



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

Załącznik nr 1 do umowy – Szczegółowy Opis Przedmiotu Zamówienia

Zadanie częściowe nr 1:

Dostawa sprzętu informatycznego oraz oprogramowania – wymagania minimalne:

1. Centralny System Bezpieczeństwa - Oprogramowanie klasy SIEM z elementami XDR Extended Detection and Response, EDR Endpoint Detection and Response, oraz monitoringiem infrastruktury IT – 1 szt.;

LICENCJA

W ramach postępowania Wykonawca jest zobowiązany dostarczyć Oprogramowanie wraz z licencją bezterminową.

Oprogramowanie musi posiadać wsparcie min. do dnia 25-05-2026 roku, w ramach wsparcia, Zamawiający musi posiadać możliwość aktualizacji do najnowszej dostępnej wersji oprogramowania, zgłaszać błędy w Oprogramowaniu do serwisu producenta.

Licencje na oprogramowanie dostarczone będą do siedziby Zamawiającego w formie papierowej lub elektronicznej.

Dostarczona licencja na Oprogramowanie Systemu nie może limitować wielkości przechowywanych danych oraz możliwości wyszukiwania informacji z zgromadzonych danych.

WYMAGANIA DOT. SYSTEMU BEZPIECZEŃSTWA:

Automatyczne Odkrywanie: Centralny System Bezpieczeństwa (dalej CSB) musi używać różnych metod, takich jak skanowanie sieci, obsługa protokołów SNMP, IPMI, i JMX, aby automatycznie wykrywać i konfigurować urządzenia w sieci.



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

Monitorowanie Wysokiej Wydajności: CSB musi umożliwiać monitorowanie wydajności przy wykorzystaniu rozwiązań agentowych lub bez agentowych metodami monitorowania (np. przez SNMP, ICMP, IPMI), CSB musi efektywnie zbierać dane o wydajności i dostępności urządzeń. System powinien być skalowalny i umożliwiać obsługę co najmniej 100 urządzeń i metryk.

Elastyczne Wyzwalacze: Wyzwalacze (akcje) w CSB powinny być wyrażeniami logicznymi, które określają warunki dla powiadomień alarmowych. W systemie musi być możliwość definiowania złożonych warunków dla generowania alertów, na przykład po przekroczeniu pewnych progów lub w przypadku wystąpienia określonych wzorców.

Wizualizacja Danych: CSB powinien posiadać intuicyjny i przejrzysty interfejs, umożliwiający wizualizację danych pod kątem ich analizy. System musi umożliwiać wizualizację przy wykorzystaniu m.in. interaktywnych wykresów i grafik ponadto system musi posiadać wbudowaną zaawansowaną wyszukiwarkę umożliwiającą odfiltrowywanie danych i ich wizualizację wg. wybranych kategorii (np. poziom istotności).

Alerty i Powiadomienia: CSB powinien umożliwiać konfigurację zaawansowanych scenariuszy powiadomień, które mogą być wysyłane poprzez e-mail, SMS, czy integracje z systemami biletowymi. Użytkownicy powinni mieć możliwość ustawiania różnych poziomów priorytetów dla alertów, a także definiowania eskalacji dla poważniejszych problemów.

Raportowanie: CSB powinien umożliwiać użytkownikom generowanie szczegółowych raportów dotyczących wydajności i dostępności monitorowanych systemów.

Wsparcie dla Szyfrowania: CSB musi być systemem bezpiecznym, umożliwiającym szyfrowaną komunikację między agentami a serwerem, co zapewnia bezpieczeństwo danych monitorowania.

Skalowalność: Architektura CSB powinna być zaprojektowana z myślą o skalowalności, co powinno pozwalać na łatwą adaptację do rosnących wymagań w miarę rozwoju infrastruktury IT.

Przetwarzanie i Wyszukiwanie Danych: CSB pod kątem agregacji logów musi być oparty na technologii, która umożliwia indeksowanie, wyszukiwanie i analizowanie dużych ilości danych w czasie rzeczywistym. Użytkownicy powinni móc wykonywać skomplikowane zapytania, aby szybko odnaleźć konkretne informacje.

Szybkość i Wydajność: Zaprojektowany do szybkiego przetwarzania dużych ilości danych, co jest kluczowe w środowiskach produkcyjnych z intensywnym ruchem danych.

Elastyczne Zbieranie Danych: CSB musi gromadzić dane z różnych źródeł jednocześnie (co najmniej urządzenia sieciowe, serwery, urządzenia klienckie).



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

Przetwarzanie i Wzbogacanie Danych: CSB musi posiadać bogaty zestaw filtrów do przetwarzania danych.

Odkrywanie i Analiza Danych: System musi umożliwiać użytkownikom przeszukiwanie, przeglądanie i analizowanie zgromadzonych danych ułatwiając identyfikację wzorców i trendów.

Wsparcie dla Wielu Platform: CSB musi być kompatybilny z wieloma systemami operacyjnymi, co najmniej Linux, Windows, macOS.

Treści pojawiające się w interfejsie użytkowników CSB będą spełniać standardy WCAG 2.1 na poziomie AA.

Cały interfejs użytkownika powinien być dostosowany pod aktualne wymagania prawne związane z dostępnością serwisów użyteczności publicznej dla osób z niepełnosprawnościami.

Na podstawie uzyskanych efektów serwis będzie mógł być udostępniony publicznie.

Treści multimedialne muszą być dostępne z poziomu klawiatury i oprogramowania dla osób niepełnosprawnych. Multimedia, które nie mogą być z przyczyn technicznych tak zbudowane, by uczynić je dostępnymi dla wszystkich użytkowników muszą posiadać alternatywny opis tekstowy, który wyjaśnia ich cel i funkcje zastosowania na stronie.

Zgodność ze standardami HTML i CSS całego serwisu www.

Kontrast kolorystyczny między tłem, a tekstem musi być zgodny z zaleceniami WCAG 2.1 AA.

System CSB musi rejestrować zdarzenia akcje i reakcje użytkowników w CSB. Historia akcji poszczególnych użytkowników musi być raportowana i możliwa do odtworzenia w logach systemowych – chronologicznie.

System musi posiadać budowę modułową, która będzie umożliwiać dodawanie nowych modułów oraz wyłączanie już uruchomionych. Dostarczony i uruchomiony system będzie posiadał co najmniej moduły:

1. MODUŁ ANALIZY PODATNOŚCI

1.1. Integracja ze stale aktualizowaną bazą danych CVE (Common Vulnerabilities and Exposures), gromadzącą informację na temat podatności urządzeń i oprogramowania.

System musi być zintegrowany z publicznym i stale aktualizowanym rejestrem gromadzącym i udostępniającym informację na temat znanych podatności w urządzeniach obsługiwanych przez system oraz oprogramowaniu zainstalowanym na urządzeniach Zamawiającego (np. UTM).



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

Połączenie z bazą danych CVE odbywać się ma przy wykorzystaniu udostępnionego API i nie powinno wymagać od użytkowników końcowych konfiguracji.

Synchronizacja z bazą CVE oraz sprawdzenie dodania do niej nowych podatności dotyczących sprzętu i oprogramowania zainstalowanego w infrastrukturze sieciowej jednostki musi odbywać się przynajmniej raz dziennie. Po zalogowaniu do CSB i wybraniu modułu analizy podatności powinny być wyświetlane wszystkie zsynchronizowane informacje wraz z danymi historycznymi. Podatności “nowe”, których użytkownik wcześniej nie widział powinny być w systemie oznaczone np. poprzez pogrubioną czcionkę lub inny kolor.

1.2. Automatyczne sprawdzenie możliwości występowania podatności w infrastrukturze sieciowej na podstawie zinwentaryzowanych urządzeń i oprogramowania.

System musi automatycznie sprawdzać możliwość wystąpienia nowej podatności tylko na urządzeniach i oprogramowaniu znajdującym się w infrastrukturze sieciowej jednostki, a dokładniej wyszczególnionych (dodanych) w module inwentaryzacji.

1.3. Powiadamianie użytkownika o nowych podatnościach występujących w jego środowisku IT.

System musi informować użytkownika/administrатора o nowych podatnościach występujących w infrastrukturze sieciowej jednostki. System powinien posiadać możliwość włączenia powiadomień na przeglądarkę internetową oraz wskazany przez użytkownika/administratora adres e-mail. Ponadto użytkownik po zalogowaniu się do systemu i wybraniu modułu analizy podatności musi być powiadomiony przez system o występujących nowych podatnościach na poszczególnych hostach infrastruktury sieciowej poprzez np. graficzne wyróżnienie hosta i oprogramowania na nim zainstalowanego. System musi informować użytkownika o treści podatności oraz jej sklasyfikowania (np. podatność krytyczna).

2. MODUŁ MONITORINGU ZASOBÓW

2.1. Monitorowanie zasobów hostów na podstawie zinwentaryzowanych w systemie urządzeń (monitoring obciążenia dysków, procesorów, ruchu sieciowego itp.)

System musi posiadać możliwość monitorowania zasobów wszystkich hostów dodanych w module inwentaryzacji. Monitorowanie, zbieranie informacji na temat obciążenia wybranego hosta musi odbywać się w sposób ciągły w ustalonych krótkich (co najmniej minutowych) odstępach czasowych. Użytkownik po zalogowaniu się do systemu i wybraniu modułu inwentaryzacji musi mieć możliwość wyświetlenia w formie graficznej (wykresów), przebiegów czasowych istotnych parametrów hosta, co najmniej takich jak: obciążenie procesora, obciążenie pamięci, obciążenie dysków, obciążenie ruchu sieciowego, skoki na procesorze, czas oczekiwania na dysk i odczyt i zapis na dysku. Ponadto system musi na bieżąco informować o aktualnym statusie hosta (dostępny, niedostępny).

2.2. Grupowanie hostów i korelacja obciążeń zasobów pomiędzy hostami



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

System musi mieć możliwość wyświetlania zgrupowanych wykresów hostów należących do tej samej grupy. Hosty muszą być pogrupowane w zasugerowany przez administratora sieci sposób w celu skorelowania ze sobą istotnych parametrów zasobów, co umożliwi porównanie zachowań poszczególnych hostów na tle grupy. Hosty powinny być podzielone co najmniej, na urządzenia sieciowe (np. serwery) oraz urządzenia końcowe (np. komputery pracowników). Użytkownik musi mieć możliwość filtrowania wykresów na poziomie poszczególnych hostów, oraz tworzenia w systemie nowych grup i wykresów parametrów dostępnych z wybieralnej listy.

2.3. Wysyłanie alertów i powiadomień dotyczących problemów i zdarzeń występujących na hostach

System musi posiadać funkcjonalność umożliwiającą użytkownikowi/administratorowi skonfigurowanie wysyłania alertów i powiadomień dotyczących problemów i zdarzeń. W systemie musi być możliwość ustawienia wysyłania wiadomości i powiadomień, poprzez wysyłanie komunikatów na przeglądarkę internetową, wysyłanie wiadomości e-maili lub wiadomości sms (w systemie powinna być możliwość dodania bramki sms - Zamawiający dopuszcza wykorzystanie autorskiej bramki sms lub wskazać zew. bramkę/serwis sms). Wysyłane przez system wiadomości muszą zawierać co najmniej informacje na temat występującego zdarzenia/problemu tj. opis, sklasyfikowanie (np. błąd, ostrzeżenie, informacja), data i godzina. Użytkownik/Administrator powinien mieć możliwość ustawienia odbiorcy wiadomości poprzez podanie adresu e-mail, czy w przypadku wiadomości SMS numeru telefonu. Użytkownik musi mieć możliwość wyboru w systemie, przy jakiego typu zdarzeniach i problemach będzie wysyłana wiadomość.

