logów o pełnym stanie maszyny, w tym usterki i sytuacje krytyczne w obrębie wbudowanej pamięci karty zarządzającej - dostęp do tych informacji musi być niezależny od stanu włączenia serwera oraz stanu sprzętowego w tym np. usterki elementów poza kartą zarządzającą; • Możliwość zarządzania poprzez złącze microUSB zamontowane z przodu serwera
Wspierane OS
- Windows 2022 Hyper-V; - Windows 2019 Hyper-V; - Windows 2016 R2 Hyper-V; Potwierdzenie kompatybilności na stronie https://www.windowsservercatalog.com - VMWare; - SuSE; - RHEL.
Gwarancja
Minimum 3 lata gwarancji producenta serwera w trybie onsite z gwarantowanym czasem reakcji najpóźniej w następnym dniu roboczym od zgłoszenia usterki (tzw. NBD);
Dokumentacja, inne

Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001 (dokumenty załączyć do oferty); Serwer musi posiadać deklarację CE (dokument załączyć do oferty); Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA (wymagane oświadczenie producenta serwera potwierdzające spełnienie wymagań dołączone do oferty); Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w Polsce; Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera.

Wymagania dodatkowe

- Instalacja sprzętu/oprogramowania w miejscu wskazanym przez Zamawiającego.
- Uruchomienie, przetestowanie, parametryzację i wstępną konfigurację zgodnie z wytycznymi Zamawiającego

Wymagania Serwer NAS na redundantny, odizolowany Backup
Procesory
Minimum jeden procesor o minimum 2 rdzeniach
Pamięć RAM
Minimum 4 GB pamięci RAM DDR4
Rodzaje wyjść/wejść
USB 3.2 Gen. 1 – minimum 2 szt. RJ45 (LAN) 1 Gbps – minimum 2 szt. RJ45 (LAN) 10 Gbps – minimum 1 szt. eSATA – minimum 2 szt. DC-in (wejście zasilania) – minimum 1 szt. PCIe 3.0 x2 – minimum 1 szt.
Dyski twarde
Dołączone minimum 2 dyski o minimalnej pojemność każdego dysku 8 TB i prędkości minimum 7200obr. Dyski dedykowane do serwerów NAS. Technologia zapisu CMR Zwiększona odporność na drgania Zgodność z systemami NAS
Interfejsy sieciowe
RJ45 (LAN) 1 Gbps – minimum 2 szt.
Kieszenie na dyski
2,5"/3,5" – minimum 5 szt. (Hot swap) M.2 PCIe NVMe – minimum 2 szt.
Poziomy RAID
0 1 5 6 10 Basic JBOD
Protokoły sieciowe
AFP HTTP

HTTPS iSCSI Klient DHCP lub statyczny adres IP Klient VPN Serwer CIFS/SMB Serwer DLNA Serwer FTP NFS Serwer VPN SNMP WebDAV LDAP CalDAV
Gwarancja
36 miesięcy
System plików
EXT4 Btrfs
Dołączone akcesoria
Zasilacz Kabel sieciowy 2szt. Kabel zasilania 1szt.

Wymagania dodatkowe

- Instalacja sprzętu/oprogramowania w miejscu wskazanym przez Zamawiającego.
- Uruchomienie, przetestowanie, parametryzację i wstępną konfigurację zgodnie z wytycznymi Zamawiającego

3. System Zarządzania Tożsamością i Uprawnieniami

Wdrożenie centralnego systemu do zarządzania uprawnieniami użytkowników

Opis postępowania:
Przedmiotem zamówienia jest dostarczenie co najmniej 2 licencji Windows Serwer Standard 2019 lub 2022 16 CORE lub równoważnych. Licencja bezterminowa oraz 50 sztuk licencji dostępowych na urządzenie (Device CAL) do dostarczanego oprogramowania Windows Server lub równoważnego bez limitu liczby dostępów użytkowników.

Wymagania minimalne

W ramach wdrożenia Wykonawca:

- Utworzy i skonfiguruje 2 wirtualne maszyny z Windows Server 2022 lub 2019
- Zainstaluje i skonfiguruje rolę Active Directory i podniesie maszynę do kontrolera domeny
- Utworzy użytkowników na podstawie listy wskazanej przez Zamawiającego
- Utworzy i skonfiguruje serwer plików
    - przygotuje strukturę folderów
    - nada uprawnienia
- Skonfiguruje politykę haseł według wytycznych Zamawiającego
- Wdroży strukturę Grup Zabezpieczeń (Założenie grup oraz przypisanie im odpowiednich praw dostępu do zasobów sieciowych)
- Przypisze konta użytkowników do odpowiednich grup zabezpieczeń

- Skonfiguruje i wdroży Zasady Grupy GPO według wytycznych Zamawiającego. Automatyczna aktualizacja na stacjach roboczych
- Skonfiguruje wykonywanie raportów z serwera plików na temat zajętości katalogów oraz plików nieużywanych od danego momentu
- Przygotuje procedurę podłączania stacji roboczych do domeny wraz z opracowaniem metody automatyzującej ten proces
- Przeprowadzi Szkolenie dla 3 administratorów w siedzibie Zamawiającego

Przez oprogramowanie równoważne Zamawiający rozumie oprogramowanie spełniające następujące warunki poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

- Praca w roli serwera domeny Microsoft Active Directory.
- Zawarta możliwość uruchomienia roli serwera DHCP, w tym funkcji klastrowania serwera DHCP (możliwość uruchomienia dwóch serwerów DHCP operujących jednocześnie na tej samej puli oferowanych adresów IP).
- Zawarta możliwość uruchomienia roli serwera DNS.
- Zawarta możliwość uruchomienia roli klienta i serwera czasu (NTP).
- Zawarta możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
- Zawarta możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
- Zawarta możliwość uruchomienia roli serwera stron WWW.
- Zawarta możliwość implementacji nieograniczonej licencyjnie liczby maszyn wirtualnych opartych o usługę Hyper-V
- W ramach dostarczonej licencji zawarte prawo do instalacji i użytkowania systemu operacyjnego na co najmniej dwóch maszynach wirtualnych
- W ramach dostarczonej licencji zawarte prawo do pobierania poprawek systemu operacyjnego, minimalnie przez okres 5 lat bez dodatkowych kosztów, licząc od dnia zawarcia umowy dostawy.
- Oprogramowanie wydane minimum po 2017 roku.
- Warunki licencjonowania systemu operacyjnego muszą zezwalać na zmianę wersji systemu operacyjnego na niższą z zachowaniem wsparcia technicznego oraz na przeniesienie licencji systemu operacyjnego na inny fizyczny serwer.
- Liczba obsługiwanej pamięci RAM minimum 24 TB
- Licencja na system operacyjny umożliwia uruchomienie kontrolera domeny będącego w pełni zgodnym z domeną wdrożoną u Zamawiającego
- System posiada graficzny interfejs użytkownika
- Możliwość definiowania polityk bezpieczeństwa dla użytkowników, grup oraz stacji roboczych z systemami MS Windows 7, 8, 10
- System posiada wbudowaną obsługę zdalnego pulpitu zgodnie z protokołem RDP
- System posiada możliwość instalacji roli umożliwiającej konfigurację serwera aktualizacji dla stacji roboczych z systemami Windows 7, 8 , 10
- System operacyjny posiada obsługę deduplikacji na potrzeby systemu plików ReFS
- System operacyjny posiada możliwość uruchomienia serwera DNS z możliwością integracji z kontrolerem domeny

4. Szkolenie z Cyberbezpieczeństwa

Przeprowadzenie serii szkoleń dla pracowników szpitala z zakresu cyberbezpieczeństwa

Opis postępowania:

Przedmiotem zamówienia jest przeprowadzenie serii szkoleń dla pracowników Zamawiającego.

