**OPIS PRZEDMIOTU ZAMÓWIENIA**

**Rozdział 1**

**PRZEDMIOT ZAMÓWIENIA**

Przedmiotem zamówienia jest dostawa i wdrożenie systemu antywirusowego Trend Micro Smart Protection Complete - 300 licencji wraz z 12 miesięcznym wsparciem producenta lub dostawa równoważnego systemu.

**Rozdział 2**

**MIEJSCE WYKONANIA ZAMÓWIENIA**

Miejscem realizacji dostawy i wdrożenia, o których mowa w Rozdziale 1 jest siedziba FRSE w Warszawie przy Alejach Jerozolimskich 142A.

**Rozdział 3**

**WDROŻENIE SYSTEMU** rozumiane jako:

1. Opracowanie projektu technicznego na podstawie wymagań Zamawiającego, dobrych praktyk i rekomendacji producenta.
2. Instalacja serwera OfficeScan Server, Smart Protection Server.
3. Instalacja serwera Control Manager Server.
4. Instalacja serwera baz danych.
5. Przygotowanie polityk ochrony stacji końcowych.
6. Integracja Systemu z MS Active Directory i MS Exchange.
7. Instalacja agentów OfficeScan na 20 stacjach końcowych.
8. Wykonanie testów poprawności działania.
9. Wsparcie przy zdalnej instalacji na 200 stacjach końcowych.
10. Opracowanie dokumentacji powykonawczej.
11. Jednodniowe szkolenie z zakresu administracji i rozwiązywania problemów wdrożonego systemu.

Środowisko, serwery i systemu operacyjne, pod produkty zapewnia Zamawiający.

**Rozdział 4**

**GWARANCJE I WSPARCIE POWDROŻENIOWE.**

1. Wykonawca udzieli Zamawiającemu gwarancji na System na okres min. 6 miesięcy od zakończenia wdrożenia.
2. Wykonawca zapewni wsparcie powdrożeniowe dla Systemu na okres min. 3 miesięcy od zakończenia wdrożenia. Wsparcie będzie obejmowało:
   1. Usuwanie awarii krytycznych Systemu.
   2. Udzielanie porad dla administratorów Systemu.
   3. Dostarczanie aktualizacji Systemu wraz z procedurami ich wdrożenia.

**Rozdział 5**

**ROZWIĄZANIE RÓWNOWAŻNE**

Zamawiający dopuszcza możliwość zaoferowania produktów równoważnych. Zaoferowane oprogramowanie równoważne musi spełniać parametry i posiadać możliwości nie gorsze niż wskazane poniżej przez Zamawiającego.

*Ochrona stacji końcowych.*

Od systemu dedykowanego do ochrony stacji końcowych i serwerów oczekuje się spełniania poniższych wymagań.

*Zarządzanie i wspierane systemy operacyjne*

1. System musi zapewniać ochronę stacji pracowników pracujących pod kontrolą systemów operacyjnych Windows XP/7/8/8.1/10.
2. System musi zapewniać ochronę systemów serwerowych: Windows serwer 2003/2003 R2/ 2008/2008 R2/2012/2016.
3. Zarządzanie systemem bezpieczeństwa powinno być możliwe z poziomu jednej, centralnej konsoli zarządzającej.
4. Konsola zarządzająca powinna umożliwiać, monitorowanie stanu bezpieczeństwa chronionych zasobów, konfigurację polityk bezpieczeństwa oraz przegląd i analizę incydentów bezpieczeństwa wygenerowanych przez system.
5. Aktualizacja bazy sygnatur oraz silników bezsygnaturowych powinna być dostępna 24h na dobę na serwerach producenta oferowanego rozwiązania.
6. Aktualizowanie silników skanujących zainstalowanych na stacjach końcowych powinno odbywać się w sposób automatyczny, zgodnie ze zdefiniowanym harmonogramem, lub na żądanie administratora bezpieczeństwa.
7. Aktualizacja sygnatur oraz silników skanujących nie może wymagać zatrzymania procesu skanowania na jakimkolwiek systemie operacyjnym.
8. Aktualizacja sygnatur oraz silników skanujących nie może wymagać restartu oprogramowania na jakimkolwiek systemie operacyjnym.
9. System musi mieć możliwość wyznaczania stacji, które będą dla wyznaczonych agentów punktem dystrybucyjnym aktualizacji sygnatur, silników skanujących oraz poprawek oprogramowania.
10. System musi mieć możliwość aktualizacji oprogramowania zabezpieczającego udostępnionego przez stację sąsiadującą znajdującą się w tej samej sieci LAN.
11. W ramach ochrony system musi umożliwiać uruchomienie serwera w strefie DMZ w celu utrzymania komunikacji ze stacjami znajdującymi się poza lokalną siecią organizacji.
12. System musi pozwalać na natychmiastowe alarmowanie o aktywności związanej z wirusami w administrowanej sieci na kilka sposobów: raportowanie do systemu centralnego zarządzania, poczta elektroniczna, powiadomienia przez SNMP TRAP, raportowanie do dziennika systemowego.
13. Serwer zarządzający systemu musi mieć możliwość integracji z MS Active Directory zarówno w rozumieniu powielenia struktury komputerów jak i autentykacji administratorów.
14. W celu zagwarantowania bezproblemowej pracy użytkownikowi podczas pełnego skanowania systemu, powinna istnieć polityka umożliwiająca wstrzymanie skanowania gdy obciążenie CPU wzrośnie powyżej zdefiniowanego progu, np. 20%, 50%.
15. System powinien umożliwiać zdefiniowanie polityki pozwalającej na pominięcie zadania pełnego skanowania systemu w przypadku gdy urządzenie (laptop) pracuje na baterii, nie jest podłączone do prądu, a naładowanie baterii jest poniżej zdefiniowanego poziomu, np. 20%, 30%, 40%.

