**Załącznik nr 1**

Numer sprawy: PK XII BIA 0412.11.2018.7

**Przedmiot zamówienia:** *Dostawa sprzętu i oprogramowania dla infrastruktury techniczno-systemowej* w ramach projektu „Rozwój Systemu Digitalizacji Akt Postępowań Przygotowawczych (iSDA)”, współfinansowanego ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa, Oś priorytetowa nr 2 „E-Administracja i otwarty rząd”

**Podstawowy zakres obowiązków Wykonawcy i założenia realizacji umowy**

Prokuratura Krajowa realizuje projekt „Rozwój Systemu Digitalizacji Akt Postępowań Przygotowawczych (iSDA)”, współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa, Oś priorytetowa nr 2 „E-Administracja i otwarty rząd”, Działanie 2.1, w ramach którego wykonawca zaprojektuje, przygotuje i wdroży system informatyczny.

Celem przedmiotowego postępowania jest utworzenie środowiska aplikacyjnego i bazodanowego Systemu iSDA.

Do obowiązków Wykonawcy w ramach realizacji zamówienia należeć będzie:

1. Dostawa licencji oprogramowania:
* System zabezpieczenia antywirusowego

Liczba licencji:

* 80 CPU (maszyny wirtualne),
* 16 serwerów fizycznych.

