Znak sprawy: IR 271.2.3.2024 **Załącznik 1 do OPZ**

Wymagania na dostawę i instalację Firewall -a

Do obowiązków Wykonawcy w ramach niniejszego zadania należy dostawa urządzeń zabezpieczających styk z Internetem do siedziby Zamawiającego, spełniającego minimalne wymagania techniczne i funkcjonalne określone poniżej oraz jego instalacja i konfiguracja.

1. Wymagania Ogólne
   - 1.1. System realizuje wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza.
   - 1.2. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. Dla wszystkich funkcji systemu musi być dostarczony dokument potwierdzony przez producenta lub autoryzowanego dystrybutora o gotowości świadczenia usług wsparcia w języku polskim oraz bezpłatnej obsługi procesu wymiany uszkodzonego urządzenia.
   - 1.3. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów:
     - 1.3.1. Routera z funkcją NAT,
     - 1.3.2. Transparentnym,
     - 1.3.3. monitorowania na porcie SPAN.
   - 1.4. System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie:
     - 1.4.1. Routingu,
     - 1.4.2. Firewall'a,
     - 1.4.3. IPSec VPN,
     - 1.4.4. Antywirus,
     - 1.4.5. IPS,
     - 1.4.6. Kontroli Aplikacji.
   - 1.5. Możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.
   - 1.6. System wspiera protokoły IPv4 oraz IPv6 w zakresie:
     - 1.6.1. Firewall.
     - 1.6.2. Ochrony w warstwie aplikacji.
     - 1.6.3. Protokołów routingu dynamicznego.
2. Redundancja, monitoring i wykrywanie awarii
   - 2.1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
   - 2.2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
   - 2.3. Monitoring stanu realizowanych połączeń VPN.
   - 2.4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.
3. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
   - 3.1. 18 portami Gigabit Ethernet RJ-45.
   - 3.2. 6 gniazdami SFP 1 Gbps.
   - 3.3. 6 gniazdami SFP+ 10 Gbps.
   - 3.4. wbudowany port konsoli szeregowej,
   - 3.5. gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
4. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

5. Parametry wydajnościowe:
   5.1. obsługa nie mniej niż 7.2 mln jednoczesnych połączeń oraz 480 tys. nowych połączeń na sekundę.
   5.2. Przepustowość Stateful Firewall: nie mniej niż 76 Gbps dla pakietów 512 B.
   5.3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 26 Gbps.
   5.4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 50 Gbps.
   5.5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 11 Gbps.
   5.6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 9 Gbps.
   5.7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – min. 7.2 Gbps.
6. Funkcje systemu bezpieczeństwa:
   6.1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
   6.2. Kontrola Aplikacji.
   6.3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
   6.4. Ochrona przed malware.
   6.5. Ochrona przed atakami - Intrusion Prevention System.
   6.6. Kontrola stron WWW.
   6.7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
   6.8. Zarządzanie pasmem (QoS, Traffic shaping).
   6.9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
   6.10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
   6.11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
   6.12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
   6.13. Wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).
7. Polityki, Firewall
   7.1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
   7.2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
      7.2.1. Translację jeden do jeden oraz jeden do wielu.
      7.2.2. Dedykowany ALG (Application-Level Gateway) dla protokołu SIP.
   7.3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
   7.4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
   7.5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
   7.6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
   7.7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
      7.7.1. Amazon Web Services (AWS).
      7.7.2. Microsoft Azure.
      7.7.3. Cisco ACI.
      7.7.4. Google Cloud Platform (GCP).
      7.7.5. OpenStack.
      7.7.6. VMware NSX.
      7.7.7. Kubernetes.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

8. Połączenia VPN
   8.1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
      8.1.1. Wsparcie dla IKE v1 oraz v2.
      8.1.2. Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
      8.1.3. Obsługa protokołu Diffie-Hellman grup 19, 20.
      8.1.4. Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
      8.1.5. Tworzenie połączeń typu Site-to-Site - co najmniej 5 połączeń jednocześnie
      8.1.6. Tworzenie połączeń Client-to-Site - co najmniej 50 połączeń jednocześnie.
      8.1.7. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
      8.1.8. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
      8.1.9. Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
      8.1.10. Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
      8.1.11. Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
      8.1.12. Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
      8.1.13. Mechanizm „Split tunneling" dla połączeń Client-to-Site.
   8.2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:
      8.2.1. Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. System zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
      8.2.2. Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
      8.2.3. Dostępne oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn nie jest przedmiotem zamówienia.
9. Routing i obsługa łączy WAN
   9.1. Obsługa routingu statycznego.
   9.2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
   9.3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
   9.4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
   9.5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
   9.6. BFD (Bidirectional Forwarding Detection).
   9.7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.
10. Funkcje SD-WAN
   10.1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
   10.2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).
11. Zarządzanie pasmem
   11.1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
   11.2. System daje możliwość określania pasma dla poszczególnych aplikacji.
   11.3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
   11.4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.
12. Ochrona przed malware
   12.1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
   12.2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
   12.3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

12.4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
12.5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
12.6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
12.7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.
12.8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
12.9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
12.10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

13. Ochrona przed atakami
13.1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
13.2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
13.3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
13.4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
13.5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
13.6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
13.7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
13.8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
13.9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

14. Kontrola aplikacji
14.1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
14.2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
14.3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
14.4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
14.5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
14.6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
14.7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

15. Kontrola WWW
15.1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
15.2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
15.3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
15.4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
15.5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
15.6. Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
15.7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

15.8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
15.9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

16. Uwierzytelnianie użytkowników w ramach sesji
16.1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:
16.2. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
16.3. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
16.4. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
16.5. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
16.6. System umożliwia budowę architektury uwierzytelniania typu SSO przy integracji ze środowiskiem AD oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
16.7. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