2.4. Funkcja korelacji występujących problemów na hostach z modułem analizy logów

Moduł monitoringu zasobów oprócz przebiegów czasowych parametrów hostów powinien również zawierać informację na temat występujących problemów i zdarzeń na poszczególnych hostach. Użytkownik/Administrator po zalogowaniu się do systemu, wybraniu Modułu Monitoringu zasobów i wyborze konkretnego hosta musi posiadać możliwość prześledzenia zdarzeń i problemów naniesionych na osi czasu. Na osi czasu powinny być wyświetlane tylko “nowe” problemy i zdarzenia oraz te, których status nie został zmieniony na “rozwiązany” bądź “anulowany”. Użytkownik/Administrator musi mieć możliwość zmiany statusu wybranego zdarzenia czy problemu wraz z dodaniem krótkiego opisu w jaki sposób problem został rozwiązany. Użytkownik/Administrator musi mieć możliwość stłumienia często powielającego się problemu, którego jest świadomy i musi poczekać na jego rozwiązanie (po włączeniu opcji tłumienia problemu, system przez pewien czas nie będzie o nim informował/alertował). Wszystkie problemy i zdarzenia raportowane w systemie muszą być skorelowane z logami pochodzącymi z konkretnych hostów. Użytkownik/Administrator po wybraniu w systemie konkretnego problemu występującego na konkretnym hoście po wybraniu zakładki logi musi zostać przekierowany do modułu analizy logów, w którym automatycznie wyświetlone będą tylko logi dotyczące hosta na którym wystąpił problem. Ponadto użytkownik/administrator w ramach tego modułu powinien mieć możliwość



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

zgłoszenia wystąpienia konkretnego problemu do np. zewnętrznego wsparcia IT. W systemie powinna być możliwość integracji systemu z zewnętrznym systemem typu: “help-desk”, przynajmniej poprzez podanie adresu e-mail, na który zostanie wysłane zgłoszenie.

2.5. Kategoryzacja istotności zdarzeń występujących w infrastrukturze sieciowej

Wszystkie zdarzenia i problemy raportowane w systemie muszą być skategoryzowane według ich poziomu istotności (priorytetów). W systemie powinny być identyfikowane problemy z priorytetami w co najmniej 4 stopniowej skali, np: Krytyczny, Wysoki, Średni, Niski. Ponadto, system powinien zapewniać dodatkowe dwa priorytety - zdarzenia nie istotne powinny być również sklasyfikowane w systemie jako informacja, a zdarzenia trudne do sklasyfikowania powinny posiadać priorytet o wartości (niesklasyfikowany).

2.6 Lista predefiniowanych zdarzeń najczęściej występujących w środowiskach IT

System musi być wyposażony w listę wcześniej zdefiniowanych zdarzeń/scenariuszy, które najczęściej występują w środowiskach IT. Użytkownik/Administrator powinien mieć możliwość wybrania konkretnego hosta lub grupy hostów i przypisania im predefiniowanych zdarzeń (np. brak miejsca na dyskach, czy zbyt wysoki ruch sieciowy). W predefiniowanych zdarzeniach/scenariuszach użytkownik/administrator powinien mieć możliwość ustawienia/edycji reguł oraz zmiany wykonywanych operacji, gdy warunki reguł zostaną spełnione. Użytkownik powinien mieć możliwość używania w regułach operatorów logicznych takich jak AND i OR oraz operatorów relacyjnych takich jak: “==”, “<=”, “>=”, “!=”. Użytkownik/Administrator systemu musi mieć możliwość ustawienia operacji różnego typu takich jak.: wysłanie wiadomości e-mail, wysłanie wiadomości SMS (Zamawiający dopuszcza wykorzystanie autorskiej bramki sms lub wskazać zew. bramkę/serwis sms), wysłanie zapytania (Request), czy uruchomienie predefiniowanego skryptu.

2.7 Dobór oraz dodawanie zdarzeń do konkretnego środowiska IT

System musi umożliwiać użytkownikowi/administratorowi dodawanie własnych zdarzeń/scenariuszy dostosowanych do jego konkretnych potrzeb. Tworzenie nowego zdarzenia w systemie powinno się odbywać poprzez podanie jego unikalnej nazwy, wybranie hosta lub grupy hostów, których dotyczy tworzone zdarzenie, zdefiniowanie warunków opisujących zdarzenie, oraz podanie operacji jakie mają być wykonane, gdy warunki zostaną spełnione. Warunki powinny korzystać z operatorów logicznych takich jak AND i OR oraz operatorów relacyjnych takich jak: “==”, “<=”, “>=”, “!=”. Użytkownik/Administrator systemu musi mieć możliwość ustawienia operacji różnego typu takich jak.: wysłanie wiadomości e-mail, wysłanie wiadomości SMS (Zamawiający dopuszcza wykorzystanie autorskiej bramki sms lub wskazać zew. bramkę/serwis sms), wysłanie zapytania (Request), czy uruchomienie predefiniowanego skryptu.



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

2.8 Zdalny dostęp do urządzeń końcowych

System musi umożliwiać zdalne połączenie się do wybranego hosta/urządzenia, które zostało wcześniej odpowiednio skonfigurowane. Zdalny dostęp musi odbywać się poprzez przeglądarkę internetową bez konieczności instalowania dodatkowego oprogramowania. Połączenie zdalne musi być możliwe przy wykorzystaniu co najmniej dwóch protokołów, konkretnie RDP i SSH.

2.9 Wywoływanie predefiniowanych skryptów na urządzeniach końcowych

System musi dawać możliwość wywołania podstawowych skryptów na hostach końcowych, na których został zainstalowany jego agent. Predefiniowane w systemie skrypty muszą obejmować co najmniej: wyłączenie i restart hosta, wysłanie wiadomości tekstowej do hosta, włączenie i wyłączenie blokady ruchu sieciowego, włączenie i wyłączenie trybu izolacji z infrastruktury sieciowej hosta z możliwością zdalnego połączenia się z nim.

2.10 Analiza ruchu sieciowego

System musi posiadać możliwość śledzenia logów pochodzących z urządzeń sieciowych typu UTM zwłaszcza tych najczęściej używanych i polecanych w środowiskach informatycznych. Użytkownik systemu/administrator musi mieć możliwość filtrowania wyświetlanych informacji, co najmniej poprzez podanie przedziału czasowego i wyboru nazwy zinwentaryzowanego urządzenia typu UTM.

2.11 Monitorowanie problemów i zdarzeń występujących na drukarkach

System musi umożliwiać monitorowanie problemów występujących na drukarkach sieciowych wykorzystujących protokół SNMP. System powinien zbierać informacje na temat występujących problemów w osi czasu, umożliwiać tłumienie problemów, wskazywać ich istotność. Ponadto w systemie powinny znajdować się możliwe do pobrania wartości parametrów drukarki oraz informacji na temat dostępności urządzenia.

3. MODUŁ ANALIZY LOGÓW

3.1. Przegląd i analiza logów pochodzących z inwentaryzowanych urządzeń/maszyn.

Moduł Analizy Logów i Moduł Monitoringu Zasobów musi być powiązany z Modułem Inwentaryzacji i wykorzystywać informację przez niego posiadane. Użytkownik/Administrator systemu musi posiadać możliwość przeglądania i analizowania logów pochodzących z wszystkich hostów dodanych w Module inwentaryzacji. W ramach modułu system musi agregować logi pochodzące z systemów operacyjnych, aplikacji i systemów dziedzinowych. Agregacja logów



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

powinna odbywać się w sposób ciągły i po osiągnięciu limitu związanego z zasobami dyskowymi serwera nadpisywać historyczne logi, począwszy od najstarszych.

3.2. Możliwość analizy tzw. „customowych” logów pochodzących z dowolnego oprogramowania, w tym systemów dziedzicznych.

System musi posiadać możliwość analizy logów pochodzących z dowolnego oprogramowania, a przede wszystkim z oprogramowania dziedzicznego stosowanego przez Zamawiającego. Użytkownik/Administrator musi mieć możliwość dodawania w module nazwy, lokalizacji i typu tzw. „customowych” logów, które będą agregowane w systemie, w celu późniejszej ich analizy. Zdefiniowane przez Użytkownika/Administratora logi powinny być skorelowane z problemami występującymi na hostach w module monitoringu zasobów. Jeśli wystąpi jakiś problem związany z działaniem np. systemu dziedzicznego, to użytkownik/administrator analizując problemy musi mieć opcję automatycznego przekierowania do logów związanych z tym systemem.

3.3. Zaawansowane filtrowanie, zarówno po hostach jak i zainstalowanym na nich oprogramowaniu.

Moduł analizy logów musi być wyposażony w zaawansowaną wyszukiwarkę umożliwiającą użytkownikowi/administratorowi wyszukiwanie i filtrowanie konkretnych logów. System powinien umożliwiać odfiltrowanie logów dla konkretnego hosta, grupy hostów, oprogramowania (w szczególności oprogramowania dziedzicznego - „customlogów”), kategorii, dowolnie wpisanej frazy oraz zakresu czasu (data – godzina, od -do). W Systemie muszą być zastosowane mechanizmy stronicowania, umożliwiające płynne przeglądanie dużej ilości informacji.

3.4. Przegląd i analiza logów dotyczących działań użytkowników.

W module analizy logów muszą być agregowane logi dotyczące działań użytkowników. W zależności od rodzaju systemu czy oprogramowania zainstalowanego na hoście w logach znajdują się informacje dotyczące różnej aktywności użytkowników (m.in. data zalogowania się użytkownika do systemu, data wylogowania, czy wybór konkretnej funkcjonalności). Użytkownik/Administrator CSB musi mieć możliwość sprawdzenia tych aktywności poprzez wyszukanie i odfiltrowanie logów po nazwie użytkownika, typie aktywności, czy dowolnie wpisanej frazie.

3.6. Dostęp do logów historycznych.

System oprócz dostępu do aktualnych logów musi uwzględniać również logi historyczne. Użytkownik/Administrator musi mieć możliwość przeglądania wszystkich logów agregowanych na zasobach dyskowych. Ilość oraz zakres czasowy agregowanych logów limitowany ma być tylko



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

zarezerwowaną przestrzenią dyskową na serwerze. Po osiągnięciu założonego limitu, system powinien nadpisywać logi poczynawszy od najstarszych. Użytkownik/Administrator podobnie jak w przypadku logów aktualnych musi mieć możliwość przeszukiwania oraz filtrowania logów historycznych po hostach, oprogramowaniu, czasie i dowolnie wpisanej frazie.

3.7. Informowanie i powiadomienia dotyczące pojawienia się nowych istotnych logów w obrębie całej infrastruktury sieciowej.

System musi być wyposażony w mechanizmy powiadamiające użytkownika/administratora o pojawieniu się istotnych logów pochodzących z urządzeń infrastruktury sieciowej. System musi posiadać możliwość konfiguracji tych powiadomień pod kątem istotności pojawiającego się wpisu w logach oraz wyboru typu logu (m.in. log systemowy, log “customowy”). Ponadto CSB musi informować użytkownika/administratora o “nowych” zagregowanych logach z poszczególnego hosta. Informacja ta powinna być wyświetlana w systemie po zalogowaniu użytkownika/administratora, a “nowe” logi to logi dodane do systemu od czasu ostatniego logowania użytkownika/administratora.

3.8. Kategoryzacja istotności logów (np.: informacja, ostrzeżenie, błąd).

System musi być wyposażony w mechanizmy kategoryzujące logi pod kątem ich istotności. System w szczególności powinien informować użytkownika/administratora o pojawieniu się logów dotyczących nieprawidłowości działania poszczególnych hostów, czy oprogramowania na nich zainstalowanych. Następnie w zależności od potrzeb użytkownika/administratora system powinien informować o pojawieniu się ostrzeżeń w oprogramowaniu kluczowym dla użytkownika. Jeśli log dotyczy tylko informacji takiej jak zalogowanie się, czy wyłączenie hosta, to użytkownik/administrator nie powinien otrzymywać powiadomienia (alertu), z wyjątkiem logów które użytkownik/administrator uzna za istotne (pomimo tego, że są skategoryzowane jako informacja).

4. MODUŁ EDR/XDR

4.1 System musi posiadać własny moduł EDR/XDR, czyli zintegrowane rozwiązanie bezpieczeństwa, którego główne funkcje to: monitorowanie i gromadzenie danych o aktywnościach użytkowników i oprogramowania na urządzeniach końcowych, analiza tych danych w celu identyfikacji wzorców zagrożeń, automatyczne reagowanie na zidentyfikowane zagrożenia w celu ich usunięcia lub powstrzymania, powiadamianie personelu bezpieczeństwa o zidentyfikowanych anomaliach.

4.2 Moduł posiadać podgląd informacji, alertów i zdarzeń występujących w środowisku IT. W CSB powinna być możliwość podglądu statystyk incydentów/zdarzeń oraz ich



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

kategorie. Użytkownik/Administrator z poziomu CSB powinien mieć możliwość uzyskania takich informacji jak rodzaj, nazwa lub źródło incydentu, opis, data wykrycia oraz kategoria/priorytet.