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
|  | System bezpieczeństwa, umożliwiający ochronę różnych systemów serwerowych (fizycznych oraz wirtualnych) w zakresie anty-malware, reputacji sieciowej, wykrywania i przeciwdziałania włamaniom oraz monitorowania integralności systemu plików |
| **Architektura systemu** | System musi posiadać architekturę dwu-warstwową, tzn. musi składać się z centralnej konsoli zarządzania oraz agentów zainstalowanych na serwerach. Centralna konsola zarządzania musi umożliwiać definiowanie polityk bezpieczeństwa (także ich przypisywanie do konkretnych maszyn oraz ich grup), zbieranie logów oraz generowanie raportów, a także zarządzanie agentami (ich aktualizacje, dystrybucja, konfiguracja). Agent odpowiada za faktyczną ochronę systemu na którym został zainstalowany. W szczególnym przypadku środowiska Vmware musi być możliwość uruchomienia także ochrony bez-agentowej, gdy funkcje poszczególnych agentów z maszyn wirtualnych oddelegowane są do pojedynczej maszyny tzw. virtual appliance, chroniącej wszystkie systemy w obrębie jednego hypervisor’a. |
| **Wsparcie dla systemów operacyjnych** | 1. Windows Server 2008, oraz 2008 R2 32-bit oraz 64-bit
2. Windows Server 2012 oraz 2012 R2 64-bit
3. Windows 10 32-bit oraz 64-bit
4. Windows Server 2016 64-bit
5. Red Hat Enterprise Linux 5,6,7 32-bit oraz 64-bit CentOS 5,6,7 32-bit oraz 64-bit
6. Oracle Linux 5,6,7 64-bit
7. SUSE Linux Enterprise Server 11 oraz 12
8. Ubuntu 14 oraz 16 64-bit
9. Cloud Linux 6,7 64-bit
10. Solaris 9, 10, 11 (Sparc oraz x86, x64)
 |
|  | Agent o budowie modularnej – wszystkie wymienione poniżej funkcje agenta powinny być realizowane w jednej aplikacji. Uruchomienie dodatkowych funkcji (modułów) nie może wymagać instalacji dodatkowych aplikacji i odbywa się poprzez ich włączenie w konsoli zarządzającej |
| **Ochrona przed malware oraz reputacja sieciowa (web reputation)** | Ochrona przed znanymi oraz nieznanymi zagrożeniami. System zabezpieczeń serwerów powinien chronić przed znanymi oraz nieznanymi zagrożeniami przy pomocy różnych silników skanujących. Ochrona powinna wykorzystywać najnowocześniejsze mechanizmy, w tym algorytmy uczenia maszynowego oraz monitorowanie zachowania kodu w celu detekcji oraz blokowania zagrożeń. |
|  | Rozwiązanie musi umożliwiać wybór obszarów skanowania anty-malware, momentu skanowania (otwarcie i/lub modyfikacja pliku) oraz typów skanowanych plików. Musi być możliwe wykluczenie ze skanowania określonych obszarów dla:1. skanowania w czasie rzeczywistym,
2. ręcznego skanowania,
3. skanowania określonego w harmonogramie;
 |
|  | Musi być możliwość wymuszenia skanowania „na żądanie” w każdej chwiliOprogramowanie musi zapewniać określenie harmonogramu skanowania (dla pojedynczych maszyn oraz grup) |
|  | Oprogramowanie musi stosować mechanizm skanowania nowych bądź zmienionych plików w celu skrócenia czasu skanowania oraz zwiększenia wydajności skanowania; |
|  | W przypadku wykrycia złośliwego oprogramowania oprogramowanie musi mieć możliwość podjęcia predefiniowanej akcji, takiej jak: czyszczenie, kwarantanna, usunięcie, przepuszczenie, a także raportowania o zdarzeniach w formie co najmniej: e-mail, SNMP TRAP. |
|  | Oprogramowanie antywirusowe musi posiadać funkcjonalność ciągłego, bieżącego i automatycznego wykrywania zagrożeń typu: „greyware”, „adware", „spyware" , „keylogger”, „dialer”, „malware” , „trojan”; |
|  | Oprogramowanie antywirusowe musi posiadać skuteczną ochronę przed zagrożeniami typu „ransomware”; Ochrona powinna także mieć możliwość wykrycia podejrzanego zachowania kodu (polegającego na szyfrowaniu dużej ilości plików), z możliwością jego zablokowania oraz odtworzenia pierwszych zaszyfrowanych plików z pamięci.  |
|  | System nie może wymagać restartu chronionych maszyn wirtualnych i serwerów po dokonaniu aktualizacji mechanizmów skanujących oraz definicji wirusów; |
|  | Oprogramowanie do ochrony serwerów musi posiadać funkcję automatycznego blokowania połączeń do adresów URL na podstawie ich reputacji i kategorii określonych przez producenta systemu, również w przypadku, gdy połączenia te są nawiązywane przez procesy działające na chronionych serwerach.  |
|  | Baza danych o adresach URL musi być na bieżąco utrzymywana przez producenta oprogramowania. Musi istnieć możliwość stworzenia lokalnej repliki tej bazy, synchronizującej się z chmurą producenta, tak aby chronione maszyny nie musiały kontaktować się z nią bezpośrednio przez Internet. |
|  | Musi istnieć możliwość zdefiniowania statycznej listy adresów URL do zablokowania |
|  | Rozwiązanie powinno pozwalać na powiadamianie użytkownika w przypadku skorzystania z niebezpiecznych zasobów lub pobrania niebezpiecznego pliku, zarówno w trybie  |
| **Monitorowanie integralności oraz inspekcja logów** | System musi, na podstawie zdefiniowanych kryteriów, pozwalać na monitorowanie wskazanych plików, katalogów, serwisów, wpisów w rejestrach oraz procesów oraz na informowanie o zmianach, które w nich nastąpiły |
|  | W przypadku serwerów wirtualnych działających pod kontrolą systemu Windows na platformie VMware system musi posiadać możliwość monitorowania wskazanych plików i informowania o wprowadzanych zmianach bez konieczności instalowania dedykowanego agenta na chronionym serwerze (w trybie bez-agentowym) |
|  | Informacja o wprowadzonych zmianach musi zawierać co najmniej:1. nazwę użytkownika lub procesu, który wprowadził zmianę
2. nazwę pliku lub wpisu w rejestrze, w którym została wprowadzona zmiana
3. datę i czas wprowadzenia zmiany
4. nazwę serwera, na którym została wprowadzona zmiana
5. nazwę reguły, która została wykorzystana
 |
|  | Musi być predefiniowany zestaw reguł dostarczonych przez producenta oprogramowania określających ważne, z punktu widzenia ochrony, kryteria monitorowania dla:1. plików
2. wpisów w rejestrach
3. monitorowanych serwisów