Wymagania minimalne

Celem szkolenia jest:

- poszerzenia praktycznej wiedzy z zakresu cyberbezpieczeństwa oraz podniesienie świadomości odnośnie bezpieczeństwa informatycznego
- przybliżenie uczestnikom, zagrożeń bezpieczeństwa informacji jak i sposobów obrony przed nimi

Zamawiający wymaga przeprowadzenia szkolenia dla wyznaczonych pracowników. Szkolenie powinno trwać 3 godziny lekcyjne dla jednej grupy szkoleniowej. Grupa szkoleniowa powinna liczyć maksymalnie 10 osób. Szkolenie będzie obejmować maksymalnie 30 osób oraz odbywać się po 2 lub 3 grupy w danym dniu roboczym do uzgodnienia z Zamawiającym.

Szkolenie, po uzgodnieniu terminu z Zamawiającym w drodze roboczej, powinno być przeprowadzone maksymalnie do końca października

Ramowy program szkolenia powinien obejmować następujące zagadnienia:

- Wprowadzenie do ustawy z dnia 05.07.2018 r. o krajowym systemie cyberbezpieczeństwa,
- Cyberzagrożenia i cyberprzestępczość,
- Obowiązki operatorów usług kluczowych,
- Jak przygotować instytucję na ataki hakerskie czy kradzież środków pieniężnych,
- Rozwiązania teleinformatyczne dla cyberbezpieczeństwa,
- rozpoznawać i zapobiegać zagrożeniom związanym z cyberprzestępczością,
- Zagrożenia bezpieczeństwa i klasyfikacja
- Rodzaje złośliwego oprogramowania
- Najpopularniejsze zagrożenia w ostatnim czasie
- Co to jest Ransomware i jak chronić się przed Ransomware
- Bezpieczne korzystanie z WWW i E-MAIL
- Bankowość i Płatności Online
- Prywatność w Internecie
- Bezpieczeństwo na portalach społecznościowych
- Szyfrowanie
- Zagrożenia mobilne
- Zarządzanie hasłami dostępowymi
- Ciemne zakątki Internetu
- Backup danych i bezpieczne usuwanie danych
- Fake News i jak go rozpoznać
- Dobre praktyki i zasady bezpiecznego używania komputerów

Wykonawca szkolenia powinien:

Zapewnić materiały dydaktyczne w formie papierowej lub elektronicznej dla każdego uczestnika.

Zapewnić realizację szkolenia w formie wykładu połączonego z warsztatami wykorzystującymi ćwiczenia indywidualne i grupowe, burzę mózgów, case studies, z zastosowaniem technik multimedialnych oraz dyskusję (część teoretyczna i praktyczna w proporcji 70/30),

Zapewnić osobę trenera lub trenerów, którzy posiadają adekwatne do tematu szkolenia wykształcenie zawodowe, wymaganą wiedzę i min. 5 -letnie doświadczenie w prowadzeniu szkoleń z zakresu opisywanej tematyki,

Posiadać certyfikaty minimum:

- SSCP System Security Certified Practitioner lub równoważny
- Information Security Management Systems (ISMS) Auditor/Lead Auditor (ISO/IEC 27001:2013 & EN IOS/IEC 27001:2017) lub równoważny

Przygotować listy obecności, zaświadczenia o ukończeniu szkolenia dla każdego uczestnika.

5. Przełączniki Sieciowe

Dostarczenie, konfiguracja i wdrożenie przełączników sieciowych w celu segmentacji sieci LAN Zamawiającego.

Opis postępowania:
Przedmiotem zamówienia jest dostawa, instalacja, konfiguracja oraz uruchomienie przez Wykonawcę przełączników sieciowych.

Wymagania minimalne

Wymagania przełączniki sieciowe do segmentacji sieci LAN
Interfejsy
Liczba portów LAN 10/100/1000 – minimum 24 szt. Liczba portów LAN 100/1000/10000 – minimum 2 szt. Lub Sloty SFP+ 10G – co najmniej 2 szt.
Dane Techniczne
Rozmiar tablicy adresów MAC minimum 16 tyś Prędkość magistrali wew. Minimum 128 Gb/s Switch Zarządzalny Warstwa przełączania L2
Zarządzanie i Administracja
IEEE 8021.Q VLAN (256 grup, statyczne) - Klasa usług IEEE 802.1p (CoS) - 8 kolejek sprzętowych (1 jest zarezerwowana dla CPU; 7 kolejek konfigurowalnych przez użytkownika) - QoS - Łącze statyczne lub dynamiczne IEEE 802.3ad Agregacja (LACP) - IEEE 802.1D Spanning Tree Protocol - IEEE 802.1w Rapid Spanning Tree Protokół - IEEE 802.1s Multiple Spanning Tree Protokół - SNMP v1, v2c, v3 - RFC 1213 - MIB II - RFC 1643 - baza MIB interfejsu Ethernet - Baza MIB mostka RFC 1493 - Klient DHCP RFC 2131 - IEEE 802.1x (RADIUS) - RADIUS accounting - Dynamiczna sieć VLAN IEEE 802.1x Zadania - HTTPS / SSL: bezpieczny GUI HTTP - Jakość usług (QoS) w warstwie 3 (DSCP) - TACACS + - Bezpieczeństwo portów przez filtr adresów MAC - Mapowanie priorytetów oparte na protokole TCP / UDP - IGMP snooping v1, v2, v3 - podsłuchiwanie MLD - Listy ACL (MAC, IPv4, IPv6 i TCP / UDP na podstawie) - Storm control for broadcast, multicast and unknown unicast packets