4.3 Oprócz posiadanego modułu EDR/XDR, system musi być otwarty tj. posiadać możliwość integracji z rozwiązaniami EDR/XDR innych producentów (co najmniej ESET, WithSecure, Bitdefender). System musi umożliwiać bezpośrednie przekierowanie do zaawansowanych opcji zintegrowanego systemu EDR/XDR (panelu administracyjnego). Dzięki integracji w module musi znajdować się funkcjonalność umożliwiająca użytkownikowi/administratorowi przejście do panelu administracyjnego systemu EDR/XDR udostępniającego zaawansowane opcje.

5. MODUŁ INWENTARYZACJI

5.1 Automatyczny (przy wykorzystaniu agentów), półautomatyczny (przy wykorzystaniu pliku CSV) lub ręczny sposób dodawania hostów oraz oprogramowania zainstalowanego w infrastrukturze sieciowej.

System musi dawać użytkownikowi/administratorowi możliwość dodawania hostów/urządzeń/oprogramowania należących do infrastruktury sieciowej na trzy różne sposoby. Pierwszy dotyczy automatycznego wykrywania i dodawania przy wykorzystaniu usług katalogowych. Wszystkie hosty i urządzenia należące do wybranej domeny powinny być automatycznie dodane do CSB wraz z zainstalowanym na nich oprogramowaniem. Drugi i trzeci sposób natomiast ma umożliwiać użytkownikowi/administratorowi dodanie urządzeń/hostów/oprogramowania nie należących do domeny poprzez “ręczne” wpisanie informacji (wypełnienie formularza) lub wczytanie pliku w formacie CSV posiadającego usystematyzowaną strukturę. Moduł inwentaryzacji musi być ściśle skorelowany (powiązany) z pozostałymi modułami systemu CSB.

5.2 Gromadzenie pełnych informacji na temat urządzeń (tj. nazwa hosta, adres IP, główny użytkownik) jak i oprogramowania (nazwa, wersja)

Informacje o urządzeniach/hostach/oprogramowaniu, które muszą znaleźć się zarówno w formularzu jak i pliku CSV to m.in. dla hosta/urządzenia: nazwa, adres IP, przypisany użytkownik, typ urządzenia/hosta oraz lista zainstalowanego na nim oprogramowania wraz z wersjami. Przy wprowadzaniu “ręcznym” system musi umożliwiać użytkownikowi/administratorowi wybór nazwy i wersji oprogramowania z listy znajdującej się bazie CVE, bądź wpisanie własnych wartości.

5.3. Generowanie raportu w formacie PDF, CSV zawierającego aktualne informacje na temat urządzeń oraz oprogramowania zainstalowanego w infrastrukturze sieciowej.



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

Moduł musi być wyposażony w funkcjonalności umożliwiającą użytkownikowi/administratorowi wygenerowania raportów z całej dodanej w systemie CSB infrastruktury sieciowej. Raporty powinny być generowane w co najmniej dwóch formatach tj. PDF i CSV oraz powinny zawierać wszystkie istotne informacje na temat urządzenia/hosta/oprogramowania m. in. takie jak: nazwa, adres, główny użytkownik, lista oprogramowania wraz z wersjami. Ponadto raport musi zawierać m.in. datę i godzinę wygenerowania, nazwę jednostki organizacyjnej oraz imię i nazwisko osoby generującej raport. Dokładny wzór (wizualny) generowanego raportu zostanie ustalony przez zamawiającego w trakcie realizacji zamówienia. Moduł musi umożliwiać generowanie raportów zarówno z całości jak i z odfiltrowanych urządzeń/hostów/oprogramowania. Użytkownik/Administrator musi mieć możliwość odfiltrowania informacji według co najmniej takich kategorii jak: nazwa użytkownika, grupa urządzeń, dowolnie wpisana fraza.

6. MODUŁ ZGŁASZANIA INCYDENTÓW (e-mail, system help-deskowy)

6.1. Integracja z systemem tiketowym.

System CSB musi w prosty i intuicyjny sposób umożliwiać użytkownikowi/administratorowi integrację z systemem typu: help-desk. Integracja powinna odbywać się poprzez ustawienie w konfiguracji CSB odpowiedniego adresu e-mail systemu help-deskowego, na który będą wysyłane zgłoszenia dotyczące problemów. Wysyłanie wiadomości ma się odbywać automatycznie po wybraniu przez użytkownika/administratora konkretnego zdarzenia w systemie CSB. Wiadomość e-mail powinna zawierać minimum nazwę jednostki organizacyjnej wysyłającej zgłoszenie, treść zgłoszenia oraz dane zgłaszającego: Imię Nazwisko, adres e-mail, numer telefonu.

6.2. Zgłaszanie incydentu/problemu, który został namierzony przez system.

Moduł zgłaszania incydentu powinien być ściśle powiązany z modułem monitoringu zasobów, a dokładniej z funkcjonalnością wyświetlającą zidentyfikowane na urządzeniach/hostach problemy. Użytkownik/Administrator systemu powinien posiadać możliwość wyboru problemu namierzonego przez CSB i automatycznego zgłoszenia go do help-desk, poprzez wybranie np. przycisku “Zgłoś Problem”. Po wybraniu opcji zgłoszenia system powinien automatycznie wysłać do systemu tiketowego zgłoszenie zawierające pełne informacje dotyczące wybranego problemu.

6.3. Bezpośrednie zgłaszane zagrożeń/cyberataków do CSIRT NASK.

System powinien umożliwiać generowanie co najmniej pliku w formacie pdf ze zgłoszeniem zagrożenia/incydentu/ cyberataku zgodnego z formularzem udostępnianym przez NASK.

7. MODUŁ WYKRYWANIA ZAGROŻEŃ



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

7.1. Wykrywanie zagrożeń na podstawie powszechnie znanych taktyk i technik wykorzystywanych przez cyberprzestępców udostępnione w ogólnodostępnej bazie danych MITRE ATT&CK.

System musi umożliwiać użytkownikowi/administratorowi włączenie reguł sprawdzających, czy w jego infrastrukturze sieciowej nie zostały zastosowane taktyki i techniki różnego rodzaju cyberataków. System musi być zintegrowany z powszechnie dostępną bazą danych MITRE ATT&CK zawierającą zbiór taktyk i technik zaobserwowanych przez specjalistów na całym świecie. System powinien posiadać wbudowane reguły umożliwiające wykrycie wielu zagrożeń opisanych w macierzy MITRE ATT&CK, system powinien wskazywać użytkownikowi, przed jakim rodzaju taktykami i technikami jest chronione jego środowisko IT. System musi pokazywać ilość wbudowanych w nim reguł wraz z ilością włączonych reguł. Użytkownik/Administrator systemu musi mieć możliwość sprawdzenia w systemie ile reguł dotyczących konkretnej techniki jest włączonych, a ile jeszcze pozostało do wyłączenia. System musi pokazywać pokrycie macierzy MITRE ATT&CK ilościom włączonych/wyłączonych reguł wykrywających cyberzagrożenia.

7.2. Kategoryzacja oraz prezentacja wykrytych zagrożeń

System musi umożliwiać użytkownikowi/administratorowi sprawdzenie zagrożeń wykrytych na poszczególnych hostach/urządzeniach zinwentaryzowanych w module inwentaryzacji. Wykryte w systemie zagrożenia muszą zawierać informację na temat: daty i czasu ich wystąpienia, rodzaju/treści oraz poziomu istotności. System powinien kategoryzować zagrożenia w co najmniej czterostopniowej skali: poziom zagrożenia niski, średni, wysoki, krytyczny.

7.3. Historia wykrytych zagrożeń

System musi posiadać możliwość sprawdzenia historii występowania zagrożeń na hostach/urządzeniach. System musi być wyposażony w rozbudowaną wyszukiwarkę hostów i zagrożeń umożliwiającą między innymi: wyszukanie hosta po nazwie, adresie IP, kategorii/priorytetów, daty wykrycia (przedziału czasowego).

7.4. Wsparcie/automatyczna ochrona po wykryciu zagrożenia

System musi posiadać możliwość włączenia „automatycznej ochrony” w wybrane dni tygodnia i w wybranych godzinach. Użytkownik/administrator musi mieć możliwość ustawienia automatycznej ochrony przed wybranymi taktykami i technikami działań cyberprzestępców poza godzinami jego pracy. System musi mieć możliwość ustawienia reakcji na wykrycie zagrożenia w zależności od wybranego poziomu istotności/priorytetu. Ponadto użytkownik/administrator musi mieć możliwość wybrania operacji/akcji z listy predefiniowanych operacji/akcji, która zostanie wykonana w razie wykrycia zagrożenia o wybranym priorytecie. Lista operacji/akcji musi umożliwiać co najmniej wyłączenie/restart hosta/urządzenia na którym wykryto zagrożenie, przesłanie informacji o wystąpieniu zagrożenia do użytkownika/administradora przy wykorzystaniu poczty e-mail bądź bramki sms, blokowanie hosta na którym występuje zagrożenie.



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

8. MODUŁ RAPORTÓW

8.1. Tworzenie zestawień i raportów z danych pochodzących z pozostałych modułów

System musi posiadać możliwość tworzenia różnego rodzaju zestawień prowadzących do sporządzenia i wyeksportowania raportu w co najmniej dwóch formatach: csv, pdf. Podczas tworzenia zestawienia użytkownik/administrator musi mieć możliwość wyboru konkretnych hostów bądź grupy hostów, dla których tworzony jest raport. Użytkownik musi posiadać możliwość wyboru modułów oraz priorytetów zdarzeń w nich występujących. Ponadto użytkownik przez administratora musi mieć możliwość wyboru przedziału czasowego, dla którego zostanie wykonany raport.

9. PANEL UŻYTKOWNIKA

9.1. Intuicyjny i przejrzysty panel użytkownika dostępny z dowolnej lokalizacji poprzez stronę www.

Panel użytkownika CSB powinien być przejrzysty i intuicyjny oraz wykonany przy wykorzystaniu najnowszych standardów i technologii stosowanych we współczesnych systemach informatycznych. Panel użytkownika/administratora systemu musi być dostępny poprzez podanie odpowiedniego adresu w przeglądarce internetowej. Dostęp do panelu użytkownika musi być bezpieczny poprzez szyfrowanie (zabezpieczenie certyfikatem SSL) oraz tzw. białą listę adresów IP - która pozwala użytkownikowi/administratorowi systemu blokować dostęp z nie znajdujących się na niej adresów. Panel użytkownika powinien również spełniać wymagania związane z dostępnością serwisów użyteczności publicznej dla osób z niepełnosprawnościami - WCAG 2.1 AA.

9.2. Wizualizacja statystyk zdarzeń i logów

Panel użytkownika CSB, powinien posiadać elementy umożliwiające prezentację statystyk zdarzeń i logów w sposób zrozumiały, ułatwiający analizę działania środowiska IT pod kątem cyberbezpieczeństwa. Wizualizacja statystyk zdarzeń i logów powinna dotyczyć przede wszystkim ilości “nowych” zdarzeń zarejestrowanych w systemie z podziałem na ich kategorię. Natomiast sposób prezentacji samych logów i zdarzeń musi być przejrzysty jasno podkreślający sklasyfikowanie zdarzenia czy wpisu do logów. Zdarzenia i logi powinny w systemie być wyświetlane w kolejności od najnowszych do najstarszych z możliwości odfiltrowania zakresu czasowego ich prezentowania.

9.3. Wykresy zdefiniowanych parametrów zasobowych aktualizowane na „żywo”.



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

Wykresy prezentujące parametry zasobów urządzeń/hostów powinny być aktualizowane w systemie na “żywo”, a dokładnie w zależności od ustaleń z zleceniodawcą system musi aktualizować wykresy w określonych odstępach czasowych (co najmniej, co minutę).

9.4. Filtrowanie wyświetlanych danych wg. hostów, oprogramowania, kategorii zdarzeń itd.

Panel użytkownika powinien być tak zaprojektowany, aby użytkownik/administrator w sposób intuicyjny mógł filtrować istotne dla niego informacje dotyczące zarówno obciążeń zasobów, zdarzeń (problemów, ostrzeżeń), czy logów. Panel użytkownika musi być wyposażony w wyszukiwarkę umożliwiającą filtrowanie informacji wg. m.in. nazwy hosta/urządzenia, nazwy oprogramowania czy kategorii zdarzeń i logów. Wyszukiwarka w panelu użytkownika powinna znajdować się w widocznym miejscu i posiadać precyzyjnie oznaczone możliwości filtrowania. Użytkownik/Administrator powinien mieć możliwość nakładania na siebie różnych filtrów.