w zależności od rodzaju i wersji systemu operacyjnego oraz aplikacji działających na chronionym serwerze |
|  |  |
|  | Musi istnieć możliwość ręcznego definiowania listy monitorowanych plików oraz wpisów w rejestrach przez administratora systemu |
|  | Oprogramowanie musi posiadać funkcję definiowania wyjątków dla plików znajdujących się w monitorowanym katalogu |
|  | Oprogramowanie antywirusowe musi umożliwiać kontrolę integralności hypervisora środowiska wirtualnego z poziomu jednej konsoli zarządzającej; |
|  | Oprogramowanie musi posiadać funkcjonalność zbierania oraz analizy logów pochodzących ze wskazanych systemów, a także aplikacji |
|  | Oprogramowanie musi posiadać predefiniowane reguły, dostarczone przez producenta, określające wskazane do zbierania i analizy logi, w zależności od chronionego systemu oraz aplikacji |
|  | Oprogramowanie musi umożliwiać ręczne definiowanie reguł zbierania i analizowanych logów |
|  | Oprogramowanie antywirusowe musi posiadać funkcjonalność dokonywania analizy logów co najmniej w formatach: 1. apache
2. Eventlog
3. Iis
4. Mysql
5. Nmapg
6. Postfix
7. postgresql
8. snort
9. squid
10. syslog
 |
|  | Oprogramowanie musi posiadać funkcję analizowania nieustandaryzowanych logów z aplikacji i systemów, w szczególności logów w postaci pojedynczej linijki tekstu |
|  | Oprogramowanie musi posiadać funkcję sugerowania administratorowi rekomendowanych do włączenia reguł inspekcji logów, definiowanych i dostarczanych przez producenta, niezależnie dla każdego chronionego serwera, w zależności od systemu operacyjnego oraz działających na nim aplikacji |
|  | Musi istnieć mechanizm automatycznego uruchamiania rekomendowanych reguł opisanych w poprzednim punkcie |
|  | Oprogramowanie musi posiadać funkcjonalność definiowania poziomu krytyczności każdej z reguł logów |
|  | Oprogramowanie musi posiadać funkcjonalność tworzenia polityk stanowiących zbiór reguł dostarczonych przez producenta oraz zdefiniowanych przez administratora |
| **3. Zapora ogniowa oraz system wykrywania i przeciwdziałania włamaniom (intrusion prevention, IPS)** | Oprogramowanie musi pozwalać na kontrolę oraz blokowanie aplikacji próbujących uzyskać połączenie z Internetem lub siecią lokalną |
|  | Oprogramowanie musi posiadać predefiniowaną bazę reguł dla najpopularniejszych aplikacji  |
|  | Oprogramowanie musi umożliwiać wykrywanie oraz blokowanie ataków typu XSS (cross-site-scripting) oraz SQL injection, wraz z możliwością ustanowienia progów dla generowanych alarmów |
|  | Musi istnieć prosty mechanizm przełączania z trybu monitorowania zdarzeń w tryb blokowania dla całego zestawu reguł dla danej maszyny lub grupy maszyn |
|  | Moduł wykrywania oraz przeciwdziałania włamań musi posiadać mechanizm zapewniający blokowanie transmisji na podstawie zdefiniowanej charakterystyki (sygnatury ruchu oraz zdefiniowane ciągi znaków - pattern). Blokowanie musi być możliwe zarówno w trybie pracy z agentem lub bez-agentowo (w przypadku środowisk VMware na to pozwalających) |
|  | Oprogramowanie powinno zawierać wbudowany zestaw reguł IPS, dostarczonych przez producenta, który może zostać zaaplikowany na podstawie rekomendacji dla danej maszyny, w zależności od zainstalowanych aplikacji, systemu operacyjnego oraz aktualnie wgranych poprawek |
|  | Stwierdzenie, które reguły IPS mają zostać zaaplikowane na danej maszynie musi odbywać się automatycznie na podstawie porównania, stanu aktualizacji danego systemu z zestawem znanych podatności i brakujących poprawek bezpieczeństwa |
|  | W przypadku stwierdzenia braku wymaganych poprawek w systemie operacyjnym i aplikacjach powinna nastąpić automatyczna instalacja reguł IPS, aby ochronić cały system przed wykrytymi podatnościami |
|  | W przypadku, gdy dana poprawka, pochodząca od producenta aplikacji lub/i systemu operacyjnego, zostanie już wgrana musi nastąpić automatyczne usunięcie odpowiadających jej reguł IPS |