*Mechanizmy zabezpieczające i silniki skanujące.*

1. System musi posiadać silnik analizy sygnaturowej.
2. System musi posiadać możliwość uruchomienia analizy heurystycznej w celu wykrywania nowych, nieznanych wirusów.
3. System musi posiadać możliwość uruchomienia analizy opartej o mechanizmy uczenia maszynowego (ang. Machine Learning). Analizy typu Machine Learning powinna być wykonywana dwuetapowo:
   1. Przed uruchomieniem potencjalnie niebezpiecznego kodu – statyczna analiza właściwości pliku.
   2. Po uruchomieniu pliku – analiza bazującą na analizie zachowania uruchomionego kodu, wykorzystująca pełen potencjał dostawcy oferowanego sytemu, w szczególności integrację z globalną chmurą reputacji.
4. System musi zapewniać wykrywanie niepożądanych, niebezpiecznych i potencjalnie niebezpiecznych aplikacji takich jak: spyware, adware, keylogger, dialer, trojan.
5. System musi zapewniać ochronę przed atakami typu ransomware (np. Cyptolocker) poprzez zablokowanie niezaufanego procesu rozpoczynającego szyfrowanie plików oraz podjęcie próby odzyskania plików już zaszyfrowanych (od czasu uruchomienia procesu nieautoryzowanego szyfrowania do chwili jego zatrzymania).
6. System musi zapewniać automatyczne wykrywanie wirusów oraz raportowanie o zaistniałym incydencie do centralnej konsoli zarządzającej.
7. System musi umożliwiać administratorowi określenie akcji jaka zostanie podjęta w przypadku wykrycia zagrożenia.
8. System musi pozwalać na określenie obszarów skanowania, t.j. pliki, katalogi, napędy lokalne, lokalizacje sieciowe.
9. System musi pozwalać na określenie typów skanowanych plików, momentu ich skanowania (otwarcie, modyfikacja) oraz wykluczenie ze skanowania określonych plików i folderów.
10. System musi udostępniać narzędzia pozwalające na usunięcie i naprawę systemu po wykryci zagrożenia.
11. System musi umożliwiać użytkownikowi uruchomienie skanowania na żądanie w celu weryfikacji pliku lub folderu.
12. System musi posiadać moduł zapory ogniowej (tzw. firewall), który będzie posiadał następujące funkcjonalności:
    1. Zabezpieczenie chronionych systemów przed atakami sieciowymi oraz nieautoryzowanymi próbami dostępu do systemu i skanowaniem jego portów.
    2. Moduł firewall musi posiadać funkcjonalność monitorowania i kontroli, jakie aplikacje łączą się poprzez interfejsy sieciowe. Wskazanie aplikacji objętej polityką powinno być możliwe co najmniej w oparciu o pełną ścieżkę do aplikacji lub o wskazanie odpowiedniego klucza rejestru Windows.
    3. Administrator musi mieć dostępną funkcjonalność definiowania połączeń, które system może inicjować i odbierać.
    4. Administrator musi mieć możliwość definiowania polityk w oparciu o protokoły: TCP, UDP, ICMP, ICMPv6. Program ma pozwalać na zdefiniowanie profili firewall na adresów IP, zakresów adresów IP, pojedynczych stacji lub domen Active Directory.
    5. Konfiguracja zezwalanego i zabronionego ruchu ma się odbywać w oparciu, o co najmniej takie informacje jak: protokół, adresy IP, numery (zakresy) portów.
    6. Zapora powinna posiadać funkcjonalność wykrywania ataków sieciowych kierowanych w stronę chronionej stacji (tzw. IDS).
    7. Zapora ogniowa powinna umożliwiać na automatyczne tworzenie wyjątków w polityce firewall dla aplikacji określonych przez producenta jako bezpieczne. Weryfikacja aplikacji powinna się odbywać w oparciu o globalną chmurę reputacji producenta.
    8. Zapora ogniowa powinna umożliwiać logowanie do centralnego serwera zarządzającego zdarzeń wynikających z naruszenia polityki.
    9. Powinna istnieć możliwość zdefiniowania częstotliwości przesyłania logów wygenerowanych przez firewall na stacji końcowej do centralnego serwera. Możliwy do zdefiniowania interwał powinien wynosić co najmniej od 1min do 1 dnia.
    10. Zapora ogniowa powinna posiadać możliwość włączenia mechanizmu powiadomień użytkownika o zablokowanych aplikacjach (lub procesach).
    11. Oprogramowanie musi mieć funkcjonalność umożliwiająca blokowanie ruchu pomiędzy interfejsami sieciowymi.