9.5. Intuicyjny panel zarządzania regułami i definiowania “customowych” logów.

Panel użytkownika powinien być wyposażony w przejrzysty i intuicyjny panel zarządzania regułami (akcjami), na podstawie których użytkownik/administrator informowany jest o zaistniałym w środowisku IT problemie. W panelu tym musi znaleźć się między innymi lista już zdefiniowanych reguł z możliwością ich usunięcia i edycji oraz opcja umożliwiająca dodanie nowej reguły. Reguły w panelu użytkownika powinny być dodawane przy wykorzystaniu przejrzystego i intuicyjnego formularza, w którym użytkownik/administrator musi podać nazwę reguły, dodać warunku oraz wybrać rodzaj operacji, która zostanie wykonana, gdy warunki będą spełnione. Użytkownik/administrator CSB musi mieć możliwość wyboru zarówno warunków, reguł jak i operacji z udostępnionych w systemie opcji. Ponad to panel użytkownika musi być wyposażony w panel zarządzania “customowymi” logami, w którym podobnie jak w przypadku reguł, użytkownik/administrator może wyświetlić listę zdefiniowanych “customlogów” wraz z możliwością ich usunięcia, edycji oraz zdefiniowania nowych. Dodanie do systemu “customlogów” musi być intuicyjne i ma polegać na podaniu unikalnej nazwy definiowanych logów, jego ścieżki (lub ścieżek) dostępu oraz nazwy hosta lub grupy hostów, których ma on dotyczyć.



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

2. UTM – 2 szt.;

Zamawiający wymaga dostawy, instalacji i konfiguracji 2 szt. urządzeń klasy UTM w podziale na 2 typu (szczegółowo opisane poniżej). Dla obu typów urządzeń Zamawiający stawia te same wymagania dot. gwarancji tj.:

Gwarancja

System musi być objęty serwisem gwarancyjnym producenta przez okres min 24 miesiące, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. **(długość gwarancji stanowi kryterium oceny ofert, deklarowaną długość gwarancji, należy podać w formularzu ofertowym).**

W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Typ 1 – 1 szt.:

Wymagania Ogólne

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. 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.

System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.

System wspiera protokoły IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klastery Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łącz sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: 10 portami Gigabit Ethernet RJ-45.
2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. System Firewall pozwala skonfigurować co najmniej 20 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System jest wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 Gbps.
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 1.4 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps.

Funkcje Systemu Bezpieczeństwa:

W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zaporę ogniową klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware.



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
13. Rozwiązanie posiada 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).

Polityki, Firewall

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
 - Translację jeden do jeden oraz jeden do wielu.
 - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
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.
 - Amazon Web Services (AWS).
 - Microsoft Azure.
 - Cisco ACI.
 - Google Cloud Platform (GCP).
 - OpenStack.



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

- VMware NSX.
- Kubernetes.

Połączenia VPN

1. System umożliwia konfigurację połączeń typu IPsec VPN. W zakresie tej funkcji zapewnia:
 - Wsparcie dla IKE v1 oraz v2.
 - Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
 - Obsługa protokołu Diffie-Hellman grup 19, 20.
 - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
 - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
 - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
 - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
 - Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
 - Możliwość ustawienia maksymalnej liczby tuneli IPsec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
 - Możliwość monitorowania wybranego tunelu IPsec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
 - Obsługę mechanizmów: IPsec NAT Traversal, DPD, Xauth.
 - Mechanizm „Split tunneling” dla połączeń Client-to-Site.
2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:
 - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
 - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
 - Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPsec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPv2), OSPF (w tym OSPFv3), BGP oraz PIM.



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

Funkcje SD-WAN

1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

Zarządzanie pasmem

1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
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.
4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
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.
8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

Ochrona przed atakami

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

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 21).
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).



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

Kontrola WWW

1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
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.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:
 - Hasel statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
 - Hasel statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
 - Hasel dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

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.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

Logowanie

1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania, raportowania, korelacji zdarzeń, powiadamiania o incydentach i funkcję analizy logów archiwalnych względem aktualnej wiedzy producenta o zagrożeniach) udostępnianej w chmurze lub musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
3. W przypadku kiedy usługa logowania, raportowania, korelacji zdarzeń realizowana jest w chmurze, wykonawca musi dostarczyć stosowne licencje upoważniające do składowania logów przez okres co najmniej jednego roku.
4. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
5. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
6. Możliwość włączenia logowania per reguła w polityce firewall.
7. System zapewnia możliwość logowania do serwera SYSLOG.
8. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać ICSA lub EAL4 dla funkcji Firewall.

Typ 2 – 1 szt.:

Wymagania Ogólne

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. 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.

System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.

System wspiera protokoły IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klastery Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.

2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łącz sieciowych.

3. Monitoring stanu realizowanych połączeń VPN.

4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum 8 portami Gigabit Ethernet RJ-45 oraz minimum 2 portami współdzielonymi RJ-45/SFP

2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.

3. System Firewall pozwala skonfigurować co najmniej 20 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.

4. System jest wyposażony w zasilanie AC.



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

Parametry wydajnościowe:

1. W zakresie Firewall’a obsługa nie mniej niż 1.5 mln. jednoczesnych połączeń oraz 45 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 Gbps.
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 1.4 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 900 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 700 Mbps.

Funkcje Systemu Bezpieczeństwa:

W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
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.
11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
13. Rozwiązanie posiada 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).

Polityki, Firewall

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
 - Translację jeden do jeden oraz jeden do wielu.
 - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.

6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.

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.

- Amazon Web Services (AWS).
- Microsoft Azure.
- Cisco ACI.
- Google Cloud Platform (GCP).
- OpenStack.
- VMware NSX.
- Kubernetes.

Połączenia VPN

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:

- Wsparcie dla IKE v1 oraz v2.
- Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
- Obsługa protokołu Diffie-Hellman grup 19, 20.
- Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
- Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
- Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
- Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
- Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
- Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
- Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
- Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
- Mechanizm „Split tunneling” dla połączeń Client-to-Site.

2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:

· Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.

· Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.

· Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

1. Routingu statycznego.



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPv2), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

Funkcje SD-WAN

1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

Zarządzanie pasmem

1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
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.
4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
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.
8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

Ochrona przed atakami



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

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

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 21).
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).

Kontrola WWW

1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
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.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

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

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:
 - Hasła statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
 - Hasła statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
 - Hasła dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

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.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

Logowanie

1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania, raportowania, korelacji zdarzeń, powiadamiania o incydentach i funkcję analizy logów archiwalnych względem aktualnej wiedzy producenta o zagrożeniach) udostępnianej w chmurze lub musi zostać dostarczony



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.

3. W przypadku kiedy usługa logowania, raportowania, korelacji zdarzeń realizowana jest w chmurze, wykonawca musi dostarczyć stosowne licencje upoważniające do składowania logów przez okres co najmniej jednego roku.

4. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.

5. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.

6. Możliwość włączenia logowania per reguła w polityce firewall.

7. System zapewnia możliwość logowania do serwera SYSLOG.

8. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać ICSA lub EAL4 dla funkcji Firewall.

3. Serwer – 2 szt.:

Zamawiający wymaga dostawy, instalacji i konfiguracji 2 szt. serwerów w różnych konfiguracjach w podziale na typy – zgodnie z poniższymi minimalnymi wymaganiami. Dla obu typu serwerów Zamawiający stawia te same wymagania dot. gwarancji, tj.:

- a) Min. 2 lata gwarancji producenta serwera w trybie on-site z gwarantowaną wizytą technika do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. Dyski twarde nie podlegają zwrotowi organizacji serwisowej (**długość gwarancji stanowi kryterium oceny ofert, deklarowaną długość gwarancji, należy podać w formularzu ofertowym**).
- b) Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu;
- c) Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych;
- d) Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie;
- e) Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki.



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

Typ 1 – 1 szt.:

1) Obudowa

- a) Typu RACK, wysokość nie więcej niż 1U;
- b) Szyny umożliwiające wysunięcie serwera z szafy stelażowej.
- c) Możliwość zamontowania ramienia porządkującego ułożenie kabli z tyłu serwera;
- d) Możliwość zainstalowania 8 dysków twardych hot plug 2,5”;
- e) Fizyczne zabezpieczenie (np. na klucz lub elektrozamek) uniemożliwiające fizyczny dostęp do dysków twardych;
- f) Zainstalowane 2 szt. dysków SSD SATA 240GB, HOT-PLUG;
- g) Zainstalowane 4 szt. dysków SAS 12G 1,2TB, HOT-PLUG; 10000 RPM;
- h) Możliwość zainstalowania dedykowanego wewnętrznego napędu blu-ray.

2) Płyta główna

- a) Dwuprocesorowa;
- b) Wyprodukowana i zaprojektowana przez producenta serwera;
- c) Możliwość instalacji procesorów 60-rdzeniowych;
- d) Zainstalowany moduł TPM 2.0;
- e) 4 złącza PCI Express x16 w tym minimum 3 złącza generacji 5;
 - Opcjonalnie możliwość uzyskania złącza typu pełnej wysokości tzw. FH;
- f) 32 gniazda pamięci RAM;
- g) Obsługa 8 TB pamięci operacyjnej RAM DDR4;
- h) Wsparcie dla technologii:
 - Memory Scrubbing;
 - SDDC;
 - ECC;
 - Memory Mirroring;
 - ADDDC;
- i) Opcjonalna możliwość instalacji 2 dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) dyski nie mogą zajmować klatek dla dysków hot-plug.
- j) BIOS UEFI w specyfikacji 2.7.

3) Procesory

- a) Jeden procesor 8-rdzeniowy, taktowanie bazowe 1,8 GHz, osiągający w teście SPEC CPU2017 Floating Point wynik SPECrate2017_fp_base 258 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

na stronie <http://spec.org/cpu2017/results/cpu2017.html> dla dowolnego serwera dwuprocesorowego z oferty producenta oferowanego serwera.

4) Pamięć RAM

- a) 64 GB pamięci RAM;

5) Kontrolery LAN

- a) Interfejsy LAN, nie zajmujące żadnego z dostępnych slotów PCI Express:
 - i. 4x 1Gbit Base-T;
 - ii. Możliwość uzyskania czterech interfejsów 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe;
- b) Interfejsy LAN zainstalowane w slotach PCI-e:
 - i. 2x 10Gbit Base-T.

6) Kontrolery I/O

- a) Kontroler SAS RAID dla dysków wewnętrznych posiadający 2GB pamięci cache, obsługujący poziomy RAID: 0,1,10,5,50,6,60 z podtrzymaniem pamięci cache w przypadku utraty zasilania;

7) Porty

- a) Zintegrowana karta graficzna ze złączem VGA z tyłu serwera;
- b) 2 porty USB 3.0 dostępne z tyłu serwera;
- c) 2 porty USB 3.0 na panelu przednim;
- d) Opcjonalny port serial, możliwość wykorzystania portu serial do zarządzania serwerem;
- e) Ilość dostępnych złączy USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera.

8) Zasilanie, chłodzenie

- a) Redundantne zasilacze hotplug o sprawności 96% (tzw. klasa Titanium) o mocy nie większej niż 550W;
- b) Redundantne wentylatory hotplug.

9) Zarządzanie



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

- a) Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii;
- i. informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów:
- karty rozszerzeń zainstalowane w dowolnym slotcie PCI Express;
 - procesory CPU;
 - pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM;
 - wbudowany na płycie głównej nośnik pamięci M.2 SSD;
 - status karty zarządzającej serwerem;
 - wentylatory;
 - bateria podtrzymująca ustawienia BIOS płyty głównej;
 - zasilacze;
 - system przewidywania/rozpoznawania awarii musi być niezależny i działać w przypadku odłączenia kabli zasilających serwera (podtrzymywany kondensatorowo lub bateryjnie w celu uruchomienia przy odłączonym zasilaniu sieciowym);
- b) Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:
- i. Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;
 - ii. Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;
 - iii. Dostęp poprzez przeglądarkę Web, SSH;
 - iv. Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;
 - v. Zarządzanie alarmami (zdarzenia poprzez SNMP);
 - vi. Możliwość przejęcia konsoli tekstowej;
 - vii. Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM);
 - viii. Obsługa serwerów proxy (autentykacja);
 - ix. Obsługa VLAN;
 - x. Możliwość konfiguracji parametru Max. Transmission Unit (MTU);
 - xi. Wsparcie dla protokołu SSDP;
 - xii. Obsługa protokołów TLS 1.2, SSL v3;
 - xiii. Obsługa protokołu LDAP;
 - xiv. Integracja z HP SIM;
 - xv. Synchronizacja czasu poprzez protokół NTP;



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

- xvi. Możliwość backupu i odtwarzania ustawień bios serwera oraz ustawień karty zarządzającej;
- c) Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna);
 - d) Dedykowana, do wbudowania w kartę zarządzającą (lub zainstalowana) pamięć flash o pojemności minimum 16 GB;
 - e) Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN;
 - f) Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej.

