Załącznik nr 1

dot. sprawy nr. 181169/2023

OPIS PRZEDMIOTU ZAMÓWIENIA

„Dostawa licencji do zakupu Web Aplication Firewall wraz z wdrożeniem i szkoleniem dla Uniwersytetu Śląskiego" – 1 szt.

Parametry wymagane	Parametry oferowane
Przedmiotem zamówienia jest oprogramowanie specjalistyczne FortiWeb VM02 z dożywotnią licencją i serwisem bezpieczeństwa na 3 lata wraz z wdrożeniem i szkoleniem. System ochrony aplikacji webowych oraz Firewall XML, którego zadaniem będzie wykrywanie i blokowanie ataków celujących w aplikacje webowe a następnie alarmowanie w wyniku wystąpienia określonych zdarzeń. Powinien zostać dostarczony w postaci komercyjnej platformy instalowanej w środowisku wirtualnym: VMware, Microsoft Hyper-V, Citrix XenServer, Open Source Xen, KVM, Amazon Web Services (AWS) and Microsoft Azure, Google Cloud, Oracle Cloud, Proxmox. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych w ww środowisku wirtualnym. W przypadku implementacji programowej dostawca musi zapewnić niezbędny odpowiednio zabezpieczony systemem operacyjny. **Architektura systemu** 1. Dla zapewnienia wysokiej sprawności i skuteczności działania wymaganym jest aby elementy systemu pracowały w oparciu o dedykowane oprogramowanie, wzmocnione z punktu widzenia bezpieczeństwa. 2. Dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się, aby wszystkie funkcje podstawowe oraz zastosowane w nich technologie pochodziły od jednego producenta. Nie dopuszcza się aby elementy funkcji	

Uniwersytet Śląski w Katowicach
Dział Zarządzania Dostawami
ul. Bankowa 14, 40-007 Katowice
tel.: 32 359 13 63, e-mail: maria.rys@us.edu.pl
www.us.edu.pl

podstawowych zastosowanych w systemie były opracowane przez firmy trzecie.
3. Musi istnieć możliwość implementacji systemu w trybach: inline reverse proxy lub transparent.
4. Produkt nie może posiadać ograniczeń co do ilości chronionych aplikacji web.
5. Powinna istnieć możliwość zdefiniowania co najmniej 4 domen administracyjnych, w których poszczególni administratorzy zarządzają określonymi funkcjami podstawowymi systemu.
6. System powinien mieć możliwość pracy w konfiguracji HA (High Availability) w trybie Active-Passive i Active-Active.

Parametry fizyczne systemu

1. System realizujący funkcje podstawowe musi obsługiwać minimum:
   - 4 interfejsy sieciowe
   - Ilość wirtualnych procesorów: 2
2. Obsługa powierzchni dyskowej - minimum 1 TB.

Parametry wydajnościowe

1. Przepustowość dla ruchu http - min 100 Mbps.

Podstawowe funkcje systemu

System musi realizować co najmniej poniższe funkcje:

1. Obsługa protokołów: - http 1.1, http 2.0, FTP.
2. Automatyczne tworzenie profili ochronnych aplikacji na bazie zaobserwowanego ruchu. Możliwość wyboru trybu wymuszania wyuczonego schematu bez konieczności akceptacji przez administratora.
3. Automatyczne tworzenie profilu ochrony przed botami na bazie zaobserwowanego ruchu użytkowników
4. Podział obciążenia na kilkanaście serwerów (loadbalancing) z mechanizmami weryfikacji stanu pracy serwerów. Wsparcie dla mechanizmów podziału obciążenia:
   - Round Robin,
   - Weighted Round Robin,
   - Least Connection,
5. Wsparcie dla mechanizmów session persistence:
   - Source IP
   - HTTP Header
   - URL parameter
   - Insert Cookie
   - Rewrite Cookie
   - Persistent Cookie

Uniwersytet Śląski w Katowicach
Dział Zarządzania Dostawami
ul. Bankowa 14, 40-007 Katowice
tel.: 32 359 13 63, e-mail: maria.rys@us.edu.pl
www.us.edu.pl

