ZAŁ. 5

Załącznik numer 5 - rozwiązania technologiczne

Zawartość:

I. Opis warstwy sprzętowej sprzętowej złożonej z:

1. System bezpieczeństwa sieciowego złożony z:
- Firewall z systemem ddos
- oprogramowanie antywirusowe
- Przełącznik rdzeniowy
- Aktualizacja oprogramowania routingu i firewall
2. Platforma serwerowa złożona z:
- serwery
- Sieciowe systemy operacyjne
- Macierz
3. Modernizacja serwerowni
Modernizacja zasilania awaryjnego
Sprzęt komputerowy
Poniżej przedstawione są parametry minimalne poszczególnych systemów:

System bezpieczeństwa sieciowego – 1 system:

SKARBNIK MIASTA
Sławosław Wróbel

oprogramowanie antywirusowe (187 szt). zapewniające pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
Zamawiający planuje objąć ochroną antywirusową wszystkie komputery które będą miały dostęp od strony sieci LAN do zasobów serwerowych. W chwili obecnej komputery chronione są przez oprogramowanie z nieaktualizowanymi wirusów.
Wykrywanie i usuwanie niebezpiecznych programów: adware, spyware, scareware, phishing, hacktools itp.
Wbudowana technologia do ochrony przed rootkitami wykrywająca aktywne i nieaktywne rootkity.
Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
Możliwość konfiguracji programu do pracy z jednym skanerem i dwoma skanerami antywirusowymi jednocześnie.
Możliwość wykluczenia ze skanowania skanera dostępowego: napędów, katalogów, plików lub procesów.
Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików na żądanie lub według harmonogramu.
Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności, rodzaj plików do skanowania, priorytet skanowania).
Skanowanie na żądanie pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
Technologia zapobiegająca powtórnemu skanowaniu sprawdzonych już plików, przy czym maksymalny czas od ostatniego sprawdzenia pliku nie może być dłuższy niż 4 tygodnie, niezależnie od tego czy plik był modyfikowany czy nie.

Możliwość określania poziomu obciążenia procesora podczas skanowania na żądanie i według harmonogramu.
Możliwość skanowania dysków sieciowych i dysków przenośnych.
Rozpoznawanie i skanowanie wszystkich znanych formatów kompresji.
Możliwość definiowania listy procesów, plików, folderów i napędów pomijanych przez skaner dostępowy.
Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
Skanowanie i oczyszczanie poczty przychodzącej POP3 w czasie rzeczywistym, zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
Możliwość definiowania różnych portów dla POP3, SMTP i IMAP na których ma odbywać się skanowanie.
Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
Dedykowany moduł chroniący przeglądarki przed szkodnikami atakującymi sesje z bankami i sklepami online.
Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
Możliwość definiowania różnych portów dla HTTP, na których ma odbywać się skanowanie.
Możliwość automatycznego wysyłania powiadomienia o wykrytych zagrożeniach do dowolnej stacji roboczej w sieci lokalnej.
W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e mail.
Możliwość zabezpieczenia hasłem dostępu do opcji konfiguracyjnych programu.
Aktualizacja dostępna z bezpośrednio Internetu lub offline – z pliku pobranego zewnętrznie.
Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
Możliwość określenia częstotliwości aktualizacji w odstępach 1 godzinowych.
Możliwość samodzielnej aktualizacji sygnatur wirusów ze stacji roboczej (np. komputery mobilne).
Program wyposażony w tylko w jeden serwer skanujący uruchamiany w pamięci,
z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, skaner HTTP).
Możliwość ukrycia programu na stacji roboczej przed użytkownikiem.
Skanowanie w trybie bezczynności - pełne skanowanie komputera przynajmniej raz na 2 tygodnie uruchamiane i wznawiane automatycznie, podczas gdy nie jest on używany.
Ochrona przed urządzeniami podszywającymi się po klawiatury USB.
Integrcja z usługami katalogowymi Sieciowego systemu operacyjnego – import kont komputerów i jednostek organizacyjnych.
Możliwość kontekstowego zastosowania ustawień danej stacji dla całej grupy.
Możliwość eksportu/importu ustawień dla stacji/grupy stacji.
Możliwość zarządzania dowolną ilością serwerów zarządzających z jednego okna konsoli.
Możliwość zarządzania różnymi wersjami licencyjnymi oprogramowania producenta z jednego okna
Możliwość tworzenia hierarchicznej struktury serwerów zarządzających (serwer główny i serwery podrzędne).

Możliwość zainstalowania zapasowego serwera zarządzającego, przejmującego automatycznie funkcje serwera głównego w przypadku awarii lub odłączenia serwera głównego.
Możliwość zdalnego zarządzania serwerem spoza sieci lokalnej przy pomocy połączenia VPN.
Możliwość zdalnego zarządzania serwerem centralnego zarządzania przez przeglądarki internetowe (z sieci lokalnej i spoza niej).
Możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych.
Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania).
Możliwość przeglądania list programów zainstalowanych na stacjach/serwerach (nazwa, wersja, producent, data instalacji).
Możliwość stworzenia białej i czarnej listy oprogramowania, i późniejsze filtrowanie w poszukiwaniu stacji je posiadających.

Przełącznik rdzeniowy – 2 szt.
Przełącznik posiadający 16 portów 10Gigabit Ethernet SFP+, mogących pracować z prędkością 100 MB, 1G lub 10G – zdefiniowane przez zainstalowane interfejsy SFP lub SFP+
Wysokość urządzenia 1U
Przełącznik musi posiadać możliwość realizacji redundancji zasilania poprzez instalację wewnętrznego dodatkowego zasilacza. Przełącznik musi mieć możliwość montażu zasilaczy AC lub DC w zależności od potrzeb
Przełącznik musi posiadać możliwość instalacji zestawu wentylatorów zapewniających chłodzenie przód-tył, lub tył-przód.
Nieblokująca architektura o wydajności przełączania min. 320 /s
Szybkość przełączania min. 238 Milionów pakietów na sekundę
Średnie opóźnienia na portach maksimum 900ns (pakiety 64 bitowe)
Możliwość łączenia min 2 przełączników w stos
Tablica MAC adresów min. 16k
Pamięć operacyjna: min. 1GB pamięci DRAM
Pamięć flash: min. 4GB pamięci Flash
Pojemność bufora pakietów min. 2MB
Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094
Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci
Obsługa Q-in-Q IEEE 802.1ad
Obsługa Quality of Service
IEEE 802.1p
DiffServ
8 kolejek priorytetów na każdym porcie wyjściowym
Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB
Obsługa LLDP Media Endpoint Discovery (LLDP-MED)
Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora.
Możliwość instalacji min. dwóch wersji oprogramowania - firmware
Możliwość przechowywania min. kilkunastu wersji konfiguracji w plikach tekstowych w pamięci Flash
Możliwość monitorowania zajętości CPU
Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring)
Wbudowany port USB pozwalający na łatwe przenoszenie konfiguracji oraz oprogramowania przełącznika

Obsługa Routingu IPv4
Sprzętowa obsługa routingu IPv4 – forwarding
Pojemność tabeli routingu min. 480 wpisów
Routing statyczny
Obsługa routingu dynamicznego IPv4
RIPv1/v2
OSPFv2 – możliwość rozszerzenia przez licencję oprogramowania
Policy Based Routing dla IPv4
Wbudowana obrona procesora urządzenia przed atakami DoS
Obsługa TACACS+ (RFC 1492)
Obsługa RADIUS Authentication (RFC 2865)
Obsługa RADIUS Accounting (RFC 2866)
RADIUS and TACACS+ per-command Authentication
Obsługa SNMPv1/v2/v3
Klient SSH2
Zabezpieczenie przełącznika przed atakami DoS
Networks Ingress Filtering RFC 2267
SYN Attack Protection
Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania
Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4
Listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika
Obsługa bezpiecznego transferu plików SCP/SFTP
Obsługa DHCP Option 82
Obsługa Gratuitous ARP Protection
Obsługa Trusted DHCP Server
Obsługa DHCP Snooping
Obsługa DHCP Secured ARP/ARP Validation

Aktualizacja oprogramowania routingu i firewall – 6 szt.

Platforma serwerowa
Serwery – 2 szt.
Obudowa: typu rack z możliwością instalacji min. 4 dysków
Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
RAM 256GB, płyta główna powinna posiadać możliwość obsługi do min. 512 GB
Gniazda PCI Minimum:
1 x PCI-Express x16 Gen.3 o przepustowości x8
2 x PCI-Express x8 Gen.3 o przepustowości x4
1 x PCI-Express o przepustowości x1
Interfejsy sieciowe zintegrowane 2 x 10/100/1000
Minimum 8 portów USB z czego minimum 2 na przednim panelu obudowy,
Sprzętowy kontroler umożliwiający konfigurację zabezpieczeń RAID min. 0,1,10,5,50.
Dwa Zasilacze Minimum 450W

Sieciowe systemy operacyjne – 2 szt.

Licencję na serwerowy system operacyjny który musi zapewnić poniżej opisane funkcjonalności dla jednego serwera posiadającego minimum dwa procesory.

Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego (SSO) w środowisku fizycznym i dwóch wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.

Serwerowy system operacyjny (SSO) musi posiadać następujące, wbudowane cechy:

- Możliwość wykorzystania, do 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym
- Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
- Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych.
- Możliwość migracji maszyn wirtualnych z możliwością kompresji danych, bez zatrzymywania ich pracy, między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.

- Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
- Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
- Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.

- Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
- Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
- Graficzny interfejs użytkownika.
- Zlokalizowane w języku polskim.
- 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.
- Oprogramowanie musi być dostarczone w najnowszej wersji

Macierz – 1 szt. o pojemności 100 TB współpracująca za pomocą sieci 10GB/s z dostarczonymi przełącznikami i serwerami

Modernizacja serwerowni

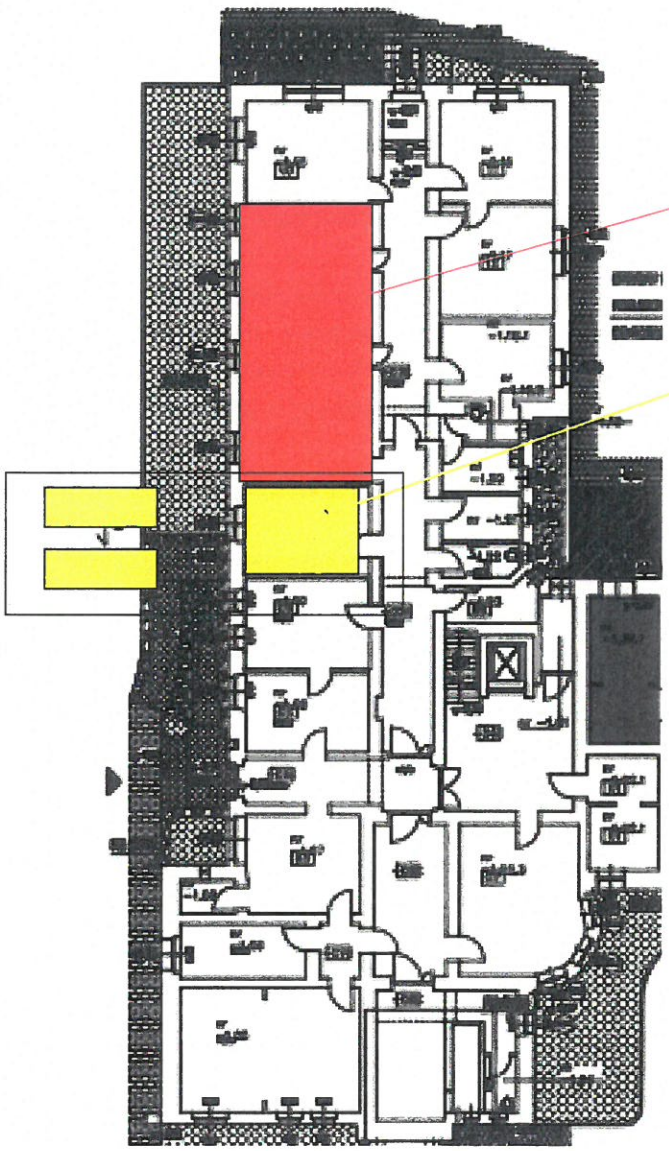
Modernizacja zasilania awaryjnego – 2 szt,

Należy zmodernizować system zasilania awaryjnego poprzez upgrade systemu sterowania z rozwiązań analogowych na rozwiązania mikroprocesorowe. Dzięki temu możliwe będzie zminimalizowanie przestojów infrastruktury a co za tym idzie również eusług. W ramach modernizacji serwerowni wykonane zostaną przeglądy modernizacyjne systemu gaszenia, systemu chłodzenia i bezpieczeństwa.

sprzęt komputerowy – 10 szt.

Zostaną zmodernizowane linki optyczne łączące serwerownie z centrum zarządzania siecią poprzez wymianę wkładek optycznych na wkładki o szybkości minimum 10 Gb/s – 6 szt
Zostaną zakupione 4 stacje zarządzające o minimalnych parametrach: procesor 4 rdzeniowy, 16 GB ram, hdd 512GB

II. Lokalizacja planowanych środków trwałych



Budynek UM Ełk, ul. Piłsudskiego 4, przyziemie

PREZYDENT MIASTA
Tomasz Andrukiewicz

GMINA MIASTO EŁK
19-300 EŁK
ul. Marsz. J. Piłsudskiego 4
REGON 790671076 NIP 848-18-25-438