10) Wspierane OS

- a) Microsoft Windows Server 2022, 2019;
- b) VMWare vSphere 8.0;
- c) Suse Linux Enterprise Server 15;
- d) Red Hat Enterprise Linux 9, 8;
- e) Microsoft Hyper-V Server 2019

11) Dokumentacja, inne

- a) 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.
- b) Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE.
- c) Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, **w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki;**
- d) W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji;
- e) Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

- f) Możliwość pracy w pomieszczeniach o wilgotności w zawierającej się w przedziale 10 - 85 %;
- g) Serwer musi być certyfikowany do pracy z systemem Ubuntu 22.04;
- h) Zgodność z normami: CB, RoHS, WEEE, GS oraz CE.

Typ 2 – 1 szt.:

1) Obudowa

- a) Typu RACK, wysokość nie więcej niż 1U;
- b) Szyny umożliwiające wysunięcie serwera z szafy stelażowej.
- c) Możliwość zamontowania ramienia porządkującego ułożenie kabli z tyłu serwera;
- d) Możliwość zainstalowania 8 dysków twardych hot plug 2,5”;
- e) Fizyczne zabezpieczenie (np. na klucz lub elektrozamek) uniemożliwiające fizyczny dostęp do dysków twardych;
- f) Zainstalowane 2 szt. dysków SSD SATA 240GB, HOT-PLUG;
- g) Zainstalowane 4 szt. dysków SAS 12G 1,2TB, HOT-PLUG; 10000 RPM;
- h) Możliwość zainstalowania dedykowanego wewnętrznego napędu blu-ray.

2) Płyta główna

- a) Dwuprocesorowa;
- b) Wyprodukowana i zaprojektowana przez producenta serwera;
- c) Możliwość instalacji procesorów 60-rdzeniowych;
- d) Zainstalowany moduł TPM 2.0;
- e) 4 złącza PCI Express x16 w tym minimum 3 złącza generacji 5;
 - Opcjonalnie możliwość uzyskania złącza typu pełnej wysokości tzw. FH;
- f) 32 gniazda pamięci RAM;
- g) Obsługa 8 TB pamięci operacyjnej RAM DDR4;
- h) Wsparcie dla technologii:
 - Memory Scrubbing;
 - SDDC;
 - ECC;
 - Memory Mirroring;
 - ADDDC;
- i) Opcjonalna możliwość instalacji 2 dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) dyski nie mogą zajmować klatek dla dysków hot-plug.
- j) BIOS UEFI w specyfikacji 2.7.



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

3) Procesory

- a) Jeden procesor 16-rdzeniowy, taktowanie bazowe 2,0 GHz osiągające w teście **SPEC CPU2017 Floating Point** wynik **SPECrate2017_fp_base 368 pkt** (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany na stronie <http://spec.org/cpu2017/results/cpu2017.html> dla dowolnego serwera dwuprocesorowego z oferty producenta oferowanego serwera.

4) Pamięć RAM

- a) 128 GB pamięci RAM;

5) Kontrolery LAN

- a) Interfejsy LAN, nie zajmujące żadnego z dostępnych slotów PCI Express:
 - i. 4x 1Gbit Base-T;
 - ii. Możliwość uzyskania czterech interfejsów 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe;
- b) Interfejsy LAN zainstalowane w slotach PCI-e:
 - i. 2x 10Gbit Base-T.

6) Kontrolery I/O

- a) Kontroler SAS RAID dla dysków wewnętrznych posiadający 2GB pamięci cache, obsługujący poziomy RAID: 0,1,10,5,50,6,60 z podtrzymaniem pamięci cache w przypadku utraty zasilania;

7) Porty

- a) Zintegrowana karta graficzna ze złączem VGA z tyłu serwera;
- b) 2 porty USB 3.0 dostępne z tyłu serwera;
- c) 2 porty USB 3.0 na panelu przednim;
- d) Opcjonalny port serial, możliwość wykorzystania portu serial do zarządzania serwerem;
- e) Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera.

8) Zasilanie, chłodzenie

- a) Redundantne zasilacze hotplug o sprawności 96% (tzw. klasa Titanium) o mocy nie większej niż 550W;



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

b) Redundantne wentylatory hotplug.

9) Zarządzanie

- a) Wbudowane diody informacyjne lub wyświetlacz informujący o stanie serwera - system przewidywania, rozpoznawania awarii;
- i. informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów:
 - karty rozszerzeń zainstalowane w dowolnym slotcie PCI Express;
 - procesory CPU;
 - pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM;
 - wbudowany na płycie głównej nośnik pamięci M.2 SSD;
 - status karty zarządzającej serwerem;
 - wentylatory;
 - bateria podtrzymująca ustawienia BIOS płyty głównej;
 - zasilacze;
 - system przewidywania/rozpoznawania awarii musi być niezależny i działać w przypadku odłączenia kabli zasilających serwer (podtrzymywany kondensatorowo lub bateryjnie w celu uruchomienia przy odłączonym zasilaniu sieciowym);
 - b) Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:
 - i. Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;
 - ii. Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;
 - iii. Dostęp poprzez przeglądarkę Web, SSH;
 - iv. Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;
 - v. Zarządzanie alarmami (zdarzenia poprzez SNMP);
 - vi. Możliwość przejęcia konsoli tekstowej;
 - vii. Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM);
 - viii. Obsługa serwerów proxy (autentykacja);
 - ix. Obsługa VLAN;
 - x. Możliwość konfiguracji parametru Max. Transmission Unit (MTU);
 - xi. Wsparcie dla protokołu SSDP;
 - xii. Obsługa protokołów TLS 1.2, SSL v3;



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

- xiii. Obsługa protokołu LDAP;
- xiv. Integracja z HP SIM;
- xv. Synchronizacja czasu poprzez protokół NTP;
- xvi. Możliwość backupu i odtwarzania ustawień bios serwera oraz ustawień karty zarządzającej;
- c) Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna);
- d) Dedykowana, do wbudowania w kartę zarządzającą (lub zainstalowana) pamięć flash o pojemności minimum 16 GB;
- e) Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN;
- f) Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej.

10) Wspierane OS

- a) Microsoft Windows Server 2022, 2019;
- b) VMWare vSphere 8.0;
- c) Suse Linux Enterprise Server 15;
- d) Red Hat Enterprise Linux 9, 8;
- e) Microsoft Hyper-V Server 2019

11) Dokumentacja, inne

- a) 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.
- b) Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE.
- c) Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, **w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki;**
- d) W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji;

- e) Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;
- f) Możliwość pracy w pomieszczeniach o wilgotności w zawierającej się w przedziale 10 - 85 %;
- g) Serwer musi być certyfikowany do pracy z systemem Ubuntu 22.04;
- h) Zgodność z normami: CB, RoHS, WEEE, GS oraz CE.

4. System operacyjny do serwera – 2 szt.,

oraz

5. Licencje dostępne do serwera – 70 szt.;

System operacyjny do serwera, oraz licencje dostępne do serwera zostały opisane wspólnie z uwagi na zintegrowane parametry techniczne, obowiązkiem Wykonawcy jest podanie nazw i cen jednostkowych proponowanych rozwiązań, które spełnią poniższe wymagania zgodnie z podziałem zamieszczonym w formularzu ofertowym.

Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie dwóch instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana, aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze.

Wymaga się, aby oferowane licencje dostępne do serwera umożliwiały korzystanie 70 użytkowników z usług katalogowych oferowanego systemu operacyjnego do serwera.

Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.

- 1) Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
- 2) Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
- 3) Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

- 4) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
- 5) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
- 6) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
- 7) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
- 8) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
- 9) Wbudowane wsparcie instalacji i pracy na wolumenach, które:
 - a) pozwalają na zmianę rozmiaru w czasie pracy systemu,
 - b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
 - c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
 - d) umożliwiają zdefiniowanie list kontroli dostępu (ACL).
- 10) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
- 11) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
- 12) Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET
- 13) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilkoma serwerami.
- 14) Wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
- 15) Dostępne dwa rodzaje graficznego interfejsu użytkownika:



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

- a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
- b) Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
- 16) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
- 17) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
- 18) Mechanizmy logowania w oparciu o:
 - a) Login i hasło,
 - b) Karty z certyfikatami (smartcard),
 - c) Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
- 19) Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych..
- 20) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
- 21) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
- 22) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
- 23) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
- 24) Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
- 25) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
 - a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
 - b) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:

- i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
- ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
- iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
- iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
- c) Zdalna dystrybucja oprogramowania na stacje robocze.
- d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
- e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
 - i. Dystrybucję certyfikatów poprzez http
 - ii. Konsolidację CA dla wielu lasów domeny,
 - iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
 - iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
- f) Szyfrowanie plików i folderów.
- g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
- h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
- i) Serwis udostępniania stron WWW.
- j) Wsparcie dla protokołu IP w wersji 6 (IPv6),
- k) Wsparcie dla algorytmów Suite B (RFC 4869),
- l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

- m) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:
- i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
 - ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
 - iii. Obsługi 4-KB sektorów dysków
 - iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
 - v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
 - vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)
- 26) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
- 27) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
- 28) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
- 29) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
- 30) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
- 31) Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

6. Dyski twarde do NAS'a – 2 szt.;

Zamawiający wymaga dostarczenia minimum SATA HDD o pojemności 10TB każdy o parametrach nie gorszych niż:

- Prędkość obrotowa: 5400 RPM
- MTBF: 1 000 000
- Obciążenie roczne: 180 TB
- Gwarancja producenta dysku: 3 lata

Dyski zgodne z listą kompatybilności producenta dla Qnap TS-432xU-RP

7. Biblioteka taśmowa – 1 szt.;

- | | | | |
|----|--|-------------|--|
| 1 | Typ napędu | LTO-9 | |
| 2 | Liczba napędów | 1 szt. | |
| 3 | Liczba slotów | 8 szt. | |
| 4 | Liczba slotów Import/Export tzw. mail slot dla wymiany nośników bez przerywania pracy napędu min.1 | | |
| 5 | Wbudowany skaner kodów paskowych na nośnikach LTO | TAK | |
| 6 | Pojemność bez kompresji (dla 8 slotów) | 144TB | |
| 7 | Pojemność z kompresją (dla 8 slotów) | 360TB | |
| 8 | Ilość magazynów | min.2 | |
| 9 | Interfejs | SAS 12GB | |
| 10 | Rozmiar bufora wewnętrznego | 1000MB | |
| 11 | Obudowa | Rack 19" 1U | |
| 12 | Zdalne zarządzanie | TAK | |
| 13 | Obsługa nośników typu WORM | TAK | |
| 14 | Obsługa przez moduł zdalnego zarządzania adresacji IP v4/v6 | TAK | |



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

- 15 Obsługa protokołu SNMP przez moduł zarządzania TAK
- 16 Obsługa szyfrowania danych na nośniku LTO-9 TAK
- 17 Do urządzenia dołączyć należy ☐ szyny do montażu w szafie rack 19”
☐ 1,5 metrowy kabel UTP do zdalnego zarządzania
☐ 9 tasiemek LTO-9 o natywnej pojemności 18 TB z naklejkami barcode
- 18 Gwarancja 3 lata z gwarantowanym czasem naprawy u zamawiającego na następny dzień roboczy od zgłoszenia usterki