- Ograniczanie szybkości wejścia / wyjścia na portach - SNTP - DNS - Zapobieganie atakom DoS i Auto DoS - Zarządzanie IPv6, multiemisja i QoS - Routing statyczny - Snooping DHCP - Funkcje ekologiczne: • EEE (Energy Efficient Ethernet) spełnienie • Niższe zużycie energii podczas połączenie w dół lub w trybie bezczynności lub z krótsza długość kabla - Sieć VLAN oparta na protokołach i adresach MAC - grupa RMON 1, 2, 3, 9 - Private Enterprise MIB - Dublowanie portów - wiele do jednego - IEEE 802.3ab LLDP - LLDP-MED - Chronione porty - Test kabli - Wykrywanie Smart Control Center - Konfiguracja internetowa - Kopia zapasowa / przywracanie konfiguracji - Kontrola dostępu za pomocą hasła - Możliwość aktualizacji oprogramowania
Standardy
IEEE 802.1ab,IEEE 802.1D,IEEE 802.1p,IEEE 802.1Q,IEEE 802.1s,IEEE 802.1w,IEEE 802.3,IEEE 802.3ab,IEEE 802.3ad,IEEE 802.3ae,IEEE 802.3an,IEEE 802.3i,IEEE 802.3u,IEEE 802.3x,IEEE 802.3z
Gwarancja
Dożywotnia

Wymagania dodatkowe

- Instalacja sprzętu/oprogramowania w miejscu wskazanym przez Zamawiającego.
- Uruchomienie, przetestowanie, parametryzację i wstępną konfigurację zgodnie z wytycznymi Zamawiającego

6. Zapora Sieciowa UTM i System XDR

Dostarczenie, konfiguracja i wdrożenie Zapory Sieciowej UTM oraz Systemu XDR na Stacjach Roboczych oraz Serwerach

Opis postępowania:
Przedmiotem zamówienia jest dostarczenie oraz wdrożenie systemu ochrony sieci, a także stacji/serwerów Zamawiającego, zbudowany z urządzenia klasy UTM oraz rozwiązania ochrony stacji roboczych i serwerów dla: 60 stacji roboczych, 5 serwerów Windows oraz 5 serwerów Linux. Zaoferowane rozwiązania muszą spełniać wymagania Zamawiającego, przedstawione w tym dokumencie

Wymagania minimalne

Wymagania Urządzenia Klasy UTM
System

System ochrony sieci powinien zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym producenta rozwiązania.
Rozwiązanie powinno być wyposażone w moduł kryptoraficzny
Rozwiązanie powinno wspierać następujące tryby pracy: routing (warstwa 3), bridge (warstwa 2), hybrydowy (część jako router, część jako bridge)
Rozwiązanie powinno ofertować możliwość budowy klastra wysokiej dostępności pracującego trybie HA Active-Passive lub Active-Active.
System ochrony nie może posiadać ograniczeń co do ilości hostów w sieci chronionej.
Rozwiązanie powinno być wyposażone w dodatkowy procesor do akceleracji ruchu dla warstwy aplikacji.

Rozwiązanie musi być wyposażone w co najmniej jeden dysk SSD służący m.in. do przechowywania logów i raportów bezpośrednio na urządzeniu.
Urządzenie w metalowej obudowie o wysokości 1U z możliwością montażu w szafie rack 19"
Wbudowany port konsolowy zgodny z RS-232 (RJ-45 i/lub micro-USB).
Wbudowany port USB umożliwiający podłączenie modemów 3G/4G/LTE produkowanych przez firmy trzecie.
Wbudowany port USB umożliwiający podłączenie pamięci flash
Możliwość rozbudowy o dodatkowe moduły interfejsów sieciowych
Pamięć operacyjna RAM nie mniej niż (GB): 4
Przestrzeń do przechowywania logów i raportów nie mniej niż (GB) 64
Liczba fizycznych interfejsów 1000BASE-T nie mniej niż: 12
Liczba fizycznych interfejsów 1000BASE-X nie mniej niż: 2
Liczba wirtualnych interfejsów (VLAN) IEEE 802.1Q nie mniej niż: 128

Wydajność

Wydajność Firewall nie mniej niż (Gbps) 10
Wydajność Firewall IMIX nie mniej niż (Gbps) 4
Wydajność IPS nie mniej niż (Gbps) 2,5
Wydajność FW+IPS+AV nie mniej niż (Gbps) 0,8
Wydajność NGFW nie mniej niż (Gbps) 2,5
Liczba równoczesnych połączeń nie mniejsza niż: 5000000
Liczba nowych połączeń na sekundę nie mniejsza niż: 60000
Wydajność IPsec VPN nie mniej niż (Gbps): 4
Wydajność dla inspekcji ruchu SSL/TLS nie mniej niż (Gbps): 0,8
Liczba równoczesnych tuneli SSL VPN nie mniejsza niż: 500

Zarządzanie

Rozwiązanie powinno być zarządzanie przez webowy graficzny interfejs administratora (Web GUI) działający w czasie rzeczywistym.
Webowy graficzny interfejs administratora zabezpieczony protokołem HTTPS z certyfikatem self-signed z możliwością zmiany na podpisany przez zewnętrznego zaufanego wystawcę certyfikatów
Rozwiązanie powinno oferować mechanizm uwierzytelnianiania dwuskładnikowego w oparciu o token sprzętowy lub programowy dla zabezpieczenia dostępu do Web GUI jak i VPN.
Wbudowany webowy graficzny interfejs administratora powinien oferować narzędzia diagnostyczne takie jak co najmniej: ping, traceroute, name lookup, route lookup czy packet capture
Interfejs graficzny administratora powinien zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych, wyświetlania tablicy ARP
Rozwiązanie powinno oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych urządzenia na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.
System powinien oferować opcję automatycznego wylogowania sesji administratora po zdefiniowanym czasie bezczynności.
System powinien oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła.
System powinien oferować mechanizm blokady kolejnych połączeń w przypadku prób nieautoryzowanego dostępu do interfejsu do zarządzania. Liczba takich prób oraz czas blokady powinny być swobodnie definiowane przez administratora.

Rozwiązanie powinno posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego wraz z automatycznym procesem ich aplikowania (upgrade) i wycofywania (rollback).
System powinien oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników, klient, serwer z możliwością wykorzystania ich do budowy polityk bezpieczeństwa
System powinien oferować mechanizm pozwalający na śledzenie zmian w konfiguracji (tzw. changelog).

Rozwiązanie powinno zapewniać elastyczne zarządzanie dostępem do usług administracyjnych per strefa zapory sieciowej.
System powinien być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołu SMTPS (STARTTLS lub SSL/TLS).
Rozwiązanie powinno oferować monitorowanie stanu pracy w oparciu o protokoły SNMP v1, v2c i v3
System musi oferować wsparcie dla co najmniej Netflow v5 (lub jego odpwiednika).
System powinien zapewniać monitorowanie w czasie rzeczywistym stanu urządzenia (użycie CPU, RAM, HDD, obciążenie interfejsów sieciowych). Podobne statystyki powinny być dostępne również dla danych historycznych, z retencją do 12 miesięcy w ramach webowego interfejsu graficznego urządzenia.
Wymagane jest aby rozwiązanie oferowało wbudowany mechanizm do automatycznego tworzenia szyfrowanych hasłem kopii zapasowych konfiguracji z zapisem do pliku lokalnego, do serwera FTP, lub poprzez email
Rozwiązanie powinno oferować wbudowany mechanizm pozwalający na automatyczne tworzenie szyfrowanych hasłem kopii zapasowych konfiguracji w odstępach czasowych: codziennie, raz w tygodniu lub raz w miesiącu.
Rozwiązanie musi umożliwiać przechowywanie przynajmniej dwóch wersji oprogramowania systemowego (firmware). Informacja o dostępności nowej wersji powinna pojawiać się w Web GUI.
Producent powinien oferować mechanizm automatycznego łatania wykrytych w oprogramowaniu systemowym podatności przez tzw. hotfixies, przy czym administrator powinien móc funkcjonalność tą wyłączyć.
Rozwiązanie powinno oferować mechanizm szyfrowania danych takich jak loginy, hasła, klucze które przechowywane są w konifiguracji urządzenia
Rozwiązanie powinno zapewniać możliwość zmiany nazw interfejsów sieciowych.