17. Zarządzanie
17.1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
17.2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
17.3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego.
17.4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
17.5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
17.6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
17.7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
17.8. Możliwość przypisywania administratorom praw do zarządzania częściami systemu (RBM).
17.9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

18. Logowanie
18.1. Elementy systemu bezpieczeństwa umożliwiają logowanie i raportowanie z aplikacji udostępnianej w chmurze, lub zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
18.2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
18.3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
18.4. Możliwość włączenia logowania per reguła w polityce firewall.
18.5. System zapewnia możliwość logowania do serwera SYSLOG.
18.6. Przesyłanie SYSLOG do zewnętrznych systemów z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

19. Wymagane licencje i serwisy: kontrola aplikacji, IPS, Antywirus (w tym sygnatury dla urządzeń mobilnych - min Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen.
20. Warunki gwarancji: gwarancja producenta na minimum 36 miesięcy z gwarantowaną wymianą i dostarczeniem do siedziby Zamawiającego nowego urządzenia, w maksymalnym terminie do następnego dnia roboczego po zgłoszeniu usterki.
21. System musi być objęty serwisem producenta przez okres min 36 miesięcy, upoważniającym do aktualizacji dostarczonego oprogramowania oraz wsparcia technicznego w trybie 24x7 przez okres min 36 miesięcy

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

Znak sprawy: …….. **Załącznik 2 do OPZ**

Wymagania na dostawę i instalację Urządzenia do monitorowania ruchu sieciowego

Do obowiązków Wykonawcy w ramach niniejszego zadania należy dostawa urządzenia do monitorowania ruchu sieciowego do siedziby Zamawiającego, spełniającego minimalne wymagania techniczne i funkcjonalne określone poniżej oraz jego instalacja i konfiguracja.

1. Wymagania Ogólne
   1.1. W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.
   1.2. Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi werje: 5.0, 5.1, 5.5, 6.0, 6.5, 6.7; Microsoft Hyper-V wersje: 2008 R2, 2012, 2012 R2, 2016; Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP).
2. System musi obsługiwać co najmniej:
   2.1. 4 interfejsy sieciowe oraz
   2.2. wspierać powierzchnię dyskową o pojemności 10 TB.
3. Parametry wydajnościowe:
   3.1. System musi być w stanie przyjmować minimum 5 GB logów na dzień.
   3.2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.
4. W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:
   4.1. Logowanie
      4.1.1. Podgląd logowanych zdarzeń w czasie rzeczywistym.
      4.1.2. Możliwość przeglądania logów historycznych z funkcją filtrowania.
      4.1.3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:
         4.1.3.1. Listę najczęściej wykrywanych ataków.
         4.1.3.2. Listę najbardziej aktywnych użytkowników.
         4.1.3.3. Listę najczęściej wykorzystywanych aplikacji.
         4.1.3.4. Listę najczęściej odwiedzanych stron www.
         4.1.3.5. Listę krajów, do których nawiązywane są połączenia.
         4.1.3.6. Listę najczęściej wykorzystywanych polityk Firewall.
         4.1.3.7. Informacje o realizowanych połączeniach IPSec.
      4.1.4. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
      4.1.5. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.
      4.1.6. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.
   4.2. W zakresie raportowania system musi zapewniać:
      4.2.1. Generowanie raportów co najmniej w formatach: PDF, CSV.
      4.2.2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
      4.2.3. Funkcję definiowania własnych raportów.
      4.2.4. Możliwość spolszczenia raportów.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

4.2.5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

4.3. W zakresie korelacji zdarzeń system musi zapewniać:

4.3.1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.

4.3.2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.

4.3.3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:

4.3.3.1. Malware.

4.3.3.2. Aplikacje sieciowe.

4.3.3.3. Email.

4.3.3.4. IPS.

4.3.3.5. Traffic.

4.3.3.6. Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.

4.3.4. Funkcję analizy logów archiwalnych względem aktualnej wiedzy producenta o zagrożeniach, w celu wykrycia potencjalnych stacji - narażonych na zagrożenie w ostatnim czasie.

5. Zarządzanie

5.1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.

5.2. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.

5.3. System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.

6. System musi być objęty serwisem producenta przez okres 36 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

Znak sprawy: …….. **Załącznik 3 do OPZ**

Wymagania na dostawę i instalację Serwera zarządzania tożsamością i dostępem

Do obowiązków Wykonawcy w ramach niniejszego zadania należy dostawa Serwera zarządzania tożsamością i dostępem do siedziby Zamawiającego, spełniającego minimalne wymagania techniczne i funkcjonalne określone poniżej oraz jego instalacja i konfiguracja.

1. Parametry techniczne
   - 1.1. Obudowa typu: rack
   - 1.2. Dwa CPU, każdy o wydajności w teście Average CPU Mark minimum 19000 (według wyników testów dostępnych na https://www.cpubenchmark.net)
   - 1.3. Pamięć RAM: 192GB.
   - 1.4. Kontroler dysków: SAS z 8GB pamięci.
   - 1.5. Dwa dyski 800GB SSD MU SAS 2.5in Hot-Plug
   - 1.6. Trzy dyski 2.4TB 10K RPM SAS 2.5in Hot-Plug
   - 1.7. Kontroler wraz z dwoma modułami pamięci M.2 240GB (RAID 1)
   - 1.8. Karty sieciowe:
     - 1.8.1. 1 x Dual Port 1Gb LOM
     - 1.8.2. 1 x Quad Port 1Gb.
   - 1.9. Kontroler monitorowania i zarządzania zdalnego z pełną funkcjonalnością wirtualnego KVM.
   - 1.10. Zasilanie:
     - 1.10.1. Dual, Hot-Plug,
     - 1.10.2. FT Redundant (1+1),
     - 1.10.3. 700W Titanium.
2. Oprogramowanie systemowe o funkcjonalności jak Windows Server 2022 Standard.
3. Gwarancja:
   - 3.1. minimum na okres 36 miesięcy
   - 3.2. z czasem reakcji na awarię typu NBD
   - 3.3. w przypadku awarii dysków twardych – wymiana dysków na nowe, uszkodzone dyski pozostają u Zamawiającego

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

Znak sprawy: …….. **Załącznik 4 do OPZ**

Wymagania na dostawę i instalację Oprogramowania do zarządzania tożsamością,

Do obowiązków Wykonawcy w ramach niniejszego zadania należy instalacja Oprogramowania do zarządzania tożsamością, spełniającego minimalne wymagania funkcjonalne określone poniżej.