8. NAS Network Attached Storage – 1 szt.;

- 1) Procesor - Procesor czterordzeniowy 64bitowy o taktowaniu nie niższym niż 2.2GHz
- 2) Obudowa - RACK 19" 1U – wraz z kompletem szyn przesuwanych umożliwiającym zamontowanie w szafie RACK
- 3) Procesor liczba rdzeni nie mniej niż 4
- 4) Pamięć RAM - 2 GB DDR4 ECC z możliwością rozszerzenia do 32GB
- 5) Liczba zatok na dyski twarde – min. 4
- 6) Całkowita liczba gniazd pamięci – min. 2
- 7) Obsługiwane dyski twarde - 3.5" SATA HDD oraz 2.5" SATA SSD – Hot Swap
- 8) Zainstalowane dyski: minimum 2 dyski po 10 TB każdy.
- 9) Możliwość podłączenia modułu rozszerzającego – Tak
- 10) Maksymalna ilość dysków z opcjonalnymi modułami rozszerzającymi, nie mniej niż 8
- 11) Porty na karty rozszerzeń - 1 x Gen3 x8 PCIe (x4 link)
- 12) Porty LAN - Wbudowane min. 4 x RJ-45 1GbE
- 13) Porty USB 3.2 – min. 2
- 14) Port eSATA – min. 1
- 15) Zasilanie - Max. 150W



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

- 16) Mechanizm szyfrowania sprzętowego - Tak, min AES-NI
- 17) Wewnętrzny system plików - BTRFS, EXT4
- 18) Obsługiwane tryby RAID - JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10
- 19) Funkcje backup - Możliwość tworzenia kopii bezpieczeństwa urządzeń pod Windows (Bare Metal) oraz usług chmur publicznych, portal użytkownika do przywracania danych kopii zapasowej (bez uprawnień administratora), serwer Apple Time Machine, backup na zewnętrzne dyski twarde, obsługa minimum 1024 migawek na folder udostępniony, obsługa minimum 65000 migawek na cały system
- 20) Darmowe aplikacje na urządzenia mobilne - Monitoring / Zarządzanie / Współdzielenie plików
- 21) Minimum obsługiwane aplikacje/usługi - Serwer plików, Serwer FTP, WebDav, Serwer WEB, Serwer kopii zapasowych, Serwer Monitoringu (min. 2 licencje bezpłatne), możliwość utworzenia klastra wysokiej dostępności z 2 identycznych urządzeń, Serwer pocztowy (min. 5 licencji w cenie)
- 22) VPN - VPN Server dla min. 40 połączeń
- 23) Gwarancja producenta - min. 2 lata (**długość gwarancji stanowi kryterium oceny ofert, deklarowaną długość gwarancji, należy podać w formularzu ofertowym**).

9. UPS – 2 szt.:

- 1) Moc pozorna - 3000 VA
- 2) Moc rzeczywista - 3000 W
- 3) Topologia (klasyfikacja IEC 62040-3) - Line-interactive z AVR
- 4) Współczynnik mocy – 1
- 5) Czas przełączenia na baterię - <4 ms
- 6) Liczba, typ gniazd wyjściowych - 8 x IEC C13 (2 grupy gniazd sterowalnych za pomocą oprogramowania oraz z poziomu wyświetlacza 2x2 IEC C13 10A), 1 x IEC C19 16A
- 7) Typ gniazda wejściowego - IEC C20 16A
- 8) Czas podtrzymania dla 2500W obciążenia - 4 min
- 9) Czas podtrzymania przy 1200W obciążenia -13 min
- 10) Czas podtrzymania przy 3000W obciążenia z dodatkowym modulem baterijnym -17 min
- 11) Dodatkowe baterie - Możliwość dodania do 4 dodatkowych modułów baterii w celu wydłużenia czasu podtrzymania do 84 minut dla 2500W obciążenia przy pf=1,0
- 12) Napięcie znamionowe - 200/208/220/230/240/250 V
- 13) Tolerancja napięci prostownika - 160 V – 294 V (regulacja programowa 150-294 V)



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

- 14) Częstotliwość znamionowa - 50/60 Hz autodetekcja
- 15) Tolerancja częstotliwości - 47– 70 Hz
- 16) Kształt napięcia – Sinusoidalny
- 17) Napięcie znamionowe wyjściowe - 200/208/220/230/240 V do wyboru przez użytkownika
- 18) Zakres zmian napięcia - +6/-10% napięcia nominalnego
- 19) Częstotliwość wyjściowa - 50/60 Hz
- 20) Współczynnik szczytu - 3:1
- 21) Baterie wymieniane przez użytkownika "na gorąco" – Tak
- 22) Ochrona przed przeładowaniem - Tak (ograniczenie prądu ładowarki, wyłączenie ładowarki / alarm)
- 23) Ochrona przed głębokim rozładowaniem - Tak
- 24) Okresowy automatyczny test baterii – Tak
- 25) System zarządzania pracą baterii
- 26) Możliwość uruchomienia bez napięcia w sieci "zimny start" – Tak
- 27) Baterie wewnętrzne o pojemności nie mniejszej niż - 9Ah 12V, minimum 6 szt.
- 28) Czas ładowania baterii do poziomu 90% - < 3 godz. do 90% pojemności użytkowej
- 29) Interfejs komunikacyjny:
 - a) USB
 - b) RS232 DB-9 żeński (HID)
 - c) styki przekaźnikowe
 - d) miniport wyłącznik ON/OFF
 - e) SNMP/Ethernet
- 30) Panel sterowania z wyświetlaczem LCD:
 - a) Panel LCD obrotowy (do ułatwienia odczytów przy obu wariantach montażu UPSa). Dostarcza informacji o : stanie pracy urządzenia, stanie obciążenia, pomiarach i ustawieniach. Funkcje ustawień i odczytów: lokalne, wyjścia (napięcie wyjściowe , częstotliwość wyjściowa), baterii (test baterii), pomiary i dane (numer seryjny, napięcie i częstotliwość wejściowa i wyjściowa, poziom obciążenia, pozostały czas podtrzymania, wydajność, zużycie energii w kWh).
 - b) Poziomy rząd przycisków sterowania
 - c) Poziomy rząd wskaźników stanu : zasilanie z siec(zielony), trybu bateryjnego (żółty), usterki (czerwony)
 - d) Sygnalizator akustyczny
- 31) Sygnały akustyczne, co najmniej na awarię, niski stan naładowania baterii, przeciążenie, oraz konieczność serwisu.
- 32) Przyciski sterujące i wskaźniki diodowe LED, co najmniej Przycisk Escape (anulowanie), Przyciski funkcyjne (przewijanie w górę i w dół), Przycisk Enter (potwierdzający), Przycisk ON/OFF załączenia i wyłączenia, LED trybu zasilania z siec i(kolor zielony), LED trybu baterii (kolor żółty), LED usterki (kolor czerwony).
- 33) Typ obudowy uniwersalna Tower/Rack 2U
- 34) Dane techniczne karty SNMP:
 - a) Network Support: Ethernet /10Mbps - Half duplex - 10Mbps - Full duplex - 100Mbps - Half duplex - 100Mbps - Full duplex - 1.0 Gbps - Full duplex / HTTP 1.1, SNMP V1, SNMP V3/ NTP, SMTP, DHCP/



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

- b) Tymczasowe hasła: Nadawanie użytkownikowi dostępu za pomocą konta. Konto może wygasać po odpowiedniej, wprowadzonej liczbie dni (hasło przestaje być aktywne). Blokowanie konta: Po określonej liczbie nieudanych prób wpisania hasła lub określonej liczbie dni.
- c) Protokoły: MQTT/RNDIS/LDAP/NVD/SSH/PKI
- d) Kamtybilność: SNMP v1/v3 i IP v4/v6
- e) Interfejs: HTML5
- f) Adresowanie IP: DHCP/BootP/Manualne
- g) Szyfrowanie: pakiet szyfrów TLS 1.2 z minimum SHA256
- h) Dostępny port USB (microUSB - port serwisowy)
- i) Certyfikaty: UL 2900-1, 2900-2-2
- 35) Dołączone oprogramowanie - Tak, monitorujące i zarządzające UPS, umożliwiające automatyczne zamykanie systemów operacyjnych.
- 36) Poziom hałasu w odl. 1m - do 40 dBA dla pracy normalnej
- 37) Znaki bezpieczeństwa - CE, Energy Star, IEC/EN 62040-1-1, IEC/EN 62040-2 class B, IEC/EN 62040-3
- 38) Możliwość montażu ręcznego bypassu serwisowego
- 39) Gwarancja producenta - 36 miesięcy dla elektroniki, 24 miesiące dla baterii

10. UPS dla stacji roboczych – 76 szt.:

Moc pozorna 900 VA

Moc rzeczywista 480 W

Technologia Line-Interactive

Gniazda wyjściowe z podtrzymaniem baterijnym typu E (2P+Z), minimum 2szt

Przewód zasilający Przymocowany na stałe do zasilacza UPS

Port komunikacyjny USB umieszczony na przednim panelu zasilacza UPS

Wskaźnik stanu UPS Dioda LED

Parametry wejściowe

Napięcie znamionowe 220-240 V; 50/60 Hz

Zakres napięcia wejściowego 140-300 V; 45-65 Hz

Parametry wyjściowe

Znamionowe napięcie wyjściowe 220/230/240 V

Regulacja napięcia w trybie baterijnym +/-20%



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

Sprawność w trybie normalnym >95%

Sprawność w trybie bateryjnym >60%

Regulacja częstotliwości w trybie normalnym zgodnie z siecią zasilającą

Regulacja częstotliwości w trybie bateryjnym +/-1 Hz

Częstotliwość w trybie normalnym zgodnie z siecią zasilającą

Częstotliwość w trybie bateryjnym 50/60 Hz

Przeciążalność [110%,120%] 5 min; >120% 1 s

Zdolność zwarciova w trybie bateryjnym 5A

Wytrzymywany czas przepływu prądu zwarciowego 50 ms

Czas przełączania 10 ms dla przejścia z trybu normalnego do trybu bateryjnego

Bateria

Specyfikacja 12 V DC – 1 x 12 V, 7 Ah

Typ Valve Regulated Lead-Acid (VRLA) szczelne, bezobsługowe, z minimalną żywotnością 3 lat w temperaturze 25°C

Monitoring Zaawansowany monitoring z wczesnym wykrywaniem awarii oraz powiadamianiem.

Zimny start Tak

Stopień ochrony IP20

Gwarancja 24 miesiące

11. Dostosowanie usług katalogowych dla użytkowników, wraz z wdrożeniem Centralnego Systemu Bezpieczeństwa – 1 usługa w wysokości max. 168 godzin.

W ramach zadania obowiązkiem Wykonawcy będzie dostosowanie usług katalogowych dla użytkowników, wraz z wdrożeniem Centralnego Systemu Bezpieczeństwa.



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

Z uwagi na minimalizowanie ingerencji w prace Urzędu, wdrożenie usług katalogowych wraz z wdrożeniem Centralnego Systemu Bezpieczeństwa nie może trwać dłużej niż 168 roboczogodzin, realizowanych w trakcie 90 dni przeznaczonych na realizację projektu.

Obowiązkiem Wykonawcy jest omówienie harmonogramu wykonania usługi z Zamawiającym.

W harmonogramie powinna znaleźć się informacja o anonsowaniu planowanych prac przez Wykonawcę i forma jej potwierdzenia przez Zamawiającego. Harmonogram musi być zaakceptowany przez strony.

1.1 Wdrożenie i skonfigurowanie usług katalogowych musi zapewniać efektywne zarządzania dostępem do zasobów informatycznych u Zamawiającego. Obowiązkiem Wykonawcy będzie utworzenie struktury organizacyjnej, grup, kont użytkowników oraz polityk bezpieczeństwa. Szczegółowy zakres prac zawiera:

a. Analiza i Projektowanie:

- Ocena infrastruktury istniejącej w celu dostosowania projektu do istniejących zasobów.
- Zaprojektowanie struktury organizacyjnej usług katalogowych z uwzględnieniem potrzeb Zamawiającego.

Efektem działań będzie utworzenie dokumentu zawierającego ustaloną strukturę usług katalogowych. Dokument ten zostanie zatwierdzony przez zamawiającego w celu kontynuowania prac.

b. Wdrożenie:

- Instalacja na infrastrukturze Zamawiającego (serwerach z oprogramowaniem).
- Konfiguracja globalnych i lokalnych polityk bezpieczeństwa.
- Utworzenie grup użytkowników i przydzielanie odpowiednich uprawnień.
- Integracja usługi z istniejącymi systemami.
- Wpięcie max 50 sztuk urządzeń klienckich, wraz z przeniesieniem profili użytkownika.
- Wsparcie w rozwiązywaniu problemów związanych z wdrażaniem urządzeń klienckich.