Zapora sieciowa, konfiguracja sieciowa oraz routing

Zapora sieciowa

Wymagane jest aby zapora sieciowa działała w oparciu o mechanizm Stateful Packet Inspection.
System powinien umożliwiać budowanie niezależnych stosów reguł dla protokołów IPv4 oraz IPv6.
Rozwiązanie powinno umożliwiać budowanie polis w oparciu o takie obiekty jak sieć, usługa, użytkownik, grupa użytkowników lub czas.
System powinien umożliwiać budowanie polis bezpieczeństwa dla użytkowników i grup użytkowników w oparciu o definiowane przez administratora harmonogramy czasowe.
System powinien pozwalać na selektywne wyłączanie reguł zapory sieciowej (bez konieczności ich usuwania).
Rozwiązanie powinno zapewniać możliwość tworzenia polis w oparciu o relacje między strefami zapory sieciowej.
System ochrony powinien zawierać predefiniowane strefy zapory typu: LAN, WAN, DMZ, VPN.
Rozwiązanie powinno oferować możliwość definiowania własnych stref zapory sieciowej.
System powinien umożliwiać blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP).
System powinien pozwalać na filtrowanie widoku stosu reguł na bazie dowolnego ich składnika.

Pozostałe

Rozwiązanie powinno oferować możliwość łączenia interfejsów w warstwie L2 (bridge) wraz z STP oraz przekazywaniem ruchu rozgłoszeniowego ARP.
System powinien oferować funkcjonalność serwera DHCP dla IPv4 oraz IPv6 i DHCP Relay.
System powinien oferować wsparcie dla IEEE 802.1Q VLAN z możliwością konfiguracji niezależnych puli DHCP.
Rozwiązanie powinno oferować możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP).
Rozwiązanie powinno obsługiwać ramki Ethernet o rozmiarze 9000 bajtów (tzw. ramki jumbo).

Rozwiązanie powinno umożliwiać tworzenie interfejsów typu alias przypisanych do nadrzędnych interfejsów fizycznych.
Kontroler sieci bezprzewodowej
System powinien zapewniać obsługę punktów dostępowych sieci bezprzewodowej producenta rozwiązania. Wymagana jest obsługa punktów dostępowych sieci bezprzewodowej pracujących w trybach Access Point, Wireless Bridge oraz Wireless Repeater. Zarządzanie punktami dostępowymi sieci bezprzewodowej powinno odbywać się z poziomu webowego interfejsu graficznego rozwiązania oferując centralne monitorowanie i zarządzanie tak punktami dostępowymi jak klientami sieci bezprzewodowej. Rozgłaszane sieci bezprzewodowe powinny być powiązane z siecią lokalną, siecią VLAN lub dedykowaną strefą zapory zachowując przy tym możliwość izolacji klientów sieci bezprzewodowej. Rozwiązanie powinno umożliwiać rozgłaszanie wielu SSID w możliwością wyłączenia rozgłaszania identyfikatorów sieci bezprzewodowej (Hide SSID). Rozwiązanie powinno oferować wsparcie dla WPA2 Personal oraz WPA2 Enterprise. Rozwiązanie powinno zapewniać wsparcie dla uwierzytelniania klientów w oparciu o IEEE 802.1X (RADIUS Authentication). System powinien umożliwiać tworzenie hot spotów z możliwością definiowania własnych voucherów. Dostęp do sieci bezprzewodowej powinien być możliwy po zaakceptowaniu warunków, wprowadzeniu hasła dnia, kodu z vouchera lub po autoryzacji z użyciem nazwy użytkownika oraz hasła dla gości. System powinien pozwalać na rozgłaszanie sieci bezprzedowodych w oparciu o harmonogramy czasowe. Rozwiązanie powinno zawierać działający w tle mechanizm cyklicznego automatycznego doboru kanałów sieci bezprzewodowej oraz wykrywania wrogich punktów dostępowych (Rogue AP detection). Jeżeli funkcjonalność Kontrolera sieci bezprzewodowej jest licencjonowana, Zamawiający nie wymaga dostarczenia tej licencji w ramach przedmiotowego postępowania
Uwierzytelnianie i obsługa użytkowników
Wymagane uwierzytelniaine użytkowników w trybach Transparent Proxy Authentication (NTLM/Kerberos), SSO (Single Sign On) lub przy użyciu agenta. Rozwiązanie powinno być wyposażone w lokalną bazę użytkowników. System powinien zapewniać możliwość uwierzytelniania w oparciu o takie usługi jak Active Directory, RADIUS, LDAP Rozwiązanie powinno umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory System powinien oferować możliwość uwierzytelniania użytkowników za pośrednictwem agenta dostępnego dla platform Windows, Mac OS X, Linux, iOS, Android. Rozwiązanie powinno oferować Captive Portal i wykorzystywać go jako podstawowy mechanizm uwierzytelniania użytkowników w sieci. Rozwiązanie powinno umożlwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik instalacyjny agenta do uwierzytelniania. Rozwiązanie powinno umożlwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik z konfiguracją klienta SSL VPN dla Windows Mac OS, Linux, iOS, Android.
Koncentrator VPN
System musi umożliwiać konfigurację połączeń typu IPsec site-to-site VPN dla IKE v1 oraz IKE v2. System musi obsługiwać połączenia IPsec szyfrowane przy użyciu AES256 z SHA512 wraz z grupami kluczy Diffie-Hellman: 19 (ecp256), 21 (ecp521) czy 31 (curve25519). System musi obsługiwac połączenia IPsec site-to-site VPN jak i IPsec client-to-site VPN oraz SSL client-to-site VPN. Rozwiązanie musi oferować mechanizmy monitorujące i utrzymujące stan aktywności tuneli IPsec site-to-site VPN. Rozwiązanie musi oferować mechanizmy IPsec VPN Failover i Failback. Producent musi dostarczać bezpłatnie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPsec client-to-site VPN jak i SSL client-to-site VPN.
Logowanie i raportowanie
System musi możliwiać monitorowanie logów ruchu w czasie rzeczywistym.