• Embedded Cookie • ASP Session ID • PHP Session ID • JSP Session ID • SSL Session ID 6. Terminowanie połączeń SSL dla wybranych chronionych serwisów. Wsparcie dla TLS 1.1, TLS 1.2. TLS 1.3. 7. Możliwość analizy ruchu do aplikacji po protokołach HTTP/HTTPS w oparciu o zaimplementowane polityki bezpieczeństwa. 8. Ochrona aplikacji www przed takimi zagrożeniami jak: • SQL and OS Command Injection. • Cross Site Scripting (XSS). • Cross Site Request Forgery. • Outbound Data Leakage. • HTTP Request Smuggling. • Buffer Overflow. • Encoding Attacks. • Cookie Tampering / Poisoning. • Session Hijacking. • Broken Access Control. • Forceful Browsing /Directory Traversal. • Ochrona przed innymi zagrożeniami specyfikowanymi przez listę OWASP. • DoS w warstwie aplikacji. • Ochrona przed atakami typu Brute force. • Ochrona przed atakami clickjacking. 9. Mechanizmy ochrony przed wyciekiem informacji poufnych. 10. Filtrowanie ruchu do aplikacji w oparciu o geo-lokalizację. 11. Analiza komunikacji w oparciu o bazy reputacyjne adresów IP, dostarczane przez producenta rozwiązania. 12. Integracja z zewnętrznymi systemami uwierzytelniania dwu-składnikowego. 13. Wsparcie dla ochrony HTTP/1.1 i HTTP/2 oraz offload dla HTTP/1.1 i HTTP/2 w trybie pracy reverse proxy. 14. Wsparcie dla ochrony cookie, w tym szyfrowania oraz sprawdzania flag „Secure" „ oraz „http only". 15. Content routing na bazie parametrów http oraz certyfikatów X.509. 16. Ochrona przed Web Scraping. 17. Wsparcie dla kompresji danych oraz cache.	

Uniwersytet Śląski w Katowicach
Dział Zarządzania Dostawami
ul. Bankowa 14, 40-007 Katowice
tel.: 32 359 13 63, e-mail: maria.rys@us.edu.pl
www.us.edu.pl

18. Publikacja aplikacji web oraz OWA z zastosowaniem single sign on (http basic, kerberos).
19. Wsparcie dla aplikacji wykorzystujących AJAX oraz JSON, XML, AMF3.
20. Ochrona przed atakami typu SLOW (Slowloris i podobne).
21. Możliwość selektywnego wyłączania blokowania ataków dla sygnatur oraz obszarów aplikacji. Dodanie wyjątków dla sygnatur na podstawie wielu parametrów:
    - Metoda HTTP.
    - IP klienta.
    - Host.
    - URI.
    - Cały URL.
    - Parametr.
    - Cookie.
    - http Header
    - JSON Elements
22. Funkcja korzystania ze źródłowego adresu IP przekazywanego w nagłówku http „X-Forwared-For".
23. Wszelkie klucze prywatne zapisywane na dyskach urządzenia muszą być zapisywane w postaci zaszyfrowanej.
24. Możliwość konfigurowania własnych stron z informacjami o błędzie per polityka.
25. Sprawdzanie pól w nagłówkach http oraz samym protokole. Sprawdzanie długości payload'u HTML.
26. Wsparcie dla walidacji OpenAPI, JSON i XML.
27. Blokowania „Illegal XML Format" oraz „Illegal JSON Format".
28. Możliwość wysłania odszyfrowanego przez system ruchu do innego systemu celem dalszej analizy.
29. Przydzielanie różnych certyfikatów dla różnych nazw domenowych.
30. Ochrona przed atakami MiTB (Man-in-the-Browser) przynamniej dla Anti-keylogger, Obfuscate.
31. URL Encryption.

Wymagane funkcje dodatkowe

1. Kontrola antywirusowa dla komunikacji http realizowana na firewall'u aplikacyjnym lub zewnętrznym systemie w oparciu o protokół icap. W ramach postępowania muszą zostać dostarczone wszystkie elementy (urządzenia, licencje) niezbędne do uruchomienia tej funkcji.

Uniwersytet Śląski w Katowicach
Dział Zarządzania Dostawami
ul. Bankowa 14, 40-007 Katowice
tel.: 32 359 13 63, e-mail: maria.rys@us.edu.pl
www.us.edu.pl

Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. 2. W ramach postępowania wymaganym jest dostarczenie licencji upoważniającej do współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. 3. Skaner aplikacji WWW realizowany bezpośrednio na firewall'u aplikacyjnym lub zewnętrznym systemie (w przypadku zewnętrznego systemu skanującego – musi istnieć możliwość importu wyników skanowania do systemu WAF oraz na tej podstawie konfiguracji polityk ochrony). W ramach postępowania muszą zostać dostarczone wszystkie elementy (urządzenia, licencje) niezbędne do uruchomienia tej funkcji. 4. Ochrona przed podmianą strony WWW realizowana bezpośrednio na firewall'u aplikacyjnym lub zewnętrznym systemie. W ramach postępowania muszą zostać dostarczone wszystkie elementy (urządzenia, licencje) niezbędne do uruchomienia tej funkcji. 5. Dekodowanie Base64 oraz CSS. 6. Domyślne szablony ochrony dla Exchange, SharePoint i WordPress. 7. Uwierzytelnianie użytkowników w oparciu o protokół SAML. 8. Rozpoznawanie prawidłowo zalogowanych użytkowników do chronionej aplikacji. 9. Wsparcie dla CAPTCHA i Real Browser Enforcement do weryfikacji użytkowników. 10. Budowa rankingu punktowego lub określanie poziomu zagrożenia dla ruchu z możliwością określenia progów dla akcji: kwarantanna czasowa. 11. Możliwość uruchomienia ADFSProxy oraz stworzenia polityki w celu sprawdzania ruchu do serwerów ADFS, ich ochrony pod kątem malware, botów, exploitów, oraz ataków DoS, APT i zero day. 12. Możliwość znakowania przez administratorów systemu za pomocą znaczników (flag) lub komentarza zdarzeń zalogowanych przez urządzenie w celu późniejszej ich analizy.	

Uniwersytet Śląski w Katowicach
Dział Zarządzania Dostawami
ul. Bankowa 14, 40-007 Katowice
tel.: 32 359 13 63, e-mail: maria.rys@us.edu.pl
www.us.edu.pl

13. Ochrona przed botami dla: strony internetowej, aplikacji mobilnej, intefejsu API - przy zastosowaniu funkcji biometrycznych.
14. Cross-Origin Resource Sharing (CORS) protection.
15. Integracja z Let's encrypt pozwalająca na automatyczne generowanie certyfikatów na potrzeby terminowania połączeń SSL.

Zarządzanie

1. Dostarczony system musi umożliwiać lokalne zarządzanie z wykorzystaniem protokołów HTTPS, SSH, API.
2. Element systemu pełniący funkcję Web Application Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: packet capture.
3. Powinna istnieć możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych.
4. Możliwość przechowywania lokalnie na urządzeniu do 10 plików konfiguracyjnych.

Logowanie i Raportowanie

1. System musi zapewniać lokalne logowanie oraz raportowanie - w oparciu o zestaw predefiniowanych wzorców raportów.
2. Możliwość logowania do zewnętrznego serwera syslog i SIEM.
3. Obsługa powiadomień o zdarzeniach systemowych oraz incydentach bezpieczeństwa mailem.
4. Powiadomienia o zdarzeniach systemowych oraz incydentach bezpieczeństwa za pośrednictwem trapów SNMP.

Certyfikaty

1. Z punktu widzenia jakości i skuteczności rozwiązania koniecznym jest przedstawienie wyników testów niezależnych organizacji, np. NSS Labs, ICSA Labs lub równoważnego.

Sygnatury, subskrypcje

1. System musi być dostarczony w modelu „na własność" tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania.
2. Bazy sygnatur wykorzystywane przez funkcje ochronne powinny być systematycznie

Uniwersytet Śląski w Katowicach
Dział Zarządzania Dostawami
ul. Bankowa 14, 40-007 Katowice
tel.: 32 359 13 63, e-mail: maria.rys@us.edu.pl
www.us.edu.pl

aktualizowane zgodnie ze zdefiniowanych harmonogramem.

3. W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych i serwisów. Powinny one obejmować:
   - Kontrolę antywirusową, sygnatury ochrony dla aplikacji www oraz bazy reputacyjne adresów IP na okres 36 miesięcy.
   - Kontrolę antywirusową, sygnatury ochrony dla aplikacji www, bazy reputacyjne adresów IP, bazy wspierające działanie funkcji Credential Stuffing oraz dostęp do usługi sandbox na okres 36 miesięcy
   - Ochronę przed nieznanymi zagrożeniami w oparciu o usługę typu Sandbox na okres 36 miesięcy

Gwarancja oraz wsparcie

1. System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Rozszerzone wsparcie serwisowe

2. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 8x5 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim:
   - Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
   - Certyfikat ISO 9001 podmiotu serwisującego.

Opisy do wymagań ogólnych

1. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały

Uniwersytet Śląski w Katowicach
Dział Zarządzania Dostawami
ul. Bankowa 14, 40-007 Katowice
tel.: 32 359 13 63, e-mail: maria.rys@us.edu.pl
www.us.edu.pl

dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. 2. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.	

Uniwersytet Śląski w Katowicach
Dział Zarządzania Dostawami
ul. Bankowa 14, 40-007 Katowice
tel.: 32 359 13 63, e-mail: maria.rys@us.edu.pl
www.us.edu.pl