Efektem działań będzie przekazanie maszyny z zainstalowaną i skonfigurowaną usługą katalogową.

c. Testowanie i akceptacja:

- Przeprowadzenie testów funkcjonalnych w celu potwierdzenia poprawności działania usługi katalogowej.
- Protokolarne przekazanie dokumentacji dotyczącej konfiguracji, w tym haseł dostępowych instrukcji i postępowania w razie problemów.

1.2 Wdrożenie oferowanego Centralnego Systemu Bezpieczeństwa (dalej CSB), polegające w szczególności na instalacji oraz uruchomieniu rozwiązania. Do obowiązków Wykonawcy należeć będą:



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

- a) Instalacja fizyczna i konfiguracja funkcjonalna komponentów systemu CSB.
- b) Konfiguracja systemu CSB w środowisku Zamawiającego. Zdefiniowanie niezbędnych do poprawnego działania systemu parametrów konfiguracyjnych.
- c) Integracja z usługą katalogową w zakresie autentykacji użytkowników. Konfiguracja ról Użytkowników.
- d) Podłączenie do 3 rodzajów źródeł zdarzeń (np. UTM, switch, serwer) rozpoznawanych przez system CSB. Wykonawca przekaże wytyczne dla Zamawiającego dotyczące koniecznej konfiguracji źródeł zdarzeń Zamawiającego.
- e) Budowa minimum 1 parser dla źródeł zdarzeń nieobsługiwanych automatycznie przez system CSB.
- f) Możliwość tworzenia niestandardowych reguł korelacyjnych/scenariuszy oraz aktywacja/konfiguracja wbudowanych reguł korelacyjnych
- g) Konfiguracja polityk retencji danych
- h) Przygotowanie dokumentacji powykonawczej, zawierającej co najmniej zbiór haseł dostępowych, instrukcji i postępowania w razie problemów
- i) Przygotowanie i przetestowanie procedur kopii bezpieczeństwa i odtwarzania systemu po awarii
- j) Instalacja najnowszej wersji składników systemu

Efektem wdrożenia musi być działanie CSB (systemu klasy SIEM) w środowisku IT Zamawiającego. Dodatkowe konfiguracje (aktualizacje) będą wykonywane w ramach Specjalistycznego wsparcia IT opisanego w dalszej części dokumentu.

12. Specjalistyczne wsparcie IT w zakresie cyberbezpieczeństwa w wymiarze 8h stacjonarnie, 30h online miesięcznie – łącznie usługa wsparcia trwać będzie nie dłużej jak do 25.05.2026 ;

W ramach zadania obowiązkiem Wykonawcy będzie świadczenie specjalistycznego wsparcia IT w zakresie cyberbezpieczeństwa. Wnioskodawca w ramach każdej z zaoferowanych paczek roboczogodzin będzie świadczył specjalistyczne wsparcie IT w wymiarze 8h stacjonarnie, 30h online w następującym zakresie:

- a) Wdrożenie reguł zgodności z przepisami prawnymi oraz standardami bezpieczeństwa.
- b) Konfiguracja i zarządzanie firewallami, IDS/IPS i innymi mechanizmami obronnymi.
- c) Zarządzanie dostępem i autoryzacją użytkowników.
- d) Monitoring sieci i alarmowanie w czasie rzeczywistym.
- e) Wdrożenie (na zlecenie) reguł dla Backupu i archiwizacji danych.
- f) Szyfrowanie danych wrażliwych.



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

- g) Zabezpieczenie przed oprogramowaniem złośliwym – konfiguracja: antywirus, antimalware.
- h) Opracowanie i implementacja planu reagowania na incydenty bezpieczeństwa.
- i) Analiza po incydentach i rekomendacje.
- j) Stałe monitorowanie logów i zdarzeń związanych z bezpieczeństwem.
- k) Zlecone raporty dotyczące stanu bezpieczeństwa.
- l) Reagowanie na zgłoszone incydenty związane z bezpieczeństwem
- m) Wsparcie w obsłudze wdrożonego w ramach projektu Centralnego Systemu Bezpieczeństwa – oprogramowania klasy SIEM.

Wszystkie zapisy rozumiane jako doradztwo i konfiguracja urządzeń oraz systemów zakupionych w ramach projektu będą realizowane zgodnie z założonymi incydentami. Incydenty będą mogły być zakładane przez Zamawiającego poprzez udostępnione przez Wykonawcę kanały komunikacji, takie jak co najmniej:

Strona www (24h)

Adres email (24h)

Telefon w dni robocze (7:30 – 15:30) – infolinia w języku polskim.

Dla wsparcia stacjonarnego, Wykonawca zapewni realizację incydentów zgodnie z SLA (1/5) co oznacza 1 dzień roboczy na reakcję na zgłoszenie i 5 dni roboczych na realizację.

Dla wsparcia online, Wykonawca zapewni realizację incydentów zgodnie z SLA (1/3) co oznacza 1 dzień roboczy na reakcję na zgłoszenie i 3 dni robocze na realizację.

WSPARCIE STACJONARNE 8h w ramach paczki godzin.

W przypadku usług wykonywanych stacjonarnie, po zgłoszeniu przez Zamawiającego incydentu - konieczności wizyty stacjonarnej w Urzędzie, Wykonawca ma 5 dni roboczych na realizację tego zadania.

Wykonawca musi zaanonsować dzień swojej wizyty w Jednostce Zamawiającego w ramach czasu wskazanego na reakcję (1 dzień roboczy).

Wezwanie Wykonawcy do świadczenia usługi stacjonarnej odbywać będzie się maksymalnie w ramach dwóch wizyt w ramach jednej paczki godzin.

Każda wizyta i jej długość zostanie zaraportowana przez Wykonawcę i potwierdzona przez Zamawiającego. Raportowanie wykonanych godzin jest obowiązkiem Wykonawcy, może ono odbywać się z wykorzystaniem systemu informatycznego, lub w formie tradycyjnej (protokoły), jednak każdorazowo wykonanie usługi musi być potwierdzone przez Zamawiającego. Podpisane protokoły będą podstawą do wystawienia faktur (zgodnie z umową).

WSPARCIE ONLINE 30h w ramach paczki godzin.



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

W przypadku usług wykonywanych **online**, po zgłoszeniu przez Zamawiającego incydentu - konieczności wsparcia online, Wykonawca ma 3 dni robocze na realizację tego zadania.

Wykonawca musi zaanonsować termin wykonywanych prac w ramach czasu wskazanego na reakcję (1 dzień roboczy).

Wezwanie Wykonawcy do świadczenia usługi wsparcia online odbywać będzie się maksymalnie w ramach 5 zleceń w ramach jednej paczki.

Każda usługa wsparcia online i jej długość zostanie zaraportowana przez Wykonawcę i potwierdzona przez Zamawiającego. Raportowanie wykonanych godzin jest obowiązkiem Wykonawcy, może ono odbywać się z wykorzystaniem systemu informatycznego, lub w formie tradycyjnej (protokoły), jednak każdorazowo wykonanie usługi musi być potwierdzone przez Zamawiającego. Podpisane protokoły będą podstawą do wystawienia faktur (zgodnie z umową).

Dla zgłoszeń obu typów incydentów Zamawiający przekaze wykonawcy imienną listę osób uprawnionych do zgłaszania i raportowania incydentów (maksymalnie 3 osoby).

WYKORZYSTANIE PACZEK GODZIN

W ramach zadania, Wykonawca świadczy na rzecz Zamawiającego usługę specjalistycznego wsparcia IT w 24 paczkach godzin w wymiarze 8h stacjonarnie, 30h online (dalej **paczka godzin**), a także pozostaje w trybie gotowości do podjęcia ww. zleceń w okresie o mniejszej intensyfikacji zgłoszeń.

Specjalistyczne wsparcie IT świadczone będzie od dnia podpisania umowy.

Wykonawca przez cały okres świadczenia usługi utrzymuje stan gotowości, do realizacji zleceń – incydentów na rzecz zamawiającego.

Paczka godzin, będzie wykorzystana maksymalnie w ciągu 30 dni.

Okres 30 dni stanowi okres rozliczeniowy dla każdej kolejnej paczki godzin, rozpoczynając od dnia podpisania umowy. Kolejne okresy rozliczeniowe będą liczone od dnia wykorzystania paczki godzin, lub upływie 30 dni.

Zamawiający w okresie 30 dni może wykorzystać maksymalnie 2 paczki godzin. Wykorzystanie większej ilości wsparcia – paczek godzin, może odbyć się tylko za obopólną zgodą Zamawiającego i Wykonawcy.

Wykorzystanie paczki godzin, klasyfikowane będzie zawsze dla okresu, w którym Zamawiający przekazał zgłoszenie incydentu, także w przypadkach, kiedy Wykonawca w jego obsłudze wyszedł poza okres trwania paczki godzin (np. zgłoszenie przekazane w 29 dniu okresu rozliczeniowego pierwszej paczki godzin, obsłużone w 32 dniu będzie zaliczane dla pierwszej paczki godzin).



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

W przypadku nie wykorzystania wszystkich godzin (stacjonarnych, lub online) w ciągu 30 dni, w ramach jednej paczki godzin niewykorzystane godziny nie przechodzą na kolejny okres. Nie zmienia to wynagrodzenia Wykonawcy, pod warunkiem pozostania w gotowości do wykonania zleceń incydentów na rzecz Zamawiającego.

Jeżeli Zamawiający wykorzysta jeden typ wsparcia (godziny stacjonarne, lub online) może wymienić typ wsparcia według przelicznika: 1 godzina stacjonarna = 6 godzin online.

Podmiot realizujący usługę musi posiadać kompetencje z wdrażanego w ramach projektu Centralnego Systemu Bezpieczeństwa – oprogramowania klasy SIEM - **Na wezwanie Zamawiającego dołączyć certyfikat wystawiony przez producenta systemu potwierdzający kompetencje Wykonawcy (lub osób wskazanych do realizacji tego zadania) lub referencje z wdrożenia oferowanego systemu przez Wykonawcę (lub osoby wskazane do realizacji zadania).**

Zadanie częściowe nr 2:

Dostawa licencji na oprogramowanie – wymagania minimalne:

1. Oprogramowanie antywirusowe - dla 55 użytkowników;

Zamawiający wymaga przedłużenia licencji obecnie posiadanego oprogramowania antywirusowego firmy ESET w wersji co najmniej ESET PROTECT Entry ON-PREM na okres do dnia 25.05.2026 roku. Zamawiający dopuszcza dostarczenie rozwiązania równoważnego, przez co rozumiane jest rozwiązanie spełniające poniższe jakościowe i funkcjonalne wymagania minimalne:

Administracja zdalna w chmurze

1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego.
2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.
4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
8. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.
9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.
10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
11. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.

Ochrona stacji roboczych

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
2. Rozwiązanie musi wspierać architekturę ARM64.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
10. Rozwiązanie musi integrować się z Intel Threat Detection Technology.
11. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).

12. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.

13. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

14. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.

15. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.

16. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:

1. - tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,

1. - tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,

2. - tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,

3. - tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,

4. - tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.

5.

17. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.

18. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.

19. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.

20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antyvirus, antyspyware, metody heurystyczne).

21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

22. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.
23. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:
 1. - tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
 1. - tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
 2. - tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
 3. - tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.
 - 4.
24. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
25. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
26. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
27. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
28. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
29. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
30. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

Ochrona serwera

1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7,8 i 9, CentOS 7, Ubuntu Server (SLES) 15, Oracle Linux 8 oraz Amazon Linux.
2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

Dodatkowe wymagania dla ochrony serwerów Windows:

9. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
10. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
11. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
12. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
13. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
14. Rozwiązanie musi automatycznie wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
15. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
16. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
17. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

Dodatkowe wymagania dla ochrony serwerów Linux:

18. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
19. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
20. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.
21. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.

Szyfrowanie

1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10 32-bit i 64-bit.
2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

3. Aplikacja musi posiadać autentykację typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.
4. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.

Ochrona urządzeń mobilnych opartych o system Android

1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.
5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:
 - usunięcie zawartości urządzenia,
1. - przywrócenie urządzenia do ustawień fabrycznych,
1. - zablokowanie urządzenia,
2. - uruchomienie sygnału dźwiękowego,
3. - lokalizację GPS.
4. 6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
5. 7. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:
 - 6. - nazwę aplikacji,
 - 7. - nazwę pakietu,
 - 8. - kategorię sklepu Google Play,
 - 9. - uprawnienia aplikacji,
 - 10. - pochodzenie aplikacji z nieznanego źródła.