System powinien umożliwiać składowanie oraz archiwizację logów.
Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
Rozwiązanie musi zapewniać narzędzie do graficznej analizy logów.
Rozwiązanie musi udostępniać narzędzie analizy incydentów bezpieczeństwa
System powinien zapewniać monitoring ryzyka związanego z działaniem aplikacji sieciowych uruchamianych przez użytkowników np. klasyfikując ryzyko wg. skali.
System powinien zapewniać przeglądanie logów przy zastosowaniu funkcji filtrujących.
Rozwiązanie powinno umożliwiać wysyłanie raportów poprzez email.
Rozwiązanie powinno umożliwiać eksport raportów do plików PDF, HTML i CSV.
System powinien zapewniać podgląd wykorzystania łącza internetowego w ujęciu dziennym, tygodniowym, miesięcznym lub rocznym dla wszystkich lub indywidualnego łącza.
System powinien zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP lub aplikację.
System powinien umożliwiać automatyczne tworzenie raportów według kryteriów i harmonogramów określonych przez administratora.

Ochrona przez Malware

Rozwiązanie powinno działać jako Transparent Web Proxy zapewniając ochronę przed niebezpiecznymi treściami i szkodliwym oprogramowaniem dystrybuowanym przez HTTP, HTTPS i FTP.
Rozwiążanie powinno wykorzystywać silnik antywirusowy pochodzący bezpośrednio od producenta rozwiązania.
Wymagane jest aby system automatycznie aktualizował sygnatury zagrożeń.
System powinien filtrować pliki na podstawie tak rozszerzeń jak i nagłówków MIME.
Rozwiązanie musi przeprowadzać emulację skryptów Java.

Filtr Web

Rozwiązanie powinno zawierać przynajmniej 90 kategorii stron Web oraz umożliwiać dodawanie własnych kategorii stron.
Rozwiązanie powinno umożliwiać tworzenie granularnych polityk i wyjątków filtra Web z uwzględnieniem takich kryteriów jak co najmniej: użytkownik lub grupa użytkowników, kategoria stron czy harmonogram czasowy.
Polityki filtrujące ruch Web powinny umożliwiać wybór akcji co najmniej: zablokuj, ostrzeż, zezwól.
System powinien wyświetlać komunikat o przyczynie zablokowania dostępu do strony Web. Administrator powinien mieć możliwość modyfikowamoa treści komunikatu w tym dodania logo organizacji.
Rozwiązanie powinno umożliwiać filtrowanie stron web analzując ich zawartość wykorzystując tzw. Content Filtering na bazie haseł kluczowych.

Ochrona przed nieznanymi zagrożeniami

Rozwiązanie klasy Sandbox do ochrony przez zadrożeniami typu Zero-Day.
Rozwiązanie oferujące statyczną i dynamiczną analizę kodu przesyłanego w ramach ruchu web czy email.

Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików wykonywalnych w tym .exe, .com, .dll.

Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików dokumentów w tym .doc, .docx, .docm, .rtf.
Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików .pdf.
Rozwiązanie umożliwiające dodatkową inspekcję i detoancję archiwów w tym .zip, .bzip, .gzip, .rar, .tar, .lha, .lhz, .7z, .cab.
System zapewniający analizę pamięci, ruchu sieciowego, operacji na dysku, operacji w rejestrze systemowym po detonacji kodu.
System zapewniający analizę strukury kodu w tym analizę przeprowadzaną przez mechanizmy głębokiego uczenia maszynowego.
System powinien oferować szczegółowe raporty dowodzące przeprowadznie analizy dla w/w mechanizmów.

WYMAGANIA SYSTEMU OCHRONY STACJI ROBOCZYCH ORAZ SERWERÓW WINDOWS/LINUX

Administracja zdalna
Rozwiązanie Centralnej administracji musi wspierać instalację na systemach Windows Server, Linux lub być dostępne jako chmurowa usługa producenta Rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL. Rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi modułami. Rozwiązanie musi zapewniać centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, antyspyware, antyransomware, exploit protection, IPS które działają na stacjach roboczych w sieci. Rozwiązanie musi zapewniać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. Rozwiązanie musi zapewniać korzystanie z szablonów raportów, przygotowanych przez producenta. Rozwiązanie musi zapewniać podział uprawnień administracyjnych. Maszyny z systemami Windows, Mac i Linux muszą być zarządzane z jednej konsoli zarządzania. Musi mieć możliwość na synchronizację użytkowników/grup/komputerów z lokalnych serwerów Active Directory w celu zarządzania politykami. Tworzone polityki powinny mieć możliwość zastosowania do użytkowników lub urządzeń. Aktualizacja punktów końcowych powinna mieć możliwość ustawienia przepustowości używanej zarówno do aktualizacji oprogramowania, jak i aktualizacji definicji zagrożeń
Ochrona stacji roboczych
Rozwiązanie musi wspierać systemy operacyjne Windowds Rozwiązanie musi zapewniać wykrywanie i usuwanie znanego, jak i niespotykanemu wcześniej złośliwemu oprogramowaniu, podobnie musi być w stanie blokować złośliwe oprogramowanie przed jego uruchomieniem. Rozwiązanie musi klasyfikować pliki jako złośliwe, potencjalnie niechciane aplikacje (PUA) lub niegroźne. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. Rozwiązanie musi zapewniać wykonywanie skanowania zagrożeń Dni Zero (0 day) w trybie offline (bez dostępu do Internetu). Rozwiązanie musi chronić system nawet w trybie offline i nie będzie polegać na sygnaturach. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych. Rozwiązanie musi mieć możliwość wywołania czyszczenia stacji po każdym aktywnym wykryciu exploita lub ransomware w oparciu o pliki i procesy Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie sumy kontrolnej (SHA1) oraz lokalizacji. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów minimum HTTPS bez konieczności dystrybuowania certyfikatów. Rozwiązanie musi posiadać wbudowany moduł zapobieganie/ograniczania luk w zabezpieczeniach minimum w oparciu o ochrona wykonywania danych (DEP), randomizację układu przestrzeni adresowej (ASLR), Strukturalna ochrona przed nadpisaniem obsługi wyjątków (SEHOP), DLL Hijacking, Reflective DLL Injection, Stack Pivot, Dynamic Shellcode Rozwiązanie musi zapewniać ochronę przed atakami przepełnienia bufora Rozwiązanie musi być w stanie skanować ruch w oparciu o inspekcję pakietów (IPS) na najniższym poziomie i blokować zagrożenia przed uszkodzeniem systemu operacyjnego lub aplikacji. Rozwiązanie musi mieć możliwość przywrócenia zaszyfrowanych plików do stanu sprzed zaszyfrowania i przywróci je do ich pierwotnej lokalizacji. Rozwiązanie musi zapewnić wykrywanie komunikacji między komputerami końcowymi a serwerami dowodzenia i kontroli biorącymi udział w atakach botnetowych lub innych złośliwych programach. Rozwiązanie musi umożliwiać zarówno ochrona Anti-Exploit, jak i Ransomware bez konieczności łączenia z zewnętrzną usługa „Sandboxing” Rozwiązanie musi chronić przed złośliwym kodem (na przykład skryptami PowerShell) za pomocą interfejsu Microsoft Antimalware Scan Interface (AMSI). Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, urządzeń Bluetooth, modemów,.