1. Licencje - MS Windows Server CAL 2022 User CALs dla 150 użytkowników

Aktualnie Zamawiający posiada CAL-e systemowe środowiska Windows w wersji 2019. Aby można legalnie wdrażać i używać nowe serwery pracujące pod systemem Windows Server 2022 – konieczne jest posiadanie licencji Windows Server CAL w wersji 2022 (tj. nie niższej niż najwyższa wersja pracującego serwera Windows).

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

Znak sprawy: …….. **Załącznik 5 do OPZ**

Wymagania na dostawę i instalację Systemu bezpieczeństwa poczty elektronicznej,

Do obowiązków Wykonawcy w ramach niniejszego zadania należy dostawa Systemu bezpieczeństwa poczty elektronicznej do siedziby Zamawiającego, spełniającego minimalne wymagania techniczne i funkcjonalne określone poniżej oraz jego instalacja i konfiguracja.

1. Wymagania ogólne
   - 1.1. System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware'ową bez limitu licencyjnego na ilość chronionych kont użytkowników.
   - 1.2. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia w środowisku wirtualnym. W przypadku implementacji programowej dostawca musi zapewnić platformę w postaci odpowiednio zabezpieczonego systememu operacyjnego, na którym będzie instalowane rozwiązanie. Platformy muszą mieć możliwość uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi 5.0/5.1/5.5/6.0/6.5/7.0, Microsoft Hyper-V 2008 R2/2012/2012 R2/2016, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, AWS (Amazon Web Services), Microsoft Azure.
   - 1.3. Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o komercyjne bazy zabezpieczeń.
   - 1.4. Dostarczone rozwiązanie musi mieć możliwość pracy w każdym trybów:
     - 1.4.1. Tryb Gateway.
     - 1.4.2. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej).
2. System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności co najmniej 1 TB.
3. Ogólne funkcje systemu ochrony poczty
   - 3.1. Wsparcie dla co najmniej 20 domen pocztowych.
   - 3.2. System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 25 tys. wiadomości/godzinę.
   - 3.3. Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all).
   - 3.4. Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP.
   - 3.5. Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości).
   - 3.6. Możliwość ograniczenia ilości poczty wychodzącej do chronionych domen w oparciu o nie mniej niż: ilość jednoczesnych sesji, maksymalną liczbę wiadomości w ramach sesji, maksymalną liczbę odbiorców w zadanym czasie.
   - 3.7. Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej.
   - 3.8. Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów.
   - 3.9. Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP.
   - 3.10. Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika.
   - 3.11. Możliwość poddania ponownemu skanowaniu (antywirus, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora.
   - 3.12. Dostęp do kwarantanny użytkownika możliwy poprzez WebMail.
   - 3.13. Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki.
   - 3.14. Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI.
   - 3.15. Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu.
   - 3.16. Białe i czarne listy adresów mailowych dla poszczególnych użytkowników.
   - 3.17. Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika.
4. Kontrola antywirusowa i ochrona przed malware

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

4.1. Skanowanie antywirusowe wiadomości SMTP.
4.2. Kwarantannę dla zainfekowanych plików.
4.3. Skanowanie załączników skompresowanych.
4.4. Definiowanie komunikatów powiadomień w języku polskim.
4.5. Blokowanie załączników w oparciu o typ pliku.
4.6. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antywirusowej.
4.7. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu.
4.8. Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.
4.9. Ochronę typu wirus outbrake.
4.10. Ochronę przed zagrożeniami zawartymi wiadomościach pocztowych i w załącznikach (nie mniej niż: pliki MS Office, PDF, HTML, tekstowe) poprzez usuwanie treści będących zagrożeniem (makra, adresy URL zagnieżdżone w plikach, skrypty, ActiveX) i dostarczaniem oczyszczonych w ten sposób wiadomości.

5. Kontrola antyspamowa
5.1. Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta.
5.2. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania.
5.3. Szczegółowa kontrola nagłówka wiadomości.
5.4. Analiza Heurystyczna.
5.5. Współpraca z zewnętrznymi serwerami RBL, SURBL.
5.6. Filtrowanie w oparciu o filtry Bayes'a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen.
5.7. Możliwością dostrajania filtrów Bayes'a przez poszczególnych użytkowników.
5.8. Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF.
5.9. Kontrola w oparciu o Greylisting oraz SPF.
5.10. Filtrowanie treści wiadomości i załączników.
5.11. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości.
5.12. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antyspamowej.
5.13. Ochrona typu outbrake.
5.14. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).
5.15. Możliwość skanowania linków znajdujących się w przesyłkach pocztowych, w momencie ich kliknięcia przez adresata.
5.16. Możliwość wykrywania i ochrony przed podszywaniem się (spoofing) pod wiadomości wysyłane przez osoby na stanowiskach kierowniczych (C-level).
5.17. Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.

6. Ochrona przed atakami na usługę poczty
6.1. Ochrona przed atakami na adres odbiorcy (m.in. email bombing).
6.2. Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.
6.3. Defniowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu.
6.4. Kontrola Reverse DNS (ochrona przed Anty-Spoofing).
6.5. Weryfikacja poprawności adresu e-mail nadawcy.