13. System musi posiadać możliwość określenia działania reguł i polityk bezpieczeństwa w zależności od lokalizacji, w której znajduje się chroniony.
14. System musi posiadać moduł „kontroli podłączanych urządzeń” (tzw. device control), który będzie posiadał następujące funkcjonalności:
    1. Centralne definiowanie, wdrażanie, zarządzanie i aktualizacja polityki typu device control.
    2. Możliwość ograniczenia dostępu do urządzeń zewnętrznych takich jak: CD/DVD, dyski sieciowe, urządzenia pamięci masowej typu USB, co najmniej w zakresie: ograniczenia dostępu do odczytu, modyfikowania lub uruchomienia plików znajdujących się na urządzeniu lub dysku sieciowym, całkowitego zablokowania możliwość podłączenia danego urządzenia.
    3. W przypadku pamięci masowych typu USB rozwiązanie musi umożliwiać zdefiniowanie listy urządzeń dopuszczonych do użytku wewnątrz organizacji na podstawie numerów seryjnych urządzeń. Pozostałe urządzenia powinny być blokowane.
    4. System musi posiadać możliwość monitorowania również urządzeń innych niż pamięci masowe, takich jak: Portów COM i LPT, Modemów, Kart PCMCIA, Drukarek.
    5. Prezentowanie zdarzeń wygenerowanych przez moduł Device Control w centralnym systemie zarządzania.
15. System musi posiadać moduł ochrony przed wyciekiem danych.
    1. Rozwiązanie musi umożliwiać monitorowanie i powiadamianie o incydentach wycieku danych w czasie rzeczywistym.
    2. Rozwiązanie musi posiadać możliwość kontroli i ochrony danych wrażliwych przy wykorzystaniu co najmniej takich mechanizmów jak:
    3. Wyrażenia regularne: dane o określonej strukturze.
    4. Atrybuty plików.
    5. Słowa kluczowe: Lista wrażliwych słów i wyrażeń.
    6. System musi posiadać gotowe, dostarczane wraz z rozwiązaniem szablony wyrażeń regularnych pozwalające na kontrolę i ochronę danych typowych dla Polski (przykładowo numer dowodu, numer pesel)
    7. System musi posiadać możliwość monitorowania i ochrony następujących kanałów transmisji:
    8. Klienci poczty elektronicznej
    9. Protokoły HTTP i HTTPS
    10. Protokół SMB
    11. Poczta elektroniczna dostępna poprzez stronę Web
    12. Rejestratory Danych ( CD/DVD )
    13. Aplikacje wymiany plików peer-to-peer
    14. Drukarka
    15. Schowek systemu Windows
    16. System musi umożliwiać podjęcie następujących czynności w przypadku wykrycia naruszenia polityki ochrony przed wyciekiem poufnych danych:
    17. Pomiń – program zapewnia i protokołuje transmisję.
    18. Blokuj – program blokuje i protokołuje transmisję.
    19. Powiadom – program wyświetla powiadomienie, aby poinformować użytkownika transmisji danych o umożliwieniu lub zablokowaniu transmisji.
    20. Zachowanie danych rekordów – niezależnie od operacji podstawowej program zapisze dane oznaczone jako naruszenie polityki do dalszej analizy.
16. System musi umożliwiać weryfikację reputacji stron WEB odwiedzanych przez użytkownika i w przypadku wykrycia stron niebezpiecznych zablokować do nich dostęp, a użytkownikowi wyświetlić komunikat o zablokowaniu dostępu do strony niebezpiecznej.
    1. Administrator systemu zabezpieczającego powinien mieć możliwość przygotowania komunikatów, które będę wyświetlane podczas blokowania dostępu do stron.
    2. System powinien umożliwiać sprawdzanie reputacji domen zarówno w przypadku wykorzystania protokołu http jak i HTTPS
    3. Weryfikacja reputacji domen dla protokołu HTTP powinna być wykonywana w sposób bezagentowy.
    4. System powinien wspierać co najmniej następujące przeglądarki internetowe: Microsoft Internet Explorer, Mozilla Firefox, Chrome, Microsoft Edge.
    5. Moduł weryfikacji reputacji domen powinien pozwalać na tworzenie wyjątków poprzez zdefiniowanie listy zaufanych domen oraz listy domen niebezpiecznych, które należy blokować.
17. System powinien posiadać centralną kwarantannę, w której będą mogły zostać umieszczane pliki uznane za niebezpieczne.
18. System musi mieć możliwość wysyłania do zewnętrznego sandboxa potencjalnie niebezpiecznych plików w celu wykonania ich zaawansowanej analizy poprzez detonację ich w odizolowanym środowisku wirtualnym. Rozwiązanie sandbox nie jest przedmiotem tego zapytania.