Rozwiązanie musi być w stanie wykrywać i blokować kategorie aplikacji, które mogą nie być odpowiednie do użytku w środowisku przedsiębiorstw
Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych tzw. URL Filtering.
Rozwiązanie musi być w stanie monitorować i konfigurować Zaporę systemu Windows na zarządzanych komputerach i serwerach przy użyciu zasad Zapory systemu Windows.
Rozwiązanie musi mieć opcję generowania migawki kryminalistycznej złośliwej aktywności, która wystąpiła na chronionym punkcie końcowym.
Rozwiązanie musi posiadać opcję „automatycznego izolowania" skompromitowanych punktów końcowych od sieci.
Rozwiązanie musi mieć możliwość monitorowania lub zatrzymywania lokalnych użytkowników administracyjnych lub złośliwych procesów w celu wyłączenia ochrony punktu końcowego:

a. Zatrzymywanie usług z interfejsu usług
b. Zabicia usługi i procesu z interfejsu Menedżera zadań
c. Zmianę konfigurację usługi w interfejsie usług
d. Odinstalowania
e. Usunięcia lub modyfikacji chronionych plików lub folderów
f. Usunięcia lub modyfikacji chronionych kluczy rejestru

Rozwiązanie musi mieć możliwość zidentyfikowania, co się stało, skąd pochodziło naruszenie, jakie pliki zostały naruszone, oraz dostarczać wskazówek, jak wzmocnić postawę bezpieczeństwa organizacji
Rozwiązanie musi zapewniać widok wszystkiego, co miało wpływ na atak. Pozycje można filtrować według typu. np. pliki, procesy, klucze rejestru. Administrator może przeglądać informacje o każdej pozycji m.in. Nazwa pliku (plik ofiary lub agent złośliwego oprogramowania), identyfikator procesu, znacznik czasu rozpoczęcia/zatrzymania zdarzenia.
Rozwiązanie musi zapewniać opcję wysłania podejrzanych plików do zewnętrznych mechanizmów producenta w celu dalszej analizy.

Ochrona Serwerów Windows

Rozwiązanie musi wspierać systemy operacyjne Windows Server2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server2016, Windows Server2019, Windows Server2022.
Rozwiązanie musi zapewniać wykrywanie i usuwanie znanego, jak i niespotykanemu wcześniej złośliwemu oprogramowaniu, podobnie musi być w stanie blokować złośliwe oprogramowanie przed jego uruchomieniem.
Rozwiązanie musi klasyfikować pliki jako złośliwe, potencjalnie niechciane aplikacje (PUA) lub niegroźne.
Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
Rozwiązanie musi zapewniać wykonywanie skanowania zagrożeń Dni Zero (0 day) w trybie offline (bez dostępu do Internetu).
Rozwiązanie musi chronić system nawet w trybie offline i nie będzie polegać na sygnaturach.
Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych.
Rozwiązanie musi mieć możliwość wywołania czyszczenia stacji po każdym aktywnym wykryciu exploita lub ransomware w oparciu o pliki i procesy
Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie sumy kontrolnej (SHA1) oraz lokalizacji.
Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów minimum HTTPS bez konieczności dystrybuowania certyfikatów.
Rozwiązanie musi posiadać wbudowany moduł zapobieganie/ograniczania luk w zabezpieczeniach minimum w oparciu o ochrona wykonywania danych (DEP), randomizację układu przestrzeni adresowej (ASLR), Strukturalna ochrona przed nadpisaniem obsługi wyjątków (SEHOP), DLL Hijacking, Reflective DLL Injection, Stack Pivot, Dynamic Shellcode
Rozwiązanie musi zapewniać ochronę przed atakami przepełnienia bufora
Rozwiązanie musi być w stanie skanować ruch w oparciu o inspekcję pakietów (IPS) na najniższym poziomie i blokować zagrożenia przed uszkodzeniem systemu operacyjnego lub aplikacji.
Rozwiązanie musi mieć możliwość przywrócenia zaszyfrowanych plików do stanu sprzed zaszyfrowania i przywróci je do ich pierwotnej lokalizacji.

Rozwiązanie musi zapewnić wykrywanie komunikacji między komputerami końcowymi a serwerami dowodzenia i kontroli biorącymi udział w atakach botnetowych lub innych złośliwych programach.
Rozwiązanie musi umożliwiać zarówno ochrona Anti-Exploit, jak i Ransomware bez konieczności łączenia z zewnętrzną usługa „Sandboxing"
Rozwiązanie musi być chronić przed złośliwym kodem (na przykład skryptami PowerShell) za pomocą interfejsu Microsoft Antimalware Scan Interface (AMSI).
Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, urządzeń Bluetooth, modemów,.
Rozwiązanie musi być w stanie wykrywać i blokować kategorie aplikacji, które mogą nie być odpowiednie do użytku w środowisku przedsiębiorstw
Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych tzw. URL Filtering.
Rozwiązanie musi być w stanie monitorować i konfigurować Zaporę systemu Windows na zarządzanych komputerach i serwerach przy użyciu zasad Zapory systemu Windows.
Rozwiązanie musi mieć opcję generowania migawki kryminalistycznej złośliwej aktywności, która wystąpiła na chronionym punkcie końcowym.
Rozwiązanie musi posiadać opcję „automatycznego izolowania" skompromitowanych punktów końcowych od sieci.
Rozwiązanie musi mieć możliwość monitorowania lub zatrzymywania lokalnych użytkowników administracyjnych lub złośliwych procesów w celu wyłączenia ochrony punktu końcowego:

a. Zatrzymywanie usług z interfejsu usług
b. Zabicia usługi i procesu z interfejsu Menedżera zadań
c. Zmianę konfigurację usługi w interfejsie usług
d. Odinstalowania
e. Usunięcia lub modyfikacji chronionych plików lub folderów
f. Usunięcia lub modyfikacji chronionych kluczy rejestru

Rozwiązanie musi mieć możliwość zidentyfikowania, co się stało, skąd pochodziło naruszenie, jakie pliki zostały naruszone, oraz dostarczać wskazówek, jak wzmocnić postawę bezpieczeństwa organizacji
Rozwiązanie musi zapewniać widok wszystkiego, co miało wpływ na atak. Pozycje można filtrować według typu. np. pliki, procesy, klucze rejestru. Administrator może przeglądać informacje o każdej pozycji m.in. Nazwa pliku (plik ofiary lub agent złośliwego oprogramowania), identyfikator procesu, znacznik czasu rozpoczęcia/zatrzymania zdarzenia.
Rozwiązanie musi zapewniać opcję wysłania podejrzanych plików do zewnętrznych mechanizmów producenta w celu dalszej analizy.