7. Funkcje logowania i raportowania
7.1. Logowanie do zewnętrznego serwera SYSLOG.
7.2. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku.
7.3. Logowanie informacji na temat spamu oraz niedozwolonych załączników.
7.4. Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych.
7.5. Możliwość analizy przebiegu sesji SMTP.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

7.6. Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych.
7.7. Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu.
7.8. Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.

8. Funkcje pracy w trybie wysokiej dostępności (HA)
8.1. Konfigurację HA w każdym z trybów: gateway, transparent.
8.2. Tryb synchronizacji konfiguracji dla scenariuszy, gdy każde z urządzeń występuje pod innym adresem IP.
8.3. Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu.
8.4. Monitorowanie stanu pracy klastra.

9. Aktualizacje sygnatur, dostęp do bazy spamu
9.1. Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym.
9.2. Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.

10. Zarządzanie
10.1. System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH.
10.2. Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy.
10.3. Możliwość zdefiniowania co najmniej 3 lokalnych kont administracyjnych.

11. Certyfikaty - dostarczony system powinien posiadać co najmniej dwie z poniższych certyfikacji:
11.1. VBSpam,
11.2. VB100 rated,
11.3. Common Criteria NDPP,
11.4. FIPS 140-2 Certified.

12. Gwarancja, serwisy i licencje
12.1. System musi być objęty serwisem producenta przez okres 36 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.
12.2. System musi być dostarczony w modelu „na własność" tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu, może jedynie pozbawi możliwości pobierania aktualizacji oprogramowania.
12.3. W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: Kontrola Antyspam, URL Filtering, kontrola antywirusowa, ochrona typu Virus Outbrake, Sandbox w chmurze, ochrona typu Click Protect, Content Disarm & Reconstruction, Business Email Compromise na okres 36 miesięcy.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

Znak sprawy: …….. **Załącznik 6 do OPZ**

Wymagania na usługi instalacji i konfiguracji Ochrony styku z Internetem

Do obowiązków Wykonawcy w ramach niniejszego zadania należy wykonanie usług instalacji i konfiguracji Ochrony styku z Internetem o minimalnym zakresie określonym poniżej.

1. Wdrożenie nowego serwera (wirtualnego) usług zewnętrznego DNS UM – a w szczególności:
2. Utworzenie VM w środowisku VMware vSphere.
3. Instalacja i konfiguracja systemu operacyjnego MS Windows Server 2022, jego aktualizacja itd.
4. Instalacja roli serwera DNS i odtworzenie jego konfiguracji z dotychczasowego serwera DNS zewnętrznego.
5. Przygotowanie dwóch VMs z systemem Windows Server 2022 do migracji dwóch serwerów (APP, DB)
6. Przeniesienie konfiguracji z działającej zapory sieciowej FortiGate 500E na nowo dostarczone rozwiązane.
7. Dostosowanie konfiguracji zgodnie z wymaganiami bezpieczeństwa i dobrymi praktykami.
8. Wdrożenie urządzenia do monitorowania ruchu sieciowego.
9. Integracja Firewalla z urządzeniem do monitorowania ruchu sieciowego.
10. Wdrożenie systemu bezpieczeństwa poczty elektronicznej do pracy z istniejącym serwerem pocztowym MS Exchange.
11. Dostarczenie dokumentacji technicznej całego wdrożenia z punktów 1-10.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

Znak sprawy: …….. **Załącznik 7 do OPZ**

Wymagania na dostawę i instalację Serwera Backupu

Do obowiązków Wykonawcy w ramach niniejszego zadania należy dostawa Serwera Backupu do siedziby Zamawiającego, spełniającego minimalne wymagania techniczne i funkcjonalne określone poniżej oraz jego instalacja i konfiguracja.

1. Parametry techniczne
   - 1.1. Obudowa typu: rack
   - 1.2. CPU o wydajności w teście Average CPU Mark minimum 12000 (według wyników testów dostępnych na https://www.cpubenchmark.net)
   - 1.3. Pamięć RAM: 32GB.
   - 1.4. Kontroler dysków: SAS z 8GB pamięci.
   - 1.5. Dwa dyski każdy 2TB HDD SAS 12Gbps
   - 1.6. Karty sieciowe:
     - 1.6.1. 1 x Dual Port 1Gb LOM
     - 1.6.2. 1 x Quad Port 1Gb.
   - 1.7. Kontroler monitorowania i zarządzania zdalnego z pełną funkcjonalnością wirtualnego KVM.
   - 1.8. Zasilanie: Dual, Hot-Plug, FT Redundant (1+1), 700W Titanium
2. Oprogramowanie systemowe o funkcjonalności jak Windows Server 2022 Standard.
3. Gwarancja:
   - 3.1. minimum na okres 36 miesięcy
   - 3.2. z czasem reakcji na awarię typu NBD
   - 3.3. w przypadku awarii dysków twardych – wymiana dysków na nowe, uszkodzone dyski pozostają u Zamawiającego

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

Znak sprawy: …….. **Załącznik 8 do OPZ**

Wymagania na dostawę i instalację NAS-a

Do obowiązków Wykonawcy w ramach niniejszego zadania należy dostawa NAS-a do siedziby Zamawiającego, spełniającego minimalne wymagania techniczne i funkcjonalne określone poniżej oraz jego instalacja i konfiguracja.