*Ochrona stacji końcowych za pomocą systemu kontroli aplikacji (tzw. Application Control)*

Od systemu ochrony kontroli aplikacji oczekuje się spełniania poniższych wymagań.

1. Rozwiązanie musi umożliwiać zdefiniowanie zestawu aplikacji, które użytkownik końcowy będzie mógł uruchomić – pozostałe aplikacje powinny być blokowane.
2. Rozwiązanie musi zapewniać ochronę przed uruchamianiem niepożądanych lub nieznanych aplikacji ( plików wykonywalnych, bibliotek DLL, aplikacji Windows, sterowników urządzeń, oraz innych przenośnych plików wykonywalnych (Portable Executable files).
3. Rozwiązanie musi zapewniać mechanizm analizy zagrożeń w czasie rzeczywistym bazujący na globalnej bazie reputacji plików.
4. Rozwiązanie w celu kontroli aplikacji musi wykorzystywać polityki zawierające zdefiniowane reguły z trzema metodami kontroli aplikacji:
   1. Zezwól(Allow) – reguły zezwalające na uruchomienie określonych, wyspecyfikowanych aplikacji,
   2. Blokuj (Block – reguły blokują określone, wybrane aplikacje lub aplikacje nie określone w regułach typu „Allow”,
   3. Izolacja (Lockdown) – blokuje aplikacje dodane po zastosowaniu reguły typu „Lockdown” z możliwością użycia określonych warunków na zezwolenie uruchomienia aplikacji.
5. Agent powinien być dostępny i wspierany na następujących systemach operacyjnych w wersjach:
   1. Windows (x86/x64) 7
   2. Windows (x86/x64) 8, 8.1
   3. Windows 10
6. Agent musi posiadać mechanizmy zapobiegania zatrzymaniu lub odinstalowaniu przez użytkownika końcowego, zewnętrzną aplikację lub proces.
7. Funkcjonalność kontroli aplikacji powinna być zarządzania za pomocą jednego centralnego serwera zarządzającego.

*Dodatkowa ochrona stacji końcowych przed atakami wykorzystującymi podatności systemu operacyjnego i aplikacji*

Od systemu dodatkowej ochrony stacji końcowych przed atakami wykorzystującymi podatności systemu operacyjnego i aplikacji oczekuje się spełniania poniższych wymagań.

1. Rozwiązanie klasy Host IPS powinno chronić systemy użytkowników przed znanymi podatnościami za pomocą dostarczanych przez producenta sygnatur.
2. Rozwiązanie Host IPS powinno wykrywać skanowania portów, chronić przed atakami sieciowymi oraz wykorzystującymi znane podatności aplikacji oraz systemów operacyjnych.
3. Rozwiązanie powinno dysponować funkcjonalnością skanu rekomendacji, polegającej na wykrywaniu występujących na danej stacji podatności, a następnie uruchomieniu tylko tych sygnatur, które są związane z wykrytymi podatnościami.
4. Ochrona Host IPS powinna być zapewniona dla stacji pracujących pod kontrolą co najmniej następujących systemów operacyjnych:
   1. Windows (x86/x64) 7
   2. Windows (x86/x64) 8, 8.1
   3. Windows 10
5. Rozwiązanie Host IPS powinno być zarządzany za pomocą jednego centralnego serwera.