Ochrona Serwerów Linux

Rozwiązanie musi wspierać systemy operacyjne w oparciu o architekturę x64, kernel wspierający minimum glibc 2.7 z działająca usługą systemd z zainstalownaym Bash
Rozwiązanie musi wykrywać wykorzystywanie luk w aplikacjach Linux, w tym uszkodzenia pamięci, nietypowe zachowanie aplikacji i ucieczki z kontenerów.
Rozwiązanie musi wykrywać wykorzystywanie luk w podstawowym systemie Linux, takich jak eskalacja uprawnień, manipulowanie mechanizmami bezpieczeństwa (np. SELinux), korzystanie z popularnych metod eksploatacji jądra i ucieczki z kontenerów.
Rozwiązanie musi wykrywać utrzymanie dostępu przez ponowne uruchomienie hosta, w tym backdoory jądra lub backdoory w przestrzeni użytkownika
Rozwiązanie musi wykrywać zmiany w systemowych plikach binarnych, zmiany konfiguracji, usuwanie plików i tworzenie nietypowych plików.
Rozwiązanie musi wykrywać tzw. ruch boczny, zachowanie usług sieciowych i podsłuchiwanie sieci.
Rozwiązanie musi wykrywać nieprawidłowe wykonanie procesu, użycie kompilatora, debugowanie, zaplanowane zmiany zadań.
Rozwiązanie musi wykrywać uprzywilejowane użycie poleceń, ryzykowne działania programistów i zmiany kont użytkowników.

Endpoint Detection and Response

Rozwiązanie musi posiadać moduł EDR dla systemów Windows, MacOS, Linux współpracujący z systemem do ochrony stacji roboczych i serwerów tego samego producenta.

Rozwiązanie musi mieć możliwość późniejszego rozszerzenia moduły EDR o logi pochodzące z platform Android, iOS tego samego producenta
Rozwiązanie musi pozwolić administratorom odszukać informację dotyczące incydentów związanych z bezpieczeństwem, zapewniając wgląd w zakres ataku, sposób jego rozpoczęcia, wpływ i sposób reagowania.
Rozwiązanie musi mieć możliwość uruchamiania zapytań zabezpieczających na wszystkich zarządzanych urządzeniach, nawet jeśli są one offline.
Rozwiązanie musi mieć opcję „ręcznego izolowania" chronionych punktów końcowych od sieci podczas badania przypadku zagrożenia.
Rozwiązanie musi zapewnić interfejs wiersza poleceń umożliwiający zdalny dostęp do urządzeń w celu przeprowadzenia dalszego dochodzenia lub podjęcia odpowiednich działań. Opcja dostępu zdalnego musi być dostępna tylko dla kont administratorów korzystających z uwierzytelniania wieloskładnikowego (MFA). Zdalny dostęp musi być realizowany dla systemów operacyjnych takich jak Windows, Mac i Linux a aktywności zapisane w logach audytowych.
Rozwiązanie musi umożliwiać wyszukiwanie szczegółów dotyczących wykonanych poleceń w PowerShell
Rozwiązanie musi zapewniać detekcję w oparciu o Mitre ATT&CK Tactic and Technique
Rozwiązanie musi pozwalać na wysyłanie powiadomień do administratora w chwili utworzenia nowego dochodzenia

Wymagania dotyczące wdrożenia

- W celu zwiększenia integracji urządzenia UTM z systemem ochrony stacji/serwerów wymagane jest, aby oba te rozwiązania pochodziły od jednego producenta, zapewniając komunikację pomiędy nimi.
- Wniesienie, ustawienie, podłączenie wszystkich dostarczonych urządzeń w miejscach wskazanych przez Zamawiającego
- 3-letnia gwarancja producenta lub autoryzowanego partnera producenta w miejscu instalacji. Zgłoszenia przyjmowane w trybie 8x5, czas reakcji w następnym dniu roboczym od zgłoszenia.
- W okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z urządzeniem UTM oraz oprogramowania wewnętrznego urządzenia, sygnatur bazy systemu kontroli przed włamaniami (IDS/IPS) i systemu antywirusowego.
- W okresie gwarancji Zamawiający ma prawo do korzystania z systemu ochrony stacji roboczych/serwerów
- Rozwiązania muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego urządzenia, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta.
- Przeniesienie konfiguracji z poprzedniego UTM na nowego UTM. Przeniesienie konfiguracji powinno obejmować całą konfigurację sieci LAN, VPN, Polityk Bezpieczeństwa, Obiektów L3 i L2, Reguł firewall,
- Wdrożenie Systemu XDR na wszystkich Stacjach wskazanych przez Zamawiającego
- Wdrożenie centralnej konsoli do zarządzania UTM i XDR z poziomu jednego panelu administracyjnego
- Urządzenia i licencje powinny zostać dostarczone z licencjami na okres 36 miesięcy.
- Przeprowadzenie w siedzibie Zamawiającego szkolenia dla minimum 3 pracowników
- Prace wdrożeniowe nie mogą spowodować wyłączenia dostępu do sieci w czasie od poniedziałku o piątku w godzinach od 7:00 do 16:00
- Urządzenie musi być dostarczone w stanie fabrycznie nowym, wolnym od wad technicznych, prawnych i formalnych zwłaszcza w zakresie licencji i uprawnień do aktualizacji oprogramowania. Sprzęt nie może być wcześniej zarejestrowany na żadnego innego klienta w bazie klientów producenta sprzętu
- Zamawiający wymaga przed podpisaniem protokołu odbioru sprzętu zażądać oświadczenia producenta na podstawie numerów seryjnych, że oferowany sprzęt jest nowy i pochodzi z legalnego kanału dystrybucyjnego producenta. Jeśli sprzęt nie spełnia tych warunków Zamawiający odstąpi od umowy z winy Oferenta

7. Oprogramowanie do monitorowania systemów klasy HIS

Dostarczenie, konfiguracja i wdrożenie dedykowanego oprogramowania do monitorowania systemu klasy HIS posiadanego przez Zamawiającego

Opis postępowania:
Przedmiotem zamówienia jest dostawa, instalacja, konfiguracja oraz uruchomienie przez Wykonawcę dedykowanego oprogramowania do monitorowania systemu klasy HIS posiadanego przez Zamawiającego.

Wymagania minimalne

Wymagania oprogramowania do monitorowania systemu klasy HIS
Dostarczone oprogramowanie musi być autoryzowanym oprogramowaniem przez producenta oprogramowania HIS, które posiada Zamawiający
Funkcja rejestrowania
• centralna i automatyczna rejestracja zdarzeń serwerów aplikacyjnych i bazodanowych, • centralna i automatyczna rejestracja plików logowania serwerów aplikacyjnych i bazodanowych • centralna i automatyczna rejestracja zdarzeń występujących w systemach operacyjnych • centralna i automatyczna rejestracja wybranych zdarzeń w systemach dziedzinowych uruchomionych na serwerach aplikacyjnych • automatyczna rejestracja zdarzeń w trybie 24/7/365 • ustawienie czasu retencji przechowywanych danych historycznych
Funkcja przeglądania
• przegląd danych za pomocą centralnej konsoli dostępnej z przeglądarek internetowych, • przegląd danych za pomocą typów wykresów: słupkowy, kołowy, wykres w czasie, tabela, zegarowy, histogram • przegląd danych historycznych • przegląd w czasie rzeczywistym wskazanych zdarzeń reprezentujących stan środowiska systemowego, aplikacyjnego i bazodanowego, • przegląd w czasie rzeczywistym wybranych zdarzeń w systemach uruchomionych na serwerach aplikacyjnych
Funkcja powiadamiania
• natychmiastowa wysyłka powiadomień o ostrzeżeniach i awariach • przekazywanie powiadomień w zależności od przyjętych wartości krytycznych dla zdarzeń • przekazywanie powiadomień za pomocą poczty elektronicznej • przekazywanie powiadomień za pomocą komunikatora działającego na platformie mobilnej

Wymagania dodatkowe

- Instalacja sprzętu/oprogramowania w miejscu wskazanym przez Zamawiającego.
- Uruchomienie, przetestowanie, parametryzację i wstępną konfigurację zgodnie z wytycznymi Zamawiającego

8. Oprogramowanie do monitorowania, gromadzeni, analizy zdarzeń

Opracowanie i wdrożenie systemu do monitorowania, gromadzenia, analizy i korelacji zdarzeń oraz automatycznego wykrywania incydentów

Opis postępowania:
Przedmiotem zamówienia jest dostawa, instalacja, konfiguracja oraz uruchomienie przez Wykonawcę systemu bezpieczeństwa do gromadzenia, analizy i korelacji i agregacji zdarzeń/logów oraz automatycznego wykrywania incydentów.

W ramach wdrożenia Wykonawca wykona:

1. Prace organizacyjne, analityczno koncepcyjne - wykona analizę monitorowanego środowiska
2. Instalację oprogramowania, dokona jego koniecznej parametryzacji, konfiguracji lub innych zmian w celu spełnienia wymagań zamówienia i zapewnienia poprawnego działania Systemu
3. Uruchomi, skonfiguruje, przetestuje System zgodnie z wytycznymi Zamawiającego
4. Skonfiguruje System żeby pobierał logi z urządzeń, serwerów wskazanych przez Zamawiającego
5. Opracuje dokumentację powdrożeniową która powinna uwzględniać część opisową, schematy logiczne oraz schematy połączeń infrastruktury
6. Zapewni wsparcie dla wdrożonego Systemu do końca listopada 2022 roku

Wymagania minimalne:

System nie może posiadać ograniczeń w postaci ilości urządzeń z których pobierane są logi.
System musi przechowywać logi minimum przez okres 1 roku
System musi umożliwiać integrację danych gromadzonych z różnych źródeł: aplikacji, baz użytkowników, w tym katalogu Active Directory. Dane powinny być dostępne jako spójna informacja na poziomie interfejsu analitycznego systemu
Umożliwiać odbieranie danych w formatach: • Syslog (TCP, UDP, AMQP, Kafka), • GELF (TCP, UDP, AMQP, Kafka, HTTP), • AWS – AWS Logs, FlowLogs, CloudTrail, • Beats/Logstash, • CEF (TCP, UDP, AMQP, Kafka), • JSON Path from HTTP API, • Netflow (UDP), • Plain/Raw Text (TCP, UDP, AMQP, Kafka).
Umożliwiać archiwizację danych
Umożliwiać generowanie raportów
Umożliwiać monitorowanie serwerów fizycznych i wirtualnych
Umożliwiać monitorowanie urządzeń sieciowych
Umożliwiać monitorowanie stanu połączeń VPN
Umożliwiać monitorowanie maszyn wirtualnych pracujących pod kontrolą Windows i Linux
Umożliwiać monitorowanie interfejsów sieciowych przełączników, routerów, serwerów
Umożliwiać powiadamianie użytkownika o problemach przez E-mail
Umożliwiać prezentację danych na dashboardach
Umożliwiać monitorowanie Active Directory
Umożliwiać monitorowanie serwerów za pomocą agentów
Umożliwiać monitorowanie serwerów aplikacji Tomcat, Oracle WebLogic Server, Oracle Application Server
Umożliwiać monitorowanie baz danych: • ORACLE • MySQL • Postgress
Umożliwiać agregację logów z innych systemów
Umożliwiać wysyłanie logów poprzez Syslog
Umożliwiać wysyłanie logów poprzez GELF poprzez http API

9. Opracowania podstawowego pakietu dokumentów z zakresu bezpieczeństwa systemów informatycznych

Opracowania podstawowego pakietu dokumentów z zakresu bezpieczeństwa systemów informatycznych w oparciu o normę PN ISO/IEC 27001 (SZBI) zgodnie z wymaganiami normy PN ISO/IEC 22301

Opis postępowania:
Przedmiotem zamówienia jest opracowanie podstawowego pakietu dokumentów z zakresu bezpieczeństwa systemów informatycznych w oparciu o normę PN ISO/IEC 27001 (SZBI) i Ciągłości Działania (BCM/BCP) zgodnie z wymaganiami normy PN ISO/IEC 22301

Zakres dokumentacji

Aktualizacja i uzupełnienia posiadanej dokumentacji KRI o wymagania systemowe SZBI zgodnie z normą ISO 27001 i ISO 22301 wymagające wspólnego opisu do procesu bezpieczeństwa

a) Określenie i sformalizowanie zasad zarządzania w szczególności poprzez wskazanie osób odpowiedzialnych oraz wskazanie podejścia do zapewnienia zasobów niezbędnych do efektywnego zarządzania bezpieczeństwem i zarządzania usługami.
b) Opracowanie procedur przeprowadzania audytów, zawierających wskazanie częstotliwości audytów, sposobu przygotowywania i zatwierdzania ich planów, sposobu ich przeprowadzania oraz dokumentowania i raportowania ich wyników.
c) Opracowanie procedury działań korygujących w przypadku niezgodności z wymaganiami systemu zarządzania.
d) Opracowanie procedury wprowadzania działań zapobiegawczych w przypadku wystąpienia sytuacji mogącej prowadzić do niezgodności z wymaganiami systemu zarządzania.
e) Opracowanie procedury przeglądu systemu zarządzania, w szczególności określającej częstotliwość przeglądów, zakres i sposób ich przeprowadzania, materiały źródłowe niezbędne do przeprowadzenia przeglądu, tryb wdrażania wniosków.
f) Opracowanie procedury nadzoru nad dokumentami wchodzącymi w skład systemu zarządzania w tym zasady/zapisy/wymagania wersjonowania, zatwierdzania, dystrybucji, przechowywania, archiwizowania i niszczenia dokumentów.
g) Opracowanie procedury nadzoru nad zapisami, określającej zasady/zapisy/wymagania przechowywania, archiwizowania oraz niszczenia zapisów.

2. Aktualizacja i uzupełnienia posiadanej dokumentacji KRI o wymagania i zasady spełnienia 114 zabezpieczeń opisanych Załącznikiem A normy ISO 27001.