1. Urządzenie w obudowie typu tower, posiadające:
   1.1. 8 kieszeni na dyski
   1.2. 2 porty 100M/1G/2,5G
   1.3. 2 porty 10Gbps Ethernet.
2. 6 sztuk dysków do pracy ciągłej każdy o parametrach 8TB, 7200rpm, 256MB cache
   2.1. Dyski w konfiguracji w RAID6 + HS.
3. Urządzenie posiadające technologię kopii migawkowych (snapshot'ów) wolumenów.
4. Gwarancja:
   4.1. minimum na okres 36 miesięcy na dyski i NAS
   4.2. typu „door to door"
   4.3. aktualizacja oprogramowania
   4.4. w przypadku awarii dysków twardych – wymiana dysków na nowe, uszkodzone dyski pozostają u Zamawiającego.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

Znak sprawy: …….. **Załącznik 9 do OPZ**

Wymagania na dostawę i instalację Oprogramowania kopii zapasowych

Do obowiązków Wykonawcy w ramach niniejszego zadania należy instalacja Oprogramowania kopii zapasowych w siedzibie Zamawiającego, spełniającego minimalne wymagania techniczne i funkcjonalne określone poniżej.

1. Wymagana jest rozbudowa środowiska backupu o dodatkowy storage - rozszerzenie środowiska backupu o drugą instancję backupów (backup copy), polegające na wyniesieniu do lokalizacji zewnętrznej względem głównego CPD, w celu realizacji minimalnej rekomendowanej strategii kopii zapasowych „3-2-1", czyli:
   1.1. przechowuj 3 egzemplarze zasobów – dane produkcyjne, backup i jego replikę;
   1.2. wykorzystaj co najmniej 2 technologie/nośniki przechowywania danych;
   1.3. przechowuj jedną instancję danych (backup) poza głównym CPD).
2. Zamawiający obecnie używa oprogramowania VeeamB&R, jednak w aktualnej konfiguracji nie ma już żadnej wolnej licencji na serwerze backupu, aby było możliwe wykonywanie kopii nowego serwera – konieczny jest zakup dodatkowych 10 licencji typu VUL rozszerzających dotychczasowe środowisko, ich instalacja i konfiguracja do opisanego powyżej stanu.
3. Gwarancja i opieka aktualizująca:
   3.1. minimum na okres 36 miesięcy.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

Znak sprawy: …….. **Załącznik 10 do OPZ**

Wymagania na usługi instalacji i konfiguracji Backupu

Do obowiązków Wykonawcy w ramach niniejszego zadania należy wykonanie usług instalacji i konfiguracji Ochrony styku z Internetem o minimalnym zakresie określonym poniżej.

1. Upgrade aktualnego środowiska CPD - komponentów VMware vSphere (vCenter, hosty ESXi) oraz głównego repozytorium backupów.
2. Aktualizacja 4 systemów operacyjnych serwerów z systemem Windows Server 2019, a w szczególności:
   - 2.1. Aktualizacja firmware'ów obu pracujących hostów ESXi VMware vSphere
   - 2.2. Upgrade i update serwera zarządzania vCenter do wersji 8.0.
   - 2.3. Upgrade i update obu hostów ESXi do wersji 8.0.
   - 2.4. Aktualizacja firmware'u głównego, repozytorium backupów (NAS firmy QNAP).
   - 2.5. Instalacja poprawek systemów operacyjnych serwerów z systemem Windows Server 2019
3. Wdrożenie trzeciego hosta ESXi w celu rozbudowy vSphere'a, a w szczególności:
   - 3.1. Instalacja i konfiguracja serwera
   - 3.2. Aktualizacja firmware'ów, konfiguracja BIOS, iDRAC, kontrolera BOSS, kontrolera dysków, puli dyskowych itp.
   - 3.3. Instalacja i konfiguracja hypervisor'a ESXi w wersji 8.0, przełączników wirtualnych itp.
   - 3.4. Przyłączenie nowego hosta do serwera zarządzania vCenter.
   - 3.5. Konfiguracja magazynów na nowym hoście ESXi.
4. Wdrożenie dodatkowego repozytorium (kopii backupów), w szczególności:
   - 4.1. Instalacja i konfiguracja nowego NAS-a.
   - 4.2. Aktualizacja firmware'u, konfiguracja użytkowników, interfejsów sieci LAN, puli dyskowej, RAID-u, wolumenów itp.
5. Wdrożenie nowego serwera fizycznego, w szczególności:
   - 5.1. Instalacja i konfiguracja serwera backupu w serwerowni
   - 5.2. Aktualizacja firmware'ów, konfiguracja BIOS, iDRAC, kontrolera dysków, puli dyskowej itp.
   - 5.3. Instalacja i konfiguracja systemu operacyjnego, jego aktualizacja itp., w tym instalacja roli serwera DHCP i odtworzenie jego konfiguracji z serwera dotychczasowego.
   - 5.4. Instalacja i konfiguracja oprogramowania narzędziowego - do wykonywania kopii zapasowych: Veeam Backup & Replication, w tym:
     - 5.4.1. Przeniesienie i odtworzenie elementów konfiguracji (repositories, proxies, jobs itd.) i zasobów repozytorium backupów.
     - 5.4.2. Upgrade i aktualizacja binariów VB&R do najnowszej możliwej wersji.
     - 5.4.3. Konfiguracja dodatkowego repozytorium dla kopii backupów wraz z zadaniami typu „copy backup".
   - 5.5. Instalacja i konfiguracja uzupełniającego oprogramowania narzędziowego do wykonywania kopii zapasowych, w tym przeniesienie zadania wykonywania kopii zapasowych z dotychczasowego serwera.
   - 5.6. Upgrade i aktualizacja binariów oprogramowania narzędziowego do wykonywania kopii zapasowych do najnowszej możliwej wersji.
6. Rekonfiguracja zadania backupu VM.
7. Wdrożenie nowego serwera (wirtualnego) usług zewnętrznego DNS – a w szczególności:
   - 7.1. Utworzenie VM w środowisku VMware vSphere.
   - 7.2. Instalacja i konfiguracja systemu operacyjnego MS Windows Server 2022, jego aktualizacja.
   - 7.3. Instalacja roli serwera DNS i odtworzenie jego konfiguracji z dotychczasowego serwera DNS zewnętrznego.
8. Rekonfiguracja zadania backupu VM
9. Przygotowanie dwóch VMs z systemem Windows Server 2022 do migracji 2 serwerów (APP, DB) w tym:
   - 9.1. Utworzenie VMs w środowisku VMware vSphere.
   - 9.2. Instalacja i konfiguracja systemu operacyjnego MS Windows Server 2022, jego aktualizacja itd.
10. Konfiguracja zadań backupu VMs