*Ochrona urządzeń mobilnych*

Od systemu dedykowanego do ochrony urządzeń mobilnych oczekuje się spełniania poniższych wymagań.

1. System musi umożliwiać ochronę systemów operacyjnych Apple iOS oraz Android w następujących wersjach:
   1. iOS: 6.x, 7.x, 8.x, 9.x, 10.x, 11.x
   2. Android: 4.0, 4.1, 4.2, 4.3, 4.4, 5.0, 5.1, 6.0, 7.0, 7.1, 8.0
2. Zarządzenie systemem ochrony urządzeń mobilnych powinno odbywać się z poziomy jednej centralnej konsoli.
3. Komunikacja z chronionymi urządzeniami mobilnymi musi być możliwa co najmniej poprzez dedykowany serwer zainstalowany w infrastrukturze zamawiającego (wdrożony w sieci DMZ) lub za pośrednictwem serwera dostarczanego i utrzymywanego przez dostawcę systemu i zlokalizowanego w jego infrastrukturze (tzw. chmura)
4. System musi umożliwiać skonfigurowanie polityki bezpieczeństwa dotyczącej szyfrowania urządzeń mobilnych oraz wymuszenia stosowania kodu pin przy odblokowywaniu urządzenia.
5. Administrator musi mieć możliwość przygotowania i zarządzania konfiguracją sieci bezprzewodowych WiFi.
6. System musi umożliwiać całkowite usunięcie danych z urządzania w sposób zdalny.
7. System musi pozwalać na utworzenie lokalnego, firmowego sklepu z aplikacjami (tzw. Enterprise App Store)
8. System musi umożliwiać instalację na urządzeniu modułu Anti-Malware chroniącego urządzania przed niebezpiecznym kodem oraz niebezpiecznymi aplikacjami. Moduł Anti-Malware powinien posiadać co najmniej następujące funkcjonalności:
   1. Wykrywanie niebezpiecznego kodu na urządzeniu mobilnym za pomocą analizy Machine Learning. Analiza typu Machine Learning powinna być wykonywana co najmniej w przypadku wykrycia nowych, nieznanych plików aplikacji. W przypadku wykrycia niebezpiecznego kodu rozwiązanie powinno zablokować możliwość instalacji aplikacji lub poinformować użytkownika o koniczności odinstalowania aplikacji i usunięcia pliku.
   2. Rozwiązanie powinno wykonywać co najmniej skanowanie zainstalowanych aplikacji, ruchu sieciowego kierowanego do urządzenia pod kątem obecności zagrożeń i ataków, występowania na urządzeniu certyfikatów SSL uznanych za niebezpieczne lub skompromitowane.
   3. Na urządzeniach pracujących pod kontrolą systemu Android skanowanie powinno odbywać się w sposób automatycznych. W przypadku urządzeń pracujących pod kontrolą systemu iOS dopuszcza się konieczność uruchomienia zadania skanowanie manualnie, przez użytkownika.
9. System musi zapewniać integrację z usługą Active Directory.

*Ochrona ruchu e-mail na bramie Internetowej*

Od systemu dedykowanego do ochrony ruchu e-mail oczekuje się spełniania poniższych wymagań.