Sandbox w chmurze

1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
2. Rozwiązanie musi wykorzystywać do działania chmurę producenta.
3. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
4. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
5. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
7. Po zakończonej analizie pliku, rozwiązanie musi przysyłać wynik analizy do wszystkich wspieranych produktów.
8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizację stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
10. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.
11. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo.
12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem:
 - Czysty,
 1. - Podejrzany,
 1. - Bardzo podejrzany,
 2. - Szkodliwy.
 - 13. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
 - 14. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.
 - 15. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.

2. Oprogramowanie do audytu sprzętowego i oprogramowania – 1 szt.;

LICENCJA

W ramach postępowania Wykonawca jest zobowiązany dostarczyć Oprogramowanie wraz z licencją bezterminową.

Oprogramowanie musi posiadać wsparcie min. do dnia 25-05-2026 roku, w ramach wsparcia, Zamawiający musi posiadać możliwość aktualizacji do najnowszej dostępnej wersji oprogramowania, zgłaszać błędy w Oprogramowaniu do serwisu producenta.

Licencje na oprogramowanie dostarczone będą do siedziby Zamawiającego w formie papierowej lub elektronicznej.

Dostarczona licencja na Oprogramowanie nie może limitować ilości urządzeń.

Licencja na dostarczone oprogramowanie musi umożliwiać działanie dla minimum 45 użytkowników.

OPROGRAMOWANIE – jakościowe i funkcjonalne wymagania minimalne:

Oprogramowanie musi posiadać budowę modułową, składającą się z serwera zarządzającego, zdalnych konsoli oraz Agentów. Komunikacja pomiędzy Serwerem a Agentami i Konsolami musi być nawiązywana przy użyciu szyfrowanego protokołu TLS 1.2. Program musi umożliwiać zmianę portu komunikacyjnego wykorzystywanego przez konsolę zarządzającą.



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

Moduły muszą umożliwiać kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomocy w formie interaktywnego połączenia sieciowego z obsługiwanym użytkownikiem.

Oprogramowanie musi posiadać moduły opisane poniżej.

MONITOROWANIE INFRASTRUKTURY (BEZAGENTOWO) – minimalne wymagania:

Musi obejmować m.in.: serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie:

1. Wykrywania urządzeń w sieci poprzez skanowanie ping oraz arp-ping
2. Wykrywania urządzeń na podstawie informacji odczytanych z Active Directory (wraz z informacją o OU)
3. Wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci
4. Wizualizacji urządzeń na mapach z funkcją siatki umożliwiającej korygowanie pozycji ikon na mapie do najbliższej linii siatki
5. Wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z dowolnym kolorem tła.
6. Wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków np. schematu rozmieszczenia pomieszczeń w budynku
7. Wizualizacji map urządzeń poprzez grupowanie urządzeń na narysowanych czworokątach o dowolnym rozmiarze i kolorze
8. Wizualizacji map urządzeń poprzez wstawianie dowolnego tekstu na mapie
9. Wizualizacji połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji, do którego portu przełącznika podłączone jest dane urządzenie w sposób manualny oraz automatyczny
10. Zablockowania mapy urządzeń przed przypadkową edycją
11. Serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów
12. Serwerów pocztowych:
13. Monitorowanie czasu logowania do serwisu odbierającego oraz czas wysyłania poczty
14. Możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdują się poza zakresem)
15. Możliwość wykonywania operacji testowych
16. Możliwość wysyłania powiadomienia jeśli serwer pocztowy nie działa
17. Monitorowanie serwerów WWW i adresów URL
18. Cykliczne monitorowanie czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS
19. Obsługa szyfrowania SSL/TLS w powiadomieniach e-mail
20. Obsługa urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

21. Obsługa komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych
22. Monitoring routerów i przełączników wg:
 - zmian stanu interfejsów sieciowych
 - ruchu sieciowego
 - podłączonych stacji roboczych – graficzna prezentacja panelu switcha
 - ruchu generowanego przez podłączone do portów stacje robocze
23. Monitor m.in. serwisów Windows, który alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie
24. Wyświetlanie statystyk przy każdym urządzeniu na mapie takich jak: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu
25. Monitorowanie stanu maszyn wirtualnych Vmware: działa, nie działa, wstrzymano
26. Zarządzanie stanem maszyn wirtualnych Vmware: wysyłanie poleceń włączenia, wstrzymania i wyłączenia zasilania do każdej maszyny
27. Podgląd wydajności systemów:
 - obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy

MODUŁ INWENTARYZACJA – minimalne wymagania:

1. Szczegółowe prezentacje dotyczące sprzętu m.in.: modelu, procesora, pamięci, płyty głównej, napędów, kart itp.
2. Możliwość odczytu parametrów S.M.A.R.T. dysków twardych, dysków SSD, w tym NVMe.
3. Dane m.in.: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade.
4. Informuje o zainstalowanych aplikacjach oraz aktualizacjach systemu operacyjnego co bezpośrednio ma umożliwić audytowanie i weryfikację użytkowania licencji w organizacji.
5. Zbieranie informacji w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd.
6. Posiadanie możliwości wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiegokolwiek zmiany konfiguracji sprzętowej komputera.
7. Możliwość odczytania numeru seryjnego (klucze licencyjne).
8. Możliwość automatycznego zarządzania instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych.
9. Możliwość przeglądu informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.
10. Możliwość utworzenia listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu).



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

11. Możliwość wymiany plików do i ze stacją roboczą poprzez funkcję Menedżera plików.

Moduł inwentaryzacji zasobów musi umożliwić prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i programowania:

- przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji,
- przydzielania dostępu administratorów do zasobów na podstawie praw do oddziałów,
- tworzenia powiązań między zasobami a urządzeniami,
- tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych,
- wskazania osób uprawnionych do użycia zasobów poprzez rozbudowane mechanizmy,
- definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie e-mail o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, lub własny komentarz,
- określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów,
- określenia atrybutów dodatkowych tylko dla wybranych typów zasobów,
- masową edycję atrybutów zasobów,
- definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie,
- importu danych z zewnętrznego źródła (.CSV),
- przechowywania dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp.,
- tworzenia powiązań między zasobami a dokumentami w relacji 1:N,
- oznaczania statusów zasobów, np. w użyciu, w naprawie, zutilizowany itp.,
- ewidencji czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczanego na wykonanie czynności,
- generowania zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania,
- przygotowanie wielu szablonów generowanych dokumentów i protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji,
- konfiguracji stylu automatycznego numerowania dodawanych zasobów wg zdefiniowanego wzorca,
- konfiguracji stylu automatycznego numerowania dodawanych dokumentów i protokołów wg zdefiniowanego wzorca,
- archiwizacji i porównywania audytów zasobów,



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

- tworzenia kodów kreskowych dla zasobów,
- drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy,
- inwentaryzacji zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej dla systemu Android poprzez wyszukiwanie zasobów, skanowanie etykiet, dodawanie i edycję zasobów, dodawanie czynności serwisowych, drukowanie etykiet,
- możliwość zmiany portu komunikacyjnego wykorzystywanego przez aplikację mobilną dla systemu Android,
- inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agentów poprzez manualne wykonanie skanów inwentaryzacji offline),
- definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data” z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja”).

3. Oprogramowanie do zarządzania i aktualizacji systemów operacyjnych i oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych – 1 szt.;

LICENCJA

W ramach postępowania Wykonawca jest zobowiązany dostarczyć Oprogramowanie wraz z licencją bezterminową.

Oprogramowanie musi posiadać wsparcie min. do dnia 25-05-2026 roku, w ramach wsparcia, Zamawiający musi posiadać możliwość aktualizacji do najnowszej dostępnej wersji oprogramowania, zgłaszać błędy w Oprogramowaniu do serwisu producenta.

Licencje na oprogramowanie dostarczone będą do siedziby Zamawiającego w formie papierowej lub elektronicznej.

Dostarczona licencja na Oprogramowanie nie może limitować ilości urządzeń.

Licencja na dostarczone oprogramowanie musi umożliwiać działanie dla minimum 45 użytkowników.

OPROGRAMOWANIE – jakościowe i funkcjonalne wymagania minimalne:

Oprogramowanie musi posiadać budowę modułową, składającą się z serwera zarządzającego, zdalnych konsoli oraz Agentów. Komunikacja pomiędzy Serwerem a Agentami i Konsolami musi być nawiązywana przy użyciu szyfrowanego protokołu TLS 1.2. Program musi umożliwiać zmianę portu komunikacyjnego wykorzystywanego przez konsolą zarządzającą.



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

Moduły muszą umożliwiać kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomocy w formie interaktywnego połączenia sieciowego z obsługiwany użytkownikiem.

Oprogramowanie musi posiadać moduły opisane poniżej.

MODUŁ OBSŁUGI UŻYTKOWNIKÓW – minimalne wymagania:

Badanie aktywności użytkowników poprzez monitorowanie:

- Faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy),
- Procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach,
- Rzeczywistego użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność,
- Informacji o edytowanych przez użytkownika dokumentach,
- Historii pracy (cykliczne zrzuty ekranowe),
- Listy odwiedzanych stron WWW (tytuły, adresy, liczba i czas wizyt),
- Transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika),
- Wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Program ma możliwość monitorowania kosztów wydruków,
- Nagłówków przesyłanej w aplikacjach klienckich poczty e-mail.

Dodatkowo moduł musi posiadać funkcjonalność:

- wykrywania podejrzanego aktywności przez popularne „jiggler”, mającej na celu symulowanie faktycznej pracy.
- zdefiniowania czasu (min. 15 minut) gdy wykrywana będzie symulowana aktywność wyłącznie przez ruch myszą bez kliknięcia lub wprowadzanie tego samego znaku z klawiatury.
- wyszczególnienia podejrzanego aktywności w raportach.
- wygenerowania alarmu i wykonania akcji po wykryciu podejrzanego aktywności.
- automatycznego włączenia zapisywania zrzutów ekranowych po wykryciu podejrzanego aktywności.
- blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. *.domena.pl). Reguły w postaci listy domen tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane lub współdzielone pomiędzy grupami lub kontami.



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

- integracji list stron w formie plików .TXT z dowolnego adresu zewnętrznego np. CERT.
- skorzystania z wbudowanej listy stron sklasyfikowanych jako zagrożenia.
- automatycznego odświeżania list stron zintegrowanych z adresów zewnętrznych.
- blokowania ruchu na wskazanych portach TCP/IP,
- blokowania pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem,
- prowadzenia rejestru naruszeń blokad,
- wysyłania powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia, naruszy skonfigurowane blokady,
- przygotowania zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu (który można dołączyć np. do akt pracownika),
- definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone.

MODUŁ OCHRONY DANYCH PRZED WYCIEKIEM – minimalna funkcjonalność:

1. Blokowanie urządzeń i nośników danych. Program ma mieć możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny.
2. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyski.
3. Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA.
4. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych.
5. Funkcje wspierające bezpieczeństwo systemu
6. Funkcje wspierające bezpieczeństwo systemu: zdalne szyfrowanie dysków za pomocą BitLocker.
7. Funkcje wspierające bezpieczeństwo systemu: zapisywanie klucza odzyskiwania do pliku oraz jako zasób w bazie danych programu.
8. Funkcje wspierające bezpieczeństwo systemu: integracja z Windows Defender w zakresie odczytu stanu ochrony, włączenia i wyłączenia ochrony, tworzenia reguł ruchu.
9. Funkcje wspierające bezpieczeństwo systemu: odczytanie informacji o aktywnym oprogramowaniu antywirusowym firm trzecich, innym niż Windows Defender.
10. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu modułu TPM.

Zarządzanie prawami dostępu do urządzeń:

1. Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików.
2. Autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive'ów, dysków itp. - urządzenia prywatne są blokowane.
3. Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników.
4. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci.
5. Możliwość usuwania z listy znanych urządzeń tych nośników, które np. zostały zutylizowane.

Audyt operacji na plikach na urządzeniach przenośnych:



Cyberbezpieczny Samorząd

Projekt „Cyberbezpieczna Gmina Nowa Słupia” dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

1. Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych.
2. Podłączenie/odłączenie urządzenia przenośnego.