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

Znak sprawy: …….. **Załącznik 11 do OPZ**

Wymagania na Szkolenia specjalistyczne dla kadry zarządzającej

Do obowiązków Wykonawcy w ramach niniejszego zadania należy przeprowadzenie specjalistycznych szkoleń dedykowanych dla kadry zarządzającej, spełniających minimalne wymagania określone poniżej.

1. W ramach przeprowadzonych szkoleń wymaga się przekazania niezbędnej dla kadry zarządzającej jednostką wiedzy w zakresie zagadnień wpływających na cyberbezpieczeństwo jednostki Zamawiającego.
2. Obowiązkiem Wykonawcy będzie:
   2.1. Przeprowadzić szkolenie.
   2.2. Przygotować infrastrukturę szkoleniową w udostępnionej sali szkoleniowej.
   2.3. Zapewnić każdemu uczestnikowi materiały szkoleniowe.
   2.4. Sporządzić dokumentację z przeprowadzonych szkoleń.
3. Wymagania w zakresie organizacji szkolenia:
   3.1. Zajęcia powinny odbywać się w godzinach od godz. 8 do 15,
   3.2. Zajęcia nie mogą trwać dłużej niż 6 godzin lekcyjnych dziennie.
   3.3. Szkolenia odbywać się będą w siedzibie Zamawiającego
   3.4. Zajęcia muszą być prowadzone metodą warsztatów aktywizującą uczestników szkoleń,
   3.5. Wymaga się by termin szkolenia był uzgodniony z Zamawiającym
   3.6. Liczba godzin szkoleniowych – minimum 8
   3.7. Liczba pracowników objętych szkoleniem – maksimum 6
4. Tematyka szkolenia:
   4.1. Podstawy prawne cyberbezpieczeństwa
   4.2. Wymogi wynikające z KRI, uoKSC i RODO
   4.3. Potencjalne konsekwencje dla kierownictwa jednostki, dotyczące zaniechań w obszarze cyberbezpieczeństwa.
   4.4. Przegląd znanych typów ataków na JST
   4.5. Przegląd nowoczesnych narzędzi i usług cyberbezpieczeństwa
   4.6. Zarządzanie ryzykiem w bezpieczeństwie informacji i obszarach technicznych.
   4.7. Zasady zarządzania bezpieczeństwem informacji w JST - SZBI
   4.8. Ciągłość działania
   4.9. Współpraca w ramach s46
   4.10. Identyfikowanie zagrożeń
   4.11. Ścieżka rozwoju JST w obszarze cyberbezpieczeństwa

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

Znak sprawy: …….. **Załącznik 12 do OPZ**

Wymagania na Szkolenia specjalistyczne dla kadry IT

Do obowiązków Wykonawcy w ramach niniejszego zadania należy przeprowadzenie specjalistycznych szkoleń dedykowanych dla kadry IT, spełniających minimalne wymagania określone poniżej.

1. W ramach przeprowadzonych szkoleń wymaga się przekazania niezbędnej dla kadry informatycznej Zamawiającego wiedzy w zakresie zagadnień wpływających na cyberbezpieczeństwo jednostki Zamawiającego.
2. Obowiązkiem Wykonawcy będzie:
   2.1. Przeprowadzić szkolenie.
   2.2. Przygotować infrastrukturę szkoleniową w udostępnionej sali szkoleniowej.
   2.3. Zapewnić każdemu uczestnikowi materiały szkoleniowe.
   2.4. Sporządzić dokumentację z przeprowadzonych szkoleń.
3. Wymagania w zakresie organizacji szkolenia:
   3.1. Zajęcia powinny odbywać się w godzinach od godz. 8 do 15,
   3.2. Zajęcia nie mogą trwać dłużej niż 6 godzin lekcyjnych dziennie.
   3.3. Szkolenia odbywać się będą w siedzibie Zamawiającego
   3.4. Zajęcia muszą być prowadzone metodą warsztatów aktywizującą uczestników szkoleń,
   3.5. Wymaga się by termin szkolenia był uzgodniony z Zamawiającym
4. Tematyka szkolenia:
   4.1. Szkolenie dedykowane z elementami troubleshooting'u z zakresu AD
      4.1.1. Liczba godzin szkoleniowych – minimum 10
      4.1.2. Liczba pracowników objętych szkoleniem – maksimum 3
   4.2. Szkolenie dedykowane z elementami troubleshooting'u z zakresu wdrożonego systemu backupu
      4.2.1. Liczba godzin szkoleniowych – minimum 10
      4.2.2. Liczba pracowników objętych szkoleniem – maksimum 3
   4.3. Szkolenie dedykowane z elementami troubleshooting'u z zakresu wdrożonego systemu ochrony styku z Internetem
      4.3.1. Liczba godzin szkoleniowych – minimum 10
      4.3.2. Liczba pracowników objętych szkoleniem – maksimum 3

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

Znak sprawy: …….. **Załącznik 13 do OPZ**

Wymagania na Szkolenia specjalistyczne dla pracowników Zamawiającego

Do obowiązków Wykonawcy w ramach niniejszego zadania należy przeprowadzenie specjalistycznych szkoleń dedykowanych dla pracowników Zamawiającego, spełniających minimalne wymagania określone poniżej.