|  | Komponentem agenta musi być dwukierunkowy stanowy firewall (stateful) zapewniający izolację interfejsów bez konieczności restartów chronionych serwerów. Filtrowanie ruchu musi być możliwe zarówno w trybie pracy z agentem lub bez-agentowo (w przypadku środowisk VMware na to pozwalających) |
|  | Oprogramowanie musi wspierać zarówno protokół IPv4 oraz IPv6 |
|  | Oprogramowanie musi umożliwiać kontrolę połączeń sieciowych, wychodzących i przychodzących, z możliwością kontroli niestandardowych portów TCP (reguły definiowane na podstawie numeru protokołu oraz typu ramki i flag TCP) |
|  | Musi istnieć możliwość szybkiego przełączenia reguł zapory ogniowej z trybu tylko detekcji na tryb blokowania dla danej maszyny lub grupy maszyn |
|  | Firewall musi mieć możliwość blokowania ruchu, w którym wystąpiły naruszenia definicji protokołów oraz inne anomalie, w tym w szczególności: zdeformowanych pakietów, brakujących flag, pakietów typu X-mass itp. |
|  | Oprogramowanie antywirusowe musi posiadać możliwość definiowania polityk firewall oraz IPS dla każdego serwera wirtualnego oddzielnie działających zarówno na ruchu pomiędzy środowiskiem VMware i zewnętrznym środowiskiem, jak i na ruchu pomiędzy maszynami wirtualnymi; |
|  | Oprogramowanie antywirusowe musi posiadać funkcjonalność inspekcji HTTPS bez konieczności instalacji dodatkowego oprogramowania, po wgraniu odpowiednich certyfikatów do konsoli zarządzającej |
| **Zarządzanie** | Oprogramowanie musi realizować funkcję hierarchii nadawania uprawnień i delegacji uprawnień administratorów, zarówno dla grup jak i poszczególnych obiektów w szczególności: użytkowników, maszyn wirtualnych, ról, polityk, funkcjonalności; |
|  | Oprogramowanie antywirusowe musi posiadać mechanizm kontroli aplikacji uniemożliwiający na instalowanie jakichkolwiek niezatwierdzonych do działania w środowisku aplikacji. Oprogramowanie antywirusowe musi posiadać możliwość otwierania tzw. „okien czasowych”, w których zespoły mogą wprowadzać zmiany do konfiguracji aplikacji na serwerach; |
|  | Oprogramowanie antywirusowe musi mieć funkcjonalność generowania i wysyłania e-mailem na zdefiniowany adres raportów w wybranym formacie ( co najmniej .pdf); |
|  | Oprogramowanie musi posiadać ciągle i automatycznie identyfikować i rejestrować zdarzenia, które wpływają lub mogą wpływać na bezpieczeństwo. |
|  | Musi być możliwość wyświetlania listy zdarzeń zidentyfikowanych przez oprogramowanie oraz automatycznego wyboru trybu przekazywania zdarzeń w formie zbioru informacji do centralnego serwera lub systemu typu SIEM (wg. predefiniowanego wyboru administratora) z wykorzystaniem szyfrowanego kanału komunikacji.  |
|  | Administrator systemu musi mieć możliwość zdefiniowania centralnego systemu SIEM lub odrębnych systemów dla każdej z polityk, grup chronionych serwerów lub pojedynczych serwerów; |
|  | Konsola zarządzająca oprogramowania musi posiadać API pozwalające na jego integrację z zewnętrznymi systemami zarządzającymi firm trzecich.  |
|  | Dokumentacja API zapewniająca integrację z zewnętrznymi systemami zarządzającymi firm trzecich musi być powszechnie dostępna |
|  | Oprogramowanie musi mieć funkcjonalność tworzenia ról administratorów i przydzielania im uprawnień, co najmniej w zakresie zarządzania:a. Politykami lub grupami polityk;b. Serwerami lub grupami serwerów;Poszczególnymi funkcjami systemu ochrony |
|  | Oprogramowanie musi mieć umożliwiać na automatyczne tworzenie grup serwerów w celu zarządzania nimi oraz przypisywania im określonych zasad bezpieczeństwa. Grupowanie musi odbywać się na podstawie określonych przez administratora reguł, takich jak system operacyjny, atrybuty maszyny, adresy itp. |
|  | Oprogramowanie musi mieć możliwość tworzenia drzewa polityk zależnych, w którym polityki pochodne dziedziczą ustawienia od polityk na wyższym poziomie. Administratorzy posiadający uprawnienia jedynie do polityk pochodnych nie mogą mieć możliwości wprowadzania zmian do ustawień nadrzędnych |