1. System musi być dostarczony w formie urządzenia wirtualnego umożliwiającego pracę w środowisku VMware.
2. Interfejs zarządzający systemu musi być dostępny przez przeglądarkę internetową i połączenie https.
3. System musi umożliwiać skanowanie protokołów SMTP oraz POP3.
4. System musi umożliwiać pracę w trybie transparent bridge.
5. System musi wykrywać próby ataków typu PHISHING, SPAM, VIRUS, SPYWARE, DIRECTORY HARVEST, BEC (Business Email Compromise).
6. System musi umożliwiać wysyłanie wiadomości SNMP oraz powiadomień w formie poczty elektronicznej dla zdefiniowanych zdarzeń oraz do zdefiniowanych odbiorców.
7. System musi posiadać możliwość monitorowania z zewnątrz za pomocą SNMP.
8. System musi posiadać centralna kwarantannę obsługiwaną przez administratora lub bezpośrednio przez użytkowników poprzez przeglądarkę.
9. System musi umożliwiać stworzenie kilku typów kwarantanny.
10. System musi posiadać mechanizmy automatycznego i regularnego (zgodnego z harmonogramem) powiadamiania użytkowników o zawartości kwarantanny.
11. System musi mieć możliwość konfiguracji, w której wirusy lub ataki konkretnego typu (np. mass mailing) są zawsze usuwane bez powiadamiania użytkowników.
12. Rozwiązanie powinno umożliwiać integrację z zewnętrznym środowiskiem typu sandbox tego samego producenta w celu dokonywania zaawansowanej analizy załączników bez potrzeby wysyłania ich do chmury producenta. Skanowanie w środowisku sandbox powinno odbywać się wewnątrz chronionej infrastruktury informatycznej. Integracja powinna polegać co najmniej na możliwości wysyłania podejrzanych załączników do zewnętrznego środowiska typu sandbox, odbieranie wyników analizy załączników z zewnętrznego środowiska sandbox oraz podejmowanie na podstawie otrzymanych wyników odpowiednich, zdefiniowanych akcji.
13. System musi umożliwiać definiowanie administratorów o różnych rolach administracyjnych i różnych poziomach dostępu.
14. System musi być wyposażony w moduł Antyspamowy.
15. System musi współpracować z serwerami LDAP pozwalając na stworzenie dokładnej polityki skanowania per email adres lub np. grupa użytkowników w Active Directory.
16. System musi obsługiwać białe listy adresów email definiowane przez administratora oraz przez końcowych użytkowników.
17. System musi posiadać filtr reputacyjny wykorzystujący globalną chmurę reputacji producenta, będącą zbiorem skorelowanych reputacji co najmniej stron WWW, plików oraz adresów email.
18. System musi umożliwiać skanowanie wychodzącej poczty pod kątem AV oraz heurystyką antyspamową.
19. System musi stosować filtry wykrywające spam w oparciu o techniki heurystyczne.
20. System musi umożliwiać wykorzystanie wyrażeń regularnych do definiowania polityk zapobiegających wyciekowi danych.
21. System musi stosować techniki filtrowania zawartości treści w oparciu o zdefiniowane słowa kluczowe.
22. System powinien pozwalać na definiowanie własnych nagłówków X-Headers.
23. System musi zapewniać ochronę przed wyciekiem danych wrażliwych.
    1. Moduł ochrony przed wyciekiem danych musi być integralną częścią rozwiązania.
    2. System musi posiadać możliwość kontroli i ochrony danych wrażliwych przy wykorzystaniu co najmniej takich mechanizmów jak:
       1. Wyrażenia regularne: Dane o określonej strukturze.
       2. Atrybuty plików: Właściwości plików, takie jak typ i rozmiar
       3. Słowa kluczowe: Lista wrażliwych słów i wyrażeń.
    3. System musi posiadać gotowe, dostarczane wraz z rozwiązaniem szablony wyrażeń regularnych pozwalające na kontrolę i ochronę danych typowych dla Polski (przykładowo numer dowodu, numer pesel).
    4. Konfiguracja polityki dotyczącej ochrony przed wyciekiem danych dla urządzeń końcowych, bramy email oraz bramy web powinna być konfigurowana z tej samej centralnej konsoli.

*Ochrona ruchu web na bramie Internetowej*

Od systemu dedykowanego do ochrony ruchu web oczekuje się spełniania poniższych wymagań.

1. Brama musi być dostarczona w formie wirtualnego sytemu typu appliance wspieranego kompatybilnego z następującymi systemami wirtualizacji:
   1. ESX oraz ESXi 4.0 i nowszymi
2. Interfejs zarządzający urządzenia dostępny przez przeglądarkę internetową i połączenie https.
3. Brama powinna działać na poziomie sieciowym i wspierać protokoły: FTP, HTTP, HTTPS.
4. Brama powinna umożliwiać pracę w następujących trybach: reverse-proxy, upstream-proxy, standalone, forward proxy, transparent bridge, ICAP, WCCP.
5. Brama musi wykrywać i blokować oprogramowanie szpiegujące typu spyware/greyware/malware w protokole http.
6. Brama musi wykrywać i blokować zagrożenia typu Phishing i Pharming w oparciu Usługi Potwierdzeń Reputacji.
7. Brama musi umożliwiać blokowanie skryptów oraz ActiveX.
8. Brama musi przechwytywać pliki skompresowane z możliwością co najmniej następujących akcji: blokuj, przepuszczaj.
9. Brama musi skanować media strumieniowe oraz umożliwiać wyłączanie ze skanowania pewnych ich typów.
10. Brama musi umożliwiać blokowanie klientów Instant Messaging tunelowanych http.
11. Brama musi pozwalać na stworzenie dokładnej polityki skanowania w oparciu o adresację IP, hostname (http header) oraz użytkownika lub grupę w LDAP..
12. Brama musi umożliwiać kategoryzacje stron WWW.
13. Brama musi raportować do centralnego serwera i zintegrowanego z oprogramowaniem systemowym oraz mieć możliwość zarządzania z pojedynczego punktu.
14. Brama musi pozwalać na raportowanie zablokowanych wywołań WWW do centralnej konsoli zarządzającej.
15. Brama musi umożliwiać uaktywnienie usługi potwierdzeń reputacji, pozwalającej na sprawdzanie co najmniej reputacji otwieranych przez użytkowników stron WWW poprzez wysyłanie odpowiednich zapytań do chmury reputacji producenta rozwiązania.
16. Brama musi posiadać możliwość kontroli aplikacji korzystających z Internetu pozwalając administratorom monitorować i aktywnie zarządzać poprzez odpowiednie polityki.
17. Brama musi zezwalać na inspekcję ruchu http oraz aktywne przeciwdziałanie na przykład poprzez nakładane polityki ograniczające użytkownikom transfer dużych plików.
18. Brama musi umożliwiać ominięcie ograniczeń nałożonych przez administratora poprzez podanie zdefiniowanego hasła po stronie użytkownika.
19. Brama musi zezwalać na zdefiniowanie czasu jaki użytkownicy mogą spędzić na przeglądaniu stron internetowych nie związanych bezpośrednio z charakterem wykonywanej pracy.
20. Brama musi umożliwiać bezpieczne rozszyfrowanie i skanowanie ruchu HTTPS dla zdefiniowanych kategorii stron internetowych.
21. Brama musi umożliwiać pracę w trybie wysokiej dostępności (HA)
22. Brama musi wykrywać wywołania wsteczne (callback) dla serwerów zarządzających (C&C) sieci botnetowych.
23. Brama musi posiadać silnik emulacji przeglądarki internetowej w celu wykrywania złośliwych treści web. Silnik musi działać w czasie rzeczywistym.
24. Brama musi umożliwiać integrację z zewnętrznym środowiskiem typu sandbox tego samego producenta w celu dokonywania zaawansowanej analizy plików bez potrzeby wysyłania ich do producenta. Skanowanie w środowisku sandbox powinno odbywać się wewnątrz chronionej infrastruktury informatycznej. Integracja powinna polegać co najmniej na możliwości wysyłania podejrzanych plików do zewnętrznego środowiska typu sandbox, odbieranie wyników analizy plików z zewnętrznego środowiska sandbox oraz podejmowanie na podstawie otrzymanych wyników odpowiednich, zdefiniowanych akcji.
25. Brama musi posiadać zaawansowane mechanizmy skanujące pobierane pliki i dokumenty w celu wykrycia dołączonego złośliwego kodu lub oprogramowania.
26. Brama, musi dostarczać raporty pozwalające na dokładną identyfikację docelowych użytkowników oraz grup.
27. Brama musi umożliwiać synchronizację polityk oraz konfiguracji pomiędzy instancjami bez potrzeby instalacji dodatkowego oprogramowania.
28. Brama musi umożliwiać synchronizację polityk oraz konfiguracji w sposób w pełni zautomatyzowany lub wymuszony ręcznie.
29. Rozwiązanie musi pozwalać na konfigurację polityk z centralnej konsoli zarządzającej bez potrzeby logowania się na konsolę bramy.
30. W przypadku korzystania przez użytkownika z Internetu bądź aplikacji wykorzystującej Internet rozwiązanie powinno pozwalać na zdefiniowanie treści powiadomienia naruszającego politykę.
31. Brama, lub element raportujący, musi pozwalać na konsolidację raportów z wielu rozproszonych instancji bez potrzeby instalowania dodatkowej centralnej konsoli zarządzającej.
32. Brama, lub element raportujący, musi umożliwiać stworzenie raportów w czasie zbliżonym do rzeczywistego o aktywnych użytkownikach lub aktualnie wizytowanych stronach WWW z podziałem na kategorię URL.
33. Brama, lub element raportujący, musi umożliwiać zapisywanie raportów do formatu co najmniej pdf.
34. Brama musi umożliwiać integrację z zewnętrznym środowiskiem typu sandbox tego samego producenta w celu dokonywania zaawansowanej analizy plików bez potrzeby wysyłania ich do producenta. Skanowanie w środowisku sandbox powinno odbywać się wewnątrz chronionej infrastruktury informatycznej. Integracja powinna polegać co najmniej na możliwości wysyłania podejrzanych plików do zewnętrznego środowiska typu sandbox, odbieranie wyników analizy plików z zewnętrznego środowiska sandbox oraz podejmowanie na podstawie otrzymanych wyników odpowiednich, zdefiniowanych akcji.
    1. Informacja o wykryciu przez sandbox niebezpiecznego kodu powinna nie tylko zostać przesłana do sytemu, który dostarczył próbkę do sandboxa ale również do pozostałych systemów chronionych oferowanym systemem bezpieczeństwa.
35. System musi zapewniać ochronę przed wyciekiem danych wrażliwych.
    1. Moduł ochrony przed wyciekiem danych musi być integralną częścią rozwiązania.
    2. System musi posiadać możliwość kontroli i ochrony danych wrażliwych przy wykorzystaniu co najmniej takich mechanizmów jak:
       1. Wyrażenia regularne: Dane o określonej strukturze.
       2. Atrybuty plików: Właściwości plików, takie jak typ i rozmiar
       3. Słowa kluczowe: Lista wrażliwych słów i wyrażeń.
    3. System musi posiadać gotowe, dostarczane wraz z rozwiązaniem szablony wyrażeń regularnych pozwalające na kontrolę i ochronę danych typowych dla Polski (przykładowo numer dowodu, numer pesel).
    4. Konfiguracja polityki dotyczącej ochrony przed wyciekiem danych dla urządzeń końcowych, bramy email oraz bramy web powinna być konfigurowana z tej samej centralnej konsoli.

*Ochrona zaimplementowana na serwerze Exchange*

Od systemu ochrony zaimplementowanego na serwerze Exchange oczekuje się spełniania poniższych wymagań.

1. Rozwiązanie musi wspierać następujące wersje systemów Exchange:
   1. Exchange Server 2016
   2. Exchange Server 2013
   3. Exchange Server 2010
2. Rozwiązanie powinno wykonywać analizę wiadomości email co najmniej pod kątem:
   1. Detekcji niechcianej poczty, tzw. SPAM
   2. Detekcji niebezpiecznych wiadomości email poprzez analizę:
      1. Treści wiadomości
      2. URL’i znajdujących się w wiadomości
      3. Załączników
3. Rozwiązanie powinno umożliwiać zarówno aktualizację bazy zagrożeń w sposób automatyczny jak i na żądanie.
4. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie może wymagać zatrzymania procesu skanowania na jakimkolwiek systemie operacyjnym.
5. Rozwiązanie musi umożliwiać obsługę plików skompresowanych.
6. Rozwiązanie musi umożliwiać definiowanie czarnych i białych list nadawców, odbiorców, domen internetowych, itp.
7. Rozwiązanie musi umożliwiać dodawania własnych reguł ochrony zawartości.
8. Rozwiązanie musi umożliwiać współpracę z serwerami LDAP pozwalając na stworzenie dokładnej polityki skanowania per adres email lub np. Grupę użytkowników w Active Directory.
9. Rozwiązanie musi posiadać możliwość automatycznego usuwania wirusów i zgłaszania alertów w przypadku wykrycia zagrożenia.
10. Rozwiązanie musi umożliwiać usuwanie tylko i wyłącznie niebezpiecznych elementów (np. załącznik w przesyłce e-mail ) z analizowanych danych.
11. Zarządzanie musi odbywać się poprzez przeglądarkę WWW lub centralnie z poziomu jednolitego systemu centralnego zarządzania dla systemu Anti-Malware opisanego powyżej.

*Ochrona zaimplementowana na serwerze SharePoint*

Od systemu ochrony zaimplementowanego na serwerze SharePoint oczekuje się spełniania poniższych wymagań.

1. Rozwiązanie musi aktywnie chronić serwery SharePoint przed plikami zawierającymi niebezpieczny kod, poprzez zablokowanie tych plików i uniemożliwienie ich umiejscowienia na serwerze SharePoint przez użytkownika sytemu.
2. Rozwiązanie musi umożliwiać zdefiniowanie polityki uniemożliwiającej na umieszczenie na serwerze SharePoint typów plików uznanych za pliki wysokiego ryzyka (np. Pliki wykonywalne).
3. Rozwiązanie musi umożliwiać analizę linków udostępnianych za pomocą SharePoint i blokując dostęp do stron uznanych za niebezpieczne.
4. Rozwiązanie musi wspierać co najmniej:
   1. SharePoint Server 2010
   2. SharePoint Server 2013
   3. SharePoint Server 2016

*Ochrona dedykowana do ochrony Office 365*

Od systemu ochrony Office 365 oczekuje się spełniania poniższych wymagań.

1. Rozwiązanie musi zapewniać ochronę usługi Office 365 co najmniej w zakresie Anti-Malware, Anit-Spam.
2. Rozwiązanie zabezpieczające powinno integrować się z usługą Office 365 za pomocą dostarczonego przez dostawcę usługi Office 365, firmę Microsoft API.
3. Rozwiązanie musi być dostarczona przez tego samego producenta co rozwiązanie antywirusowe dedykowane do ochrony stacji końcowych, opisane powyżej.