1. W ramach przeprowadzonych szkoleń wymaga się przekazania niezbędnej pracowników Zamawiającego wiedzy w zakresie zagadnień wpływających na cyberbezpieczeństwo jednostki Zamawiającego.
2. Obowiązkiem Wykonawcy będzie:
   - 2.1. Przeprowadzić szkolenie.
   - 2.2. Przygotować infrastrukturę szkoleniową w udostępnionej sali szkoleniowej.
   - 2.3. Zapewnić każdemu uczestnikowi materiały szkoleniowe.
   - 2.4. Sporządzić dokumentację z przeprowadzonych szkoleń.
3. Wymagania w zakresie organizacji szkolenia:
   - 3.1. Zajęcia powinny odbywać się w godzinach od godz. 8 do 15,
   - 3.2. Zajęcia nie mogą trwać dłużej niż 6 godzin lekcyjnych dziennie.
   - 3.3. Szkolenia odbywać się będą w siedzibie Zamawiającego
   - 3.4. Zajęcia muszą być prowadzone metodą warsztatów aktywizującą uczestników szkoleń,
   - 3.5. Wymaga się by harmonogram szkoleń był uzgodniony z Zamawiającym
4. Zakres szkolenia pracowników
   - 4.1. Liczba godzin szkolenia – minimum 4
   - 4.2. Liczba pracowników objętych szkoleniem – maksimum 80
   - 4.3. Grupy szkoleniowe nie będą mogły liczyć więcej niż 15 osób
5. Tematyka szkolenia:
   - 5.1. Bezpieczeństwo informacji – podstawowe wiadomości, z uwzględnieniem regulacji wewnętrznych oraz wymagań rozporządzenia KRI
     - 5.1.1. Wewnętrzne procedury w obszarze bezpieczeństwa informacji cyberbezpieczeństwa
     - 5.1.2. Wymagania dla pracowników wynikające z KRI, uoKSC oraz RODO
     - 5.1.3. System Zarządzania Bezpieczeństwem Informacji w praktyce
   - 5.2. Przegląd najpopularniejszych zagrożeń i zasady bezpiecznego korzystania z internetu
     - 5.2.1. Ochrona informacji i prywatność w internecie
     - 5.2.2. Ransomware jako poważne zagrożenie dla JST
     - 5.2.3. Phishing, oszustwa i wyłudzenia z uwzględnieniem oszustwa typu BEC
     - 5.2.4. Cyberhigiena, w tym bezpieczeństwo urządzeń i bezpieczeństwo fizyczne
     - 5.2.5. Bezpieczne hasła i uwierzytelnienie dwuskładnikowe
     - 5.2.6. Wewnętrzne zalecenia i rekomendacje, w tym sposoby reakcji na incydenty bezpieczeństwa

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

Znak sprawy: …….. **Załącznik 14 do OPZ**

Opracowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji

Opracowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), zgodnie z wymaganiami aktualnej normy PN-EN ISO/IEC 27001, o minimalnym zakresie:

1. Zabezpieczenia organizacyjne
   - 1.1. Polityki bezpieczeństwa informacji
   - 1.2. Role i obowiązki w zakresie bezpieczeństwa informacji
   - 1.3. Podział obowiązków
   - 1.4. Odpowiedzialność kierownictwa
   - 1.5. Kontakt z organami władzy
   - 1.6. Kontakt z grupami szczególnego interesu
   - 1.7. Analiza zagrożeń
   - 1.8. Bezpieczeństwo informacji w zarządzaniu projektami
   - 1.9. Rejestr informacji i innych powiązanych zasobów
   - 1.10. Dopuszczalne wykorzystanie informacji i innych powiązanych zasobów
   - 1.11. Zwrot zasobów
   - 1.12. Klasyfikacja informacji
   - 1.13. Oznakowanie informacji
   - 1.14. Transfer informacji
   - 1.15. Kontrola dostępu
   - 1.16. Zarządzanie tożsamością
   - 1.17. Informacje uwierzytelniające
   - 1.18. Prawa dostępu
   - 1.19. Bezpieczeństwo informacji w relacjach z dostawcami
   - 1.20. Uwzględnianie bezpieczeństwa informacji w umowach z dostawcami
   - 1.21. Monitorowanie, przegląd i zarządzanie zmianami w usługach dostawców
   - 1.22. Bezpieczeństwo informacji przy korzystaniu z usług w chmurze
   - 1.23. Planowanie i przygotowanie zarządzania incydentami bezpieczeństwa informacji
   - 1.24. Ocena i decyzje dotyczące zdarzeń związanych z bezpieczeństwem informacji
   - 1.25. Reagowanie na incydenty związane z bezpieczeństwem informacji
   - 1.26. Wyciąganie wniosków z incydentów bezpieczeństwa informacji
   - 1.27. Gromadzenie dowodów
   - 1.28. Bezpieczeństwo informacji w czasie zakłóceń
   - 1.29. Gotowość technologii informacyjno-komunikacyjnych do zapewnienia ciągłości działania
   - 1.30. Wymagania prawne, ustawowe, regulacyjne i umowne
   - 1.31. Prawa własności intelektualnej
   - 1.32. Ochrona zapisów
   - 1.33. Prywatność i ochrona danych osobowych
   - 1.34. Niezależny przegląd bezpieczeństwa informacji
   - 1.35. Zgodność z polityką, zasadami i normami dotyczącymi bezpieczeństwa informacji
2. Zabezpieczenia związane z zasobami ludzkimi
   - 2.1. Zasady i warunki zatrudnienia
   - 2.2. Świadomość, edukacja i szkolenie w zakresie bezpieczeństwa
   - 2.3. Postępowanie dyscyplinarne
   - 2.4. Obowiązki po rozwiązaniu lub zmianie zatrudnienia
   - 2.5. Umowy o poufności lub nieujawnianiu informacji
   - 2.6. Praca zdalna

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

Znak sprawy: …….. **Załącznik 15 do OPZ**

Wymagania na dostawę i instalację Oprogramowania do audytu i utrzymania SZBI.

Do obowiązków Wykonawcy w ramach niniejszego zadania należy instalacja Oprogramowania do audytu i utrzymania SZBI, spełniającego minimalne wymagania określone poniżej.

1. Użytkownicy
   1.1. Synchronizacja użytkowników systemu z Active Directory
2. Nadawanie uprawnień
   2.1. Zdefiniowane trzy role:
      2.1.1. Administrator,
      2.1.2. Pracownik,
      2.1.3. Kontroler
      2.1.4. Kierownik
      2.1.5. Inspektor
   2.2. uprawnienia dla w.w. ról bez możliwości zmian
3. Słowniki
   3.1. Cele kontroli - słownik celów wykorzystywanych w planach i programach kontroli
   3.2. Jednostki - słownik jednostek
   3.3. Projekty - słownik projektów wykorzystywany w zaleceniach
   3.4. Dokumenty - słownik dokumentów wykorzystywany w programach, nieprawidłowościach
   3.5. Procesy - słownik procesów wykorzystywany w nieprawidłowościach
   3.6. Systemy - słownik systemów wykorzystywany w programach, nieprawidłowościach
   3.7. Mechanizmy kontrolne - słownik mechanizmów wykorzystywany w rejestrze ryzyk i RODO
   3.8. Inspektorzy
   3.9. Administratorzy danych
   3.10. Kategorie danych
   3.11. Kategorie osób
   3.12. Cele przetwarzania
   3.13. Podstawy przetwarzania
   3.14. Skala ryzyk
   3.15. Wrażliwość
   3.16. Liczebność
   3.17. Checklisty - tworzenie własnych wielopoziomowych checklist służących do przeprowadzania kontroli i udzielania jednoznacznych odpowiedzi na każde pytanie.
4. Plany kontroli
   4.1. Dodawanie planów kontroli;
   4.2. Proces akceptacji poszczególnych planów kontroli - akceptacja planów przez osobę tworzącą
5. Programy testowania
   5.1. Dodawanie programów testowania;
   5.2. Tworzenie programów dotyczących pojedynczych obszarów, podział całego SZBI na poszczególne okresy i osoby;
   5.3. Proces akceptacji poszczególnych programów;
   5.4. Definiowanie próby kontrolnej - możliwość zdefiniowania próby kontrolnej do badania
6. Badanie
   6.1. Przeprowadzanie badania na bazie checklisty - możliwość przeprowadzenia badania na bazie checklisty dla każdego przypadku testowego w ramach próby. . Zabezpieczenie przed pominięciem odpowiedzi na pytania z checklisty podczas badania.
   6.2. Weryfikacja badania przez stronę kontrolowaną - możliwość weryfikacji wyników badania przez kontrolowanego pracownika

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

6.3. Zamykanie badania przez kontrolera - kończenie badania i akceptacja wyników kontroli celem generowania nieprawidłowości i zaleceń.

7. Nieprawidłowości
   7.1. Automatyczne generowanie nieprawidłowości z badania na podstawie udzielonych odpowiedzi - generowanie nieprawidłowości w oparciu o o szablon treści nieprawidłowości powiązany z pytaniami na checkliście.
   7.2. Ręczna ewidencja nieprawidłowości wykrytych podczas kontroli - możliwość ręcznego dodawania nieprawidłowości
   7.3. Proces zarządzania nieprawidłowościami (ewidencja, zatwierdzanie, zamykanie)
8. Zalecenia
   8.1. Automatyczne generowanie zaleceń po badaniu na podstawie udzielonych odpowiedzi - generowanie zaleceń w oparciu o szablon treści zaleceń powiązany z pytaniami na checkliście;
   8.2. Ręczna ewidencja zaleceń - możliwość ręcznego dodawania zaleceń;
   8.3. Proces akceptacji poszczególnych zaleceń - ewidencja, zatwierdzanie do realizacji zalecenia;
   8.4. Import zaleceń - możliwość importu zaleceń z pliku
   8.5. Przypisywanie zaleceń do projektów
   8.6. Proces zatwierdzania sposobu realizacji zalecenia
9. Rejestr ryzyk
   9.1. Ewidencja ryzyk - identyfikacja ryzyk wraz z możliwością szacowania i oceny, kontroli i monitorowania ryzyka
10. Rejestr czynności przetwarzania
   10.1. Ewidencja czynności przetwarzania danych osobowych - prowadzenie rejestru czynności przetwarzania realizowanych zarówno jako administrator danych, które w danej czynności są przetwarzane jak i jako podmiot przetwarzający dane osobowe (RODO)
11. Rejestr incydentów
   11.1. Ewidencja incydentów - prowadzenie ewidencji wykrytych incydentów wraz z jego oceną i klasyfikacją, określeniem rodzaju i skali incydentu oraz jego potencjalnego wpływu na jednostkę
12. Rejestr upoważnień
   12.1. Ewidencja nadanych uprawnień do systemów - prowadzenie ewidencji upoważnień do systemów informatycznych, do których użytkownik ma mieć dostęp, szkoleń dotyczących ochrony danych i podpisanych upoważnień do przetwarzania danych osobowych
13. Raporty
   13.1. Protokół pokontrolny
   13.2. Raport z planów kontroli
   13.3. Raport z programów badań
   13.4. Raport z realizacji zaleceń
   13.5. Raport z nieprawidłowości
   13.6. Raport z rejestru ryzyk
   13.7. Raport z rejestru czynności przetwarzania
   13.8. Raport z rejestru incydentów
   13.9. Raport z rejestru upoważnień
   13.10. Raport z realizacji projektów

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa