Załącznik nr B do SWZ

USZCZEGÓŁOWIONY OPIS PRZEDMIOTU I ZAKRESU ZAMÓWIENIA

I. Miejsce dostawy i montażu poszczególnych urządzeń firewall:

Akademia Sztuk Teatralnych im. Stanisława Wyspiańskiego w Krakowie, ul. Straszewskiego 21-22, 31-109 Kraków

Akademia Sztuk Teatralnych im. Stanisława Wyspiańskiego w Krakowie Filia w Bytomiu, ul. Piłsudskiego 24a, 41-902 Bytom

Akademia Sztuk Teatralnych im. Stanisława Wyspiańskiego w Krakowie Filia we Wrocławiu, ul. Braniborska 59, 53-680 Wrocław

II. Ogólny opis zamówienia

Zamówienie polega na uzupełnieniu istniejącego u Zamawiającego zestawu urządzeń o firewall o zwiększonej wydajności, działający równolegle z istniejącym urządzeniem Cisco model ASA5525X. Wzorcowe wymagane urządzenie to Cisco model FTD 1150 lub wyższy, gwarantujący spójność zarządzania na poziomie oprogramowania systemowego – zgodny z posiadanym przez Zamawiającego centralnym zarządzaniem Cisco FirePower. Nowy firewall, który zostanie zainstalowany w budynku Zamawiającego w Krakowie przy ul. Straszewskiego 21-22, jest konieczny do zwiększenia przepustowości połączeń zdalnych pomiędzy lokalizacjami Zamawiającego, tj. Krakowem - ul. Straszewskiego 21-22 i ul. Warszawska 5, Bytomiem - ul. Piłsudskiego 24a i Wrocławiem - ul. Braniborska 59 oraz pomiędzy sieciami VLAN. Ponadto w ramach zamówienia zostaną wymienione na nowe urządzenia firewall w budynkach AST przy ul. Piłsudskiego 24 a w Bytomiu i przy ul. Braniborskiej 59 we Wrocławiu.

III. Wymagania ogólne dotyczące oferowanych urządzeń

1. Sprzęt dostarczony w ramach realizacji zamówienia i umowy musi być sprzętem nowym, niepowystawowym, nieużywanym oraz niedostarczanym wcześniej w żadnych innych projektach. Dostarczony sprzęt musi posiadać gwarancję świadczoną bezpośrednio przez Producenta sprzętu lub jego autoryzowanego przedstawiciela.
2. Oferowany sprzęt musi być sprzętem zakupionym w oficjalnym kanale sprzedaży oraz zarejestrowanym na użytkownika końcowego (tj. Zamawiającego).
3. Zamawiający zastrzega sobie prawo sprawdzenia poprzez numery seryjne w trakcie odbioru, czy dostarczony sprzęt spełnia wszystkie wyżej wymienione warunki.
4. W przypadku niespełnienia przez sprzęt któregokolwiek z wyżej wymienionych warunków Zamawiający zastrzega sobie prawo zwrotu całego dostarczonego sprzętu (na koszt Wykonawcy), jak również obciążenia Wykonawcy karą umowną za niedotrzymanie warunków umowy.
5. Zamawiający wymaga, aby Wykonawca był bezpośrednio oficjalnym partnerem handlowym Producenta oferowanych urządzeń, a możliwość zweryfikowania tego faktu była publicznie dostępna poprzez stronę Producenta. Wykonawca zobowiązany jest podać w formularzu oferty adres URL pozwalający na zweryfikowanie, że jest oficjalnym partnerem handlowym producenta oferowanych urządzeń.

6. Wykonawca zobowiązany jest do podania w ofercie (wg wzoru określonego w załączniku A do SWZ) marki/typu/modelu/symbolu/numeru katalogowego itp. i producenta/ów pozwalających na jednoznaczną identyfikację oferowanych urządzeń i elementów składających się na przedmiot zamówienia (licencje, sprzęt i oprogramowanie). Informacje te będą podlegały ocenie przez Zamawiającego w celu weryfikacji, czy oferowany przedmiot zamówienia spełnia warunki określone w SWZ.

IV. Specyfikacja prac wdrożeniowych w ramach realizacji zamówienia

1. Przed rozpoczęciem prac należy ustalić plan adresacji i wykorzystania adresów. Ustalenia te będą prowadzone z wyznaczonymi do tego celu pracownikami Zamawiającego. Przed rozpoczęciem prac Wykonawca musi przeprowadzić analizę stanu sieci, serwerów i jego usług oraz ustalić harmonogram prac. Konfiguracja będzie obejmowała nowo dostarczony sprzęt oraz już znajdujące się urządzenia w infrastrukturze Zamawiającego. Ze względów bezpieczeństwa, tj. nieujawniania autorskich rozwiązań konfiguracji istniejącej u Zamawiającego, szczegółowy opis tej konfiguracji zostanie udostępniony tylko wyłonionemu Wykonawcy. **Cały sprzęt musi zostać wcześniej prekonfigurowany i sprawdzony u Wykonawcy, tak aby zminimalizować ilość prac realizowanych w budynkach Zamawiającego.**

2. **Usługa konfiguracji dostarczonych urządzeń zawierać będzie m.in.:**
   - konfigurację IPsec VPN (IKEv2) pomiędzy wszystkimi lokalizacjami,
   - konfigurację zaawansowanych funkcji ochrony przed złośliwym oprogramowanie, filtrowaniem URL oraz ochrony przed zagrożeniami IPS (Instrusion Prevention System),
   - konfigurację usługi VPN Remote Access,
   - konfigurację reguł ACL na urządzeniach brzegowych (Zamawiający zastrzega, że w tym zakresie ma bardzo złożone wymagania, które dotyczą dużej ilości usług, jaka hostowana jest w ramach infrastruktury),
   - integrację usług uwierzytelnienia VPN wskazanym serwerem RADIUS i/lub SAML,
   - protokoły VLAN, Trunk, LACP, adresację IP, konfigurację DNS, routingu,
   - baner logowania, usługa NTP, SSH, wbudowane mechanizmy RBAC oraz konta użytkowników,
   - automatyczne wykonywanie kopii zapasowej z firewall do wskazanego serwera FTP,
   - wysyłanie zdarzeń syslog do wskazanego serwera Syslog,
   - hardening urządzeń sieciowych według najlepszych praktyk Producenta,
   - personalizacja ustawień do przedstawionych wymagań,
   - integrację urządzeń z obecnymi w infrastrukturze,
   - konfigurację innych funkcjonalności dostarczonych urządzeń i oprogramowania, które okażą się potrzebne w trakcie wdrożenia, gdy Wykonawca uzna zasadności ich aktywacji oraz skonfigurowania,
   - **konfigurację urządzeń w lokalizacjach Kraków, Bytom oraz Wrocław** w terminie dogodnym dla Zamawiającego, jak np. godziny wieczorne lub nocne oraz weekendy,
   - rekonfigurację komunikacji pomiędzy budynkami w Krakowie wraz z uzgodnieniem warunków technicznych z lokalnym operatorem (tj. Cyfronetem – AGH).

3. Obecna infrastruktura sieciowa Uczelni zbudowana jest w większości na urządzeniach firmy Cisco Systems, do których należą m.in. produkty: Cisco WLC, Cisco Air, Cisco Catalyst, Cisco ASA-X. W ramach prac będzie wymagana integracja dostarczonego rozwiązania z tymi produktami oraz też migracja z niektórych produktów Cisco Systems konfiguracji i polityk, do nowodostarczonych urządzeń. Stąd wymaga się od Wykonawcy znajomości rozwiązania, jakie oferuje oraz dodatkowo posiadania minimum takich certyfikatów producenta Cisco Systems: Cisco Certified Specialist - Network Security Firepower, Cisco

Certified Specialist - Network Security VPN Implementation, Cisco Certified Network Professional Security (CCNP Security).

4. Zamawiający wymaga, aby zarządzanie firewallami odbywało się z jednej wspólnej platformy dla wszystkich posiadanych przez Zamawiającego urządzeń typu firewall. Nie dopuszcza się stosowania konwerterów polityk czy narzędzi, które będą tłumaczyć polityki.

5. Zamawiający wymaga przeprowadzenia w swojej siedzibie przy ul. Straszewskiego 21-22 w Krakowie szkolenia dla jednej osoby w wymiarze 6 godzin.

6. Urządzenia firewall wraz z licencjami pozwalającymi na kontrolę aplikacji muszą zapewnić filtrowanie adresów URL, wykonywanie inspekcji IPS oraz kontrolę/blokowanie plików.

V. Wymagane urządzenia:

Firewall typ1 – lokalizacja: Kraków, ul. Straszewskiego 21-22

Urządzenie firewall wraz z licencjami pozwalającymi na kontrolę aplikacji, filtrowanie adresów URL, wykonywanie inspekcji IPS oraz kontrolę/blokowanie plików. Wzorcowe wymagane urządzenie to Cisco FTD 1150 lub model wyższy. Dopuszcza się urządzenie równoważne, które musi pracować w trybie wysokiej dostępności (HA) z urządzeniem Cisco FTD 1150 posiadanym przez Zamawiającego, a w tym, na poziomie systemu operacyjnego ASA-OS/FTD umożliwiać tworzenie bliźniaczych i przenośnych pomiędzy oboma urządzeniami konfiguracji, które nie będą wymagać żadnych konwersji. Urządzenia muszą synchronizować pomiędzy sobą tablicę stanów, tak by w razie przełączenia urządzenia sesje ze stacji końcowych do usług nie uległy przerwaniu.

Urządzenie musi być objęte 5-letnim serwisem świadczonym bezpośrednio przez producenta w reżimie 8x5xNBD uprawniającym do wymiany sprzętu w przypadku zdiagnozowania awarii urządzenia, wsparcia telefonicznego i mailowego w zakresie konfiguracji urządzenia oraz do aktualizacji oprogramowania urządzenia. Wymagany jest dostęp do aktualizacji sygnatur IPS, mechanizmów filtrowania webowego i aktualizacji filtrów antymalware'owych przez okres 5 lat. Należy również dostarczyć przedłużenie wsparcia serwisowego oraz subskrypcji dla sygnatur IPS, mechanizmów filtrowania webowego i aktualizacji filtrów antymalware'owych dla aktualnego urządzenia posiadanego przez Zamawiającego, tak aby czas zakończenia serwisu oraz subskrypcji był taki sam dla obu urządzeń (dostarczanego i posiadanego przez Zamawiającego), ale nie krócej niż 5 lat od daty dostawy oferowanego urządzenia.

Firewall typ2 – lokalizacja: Bytom, ul. Piłsudskiego 24a

1. Urządzenie musi być dedykowaną platformą sprzętową – nie dopuszcza się rozwiązań „serwerowych" bazujących na ogólnodostępnych na rynku podzespołach PC ogólnego przeznaczenia.
2. Urządzenie musi pełnić rolę ściany ogniowej (firewall) typu statefull inspection i ściany ogniowej nowej generacji (NG Firewall).
3. Urządzenie musi być wyposażone w 8 portów 1 Gigabit Ethernet oraz 4 porty SFP.
4. Urządzenie musi obsługiwać interfejsy VLAN (802.1Q) na interfejsach fizycznych – minimum 1.000 sieci VLAN.
5. Urządzenie musi być wyposażone w dedykowany port konsoli oraz dedykowany port Gigabit Ethernet do zarządzania Out-of-Band.
6. Urządzenie musi być wyposażone w port USB 2.0.

7. Urządzenie musi mieć możliwość montażu w szafie rack 19'' (należy dołączyć niezbędne elementy montażowe).
8. Maksymalna wysokość urządzenia: 1RU.
9. Wymagana jest przepustowość teoretyczna urządzenia dla uruchomionych modułów firewall'a oraz kontroli aplikacji (AVC) na poziomie 2.2Gb/s, a dla modułów AVC oraz systemu IPS na poziomie 2.2Gb/s.
10. Urządzenie musi obsługiwać maksymalnę liczbę sesji (z kontrolą aplikacji) na poziomie 200 000 z możliwością zestawiania co najmniej 14 000 nowych połączeń na sekundę.
11. Wymagane jest wsparcie dla VPN IPSec na poziomie 1.2 Gb/s.
12. Urządzenie nie może posiadać ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej.
13. Wymagana jest możliwość uruchomienia urządzenia w trybie firewall'a L3, jak i w trybie transparentnym.
14. Urządzenie musi obsługiwać routing statyczny i dynamiczny (RIP, OSPF, BGP).
15. Urządzenie musi posiadać możliwości konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika, zapewniając integrację z usługą katalogową Microsoft Active Directory.
16. Urządzenie musi obsługiwać funkcjonalność Network Address Translation (NAT oraz PAT).
17. Urządzenie musi zapewniać mechanizmy redundancji w tym możliwość konfiguracji urządzeń w układ zapasowy (failover) działający w trybie wysokiej dostępności (HA) active/standby.
18. Urządzenie musi zapewniać funkcjonalność tzw. Firewall'a Next-Generation w zakresie:
    a. systemu automatycznego wykrywania i klasyfikacji aplikacji (Application Visibility and Control),
    b. systemu IPS (Intrusion Prevention System),
19. System musi posiadać możliwość kontekstowego definiowania reguł z wykorzystaniem informacji pozyskiwanych o hostach na bieżąco poprzez pasywne skanowanie. System ma tworzyć kontekst z wykorzystaniem co najmniej poniższych parametrów:
    a. Wiedza o użytkownikach – uwierzytelnienie.
    b. Wiedza o urządzeniach – pasywne skanowanie ruchu.
    c. Wiedza o urządzeniach mobilnych.
    d. Wiedza o aplikacjach wykorzystywanych po stronie klienta.
    e. Wiedza o podatnościach.
    f. Wiedza o bieżących zagrożeniach.
    g. Baza danych URL.
20. System musi posiadać otwarte API dla współpracy z systemami zewnętrznymi, w tym co najmniej z systemami SIEM.
21. Urządzenie musi umożliwiać konfigurację IPsec IKEv2 oraz SSL VPN Remote Access z możliwością uwierzytelniania w serwerze RADIUS/LDAP/AD. W ramach połączenia VPN system musi umożliwiać stworzenie kilku różnych grup dostępowych do sieci. System musi posiadać możliwość definiowania powitalnego banneru dla połączenia VPN RA oraz możliwości tunelowania całego ruchu jak i również tzw. „Split tunelingu" (funkcja ta jest konfigurowana per grupa VPN RA).
22. System wykrywania aplikacji AVC musi zapewniać:
    a. możliwość klasyfikacji ruchu i wykrywania co najmniej 4000 aplikacji,
    b. możliwość tworzenie profili użytkowników korzystających ze wskazanych aplikacji z dokładnością co najmniej do systemu operacyjnego, z którego korzysta użytkownik oraz wykorzystywanych usług,
    c. wykorzystanie informacji geolokacyjnych dotyczących użytkownika lub aplikacji,
    d. współpracę z otwartym systemem opisu aplikacji pozwalającym administratorowi na skonfigurowanie opisu dowolnej aplikacji i wykorzystanie go do automatycznego

wykrywania tejże aplikacji przez system AVC oraz na wykorzystanie profilu tej aplikacji w regułach reagowania na zagrożenia oraz w raportach.

23. System IPS musi zapewniać:
    a. możliwość pracy w trybie in-line (wszystkie pakiety, które mają być poddane inspekcji muszą przechodzić przez system),
    b. możliwość pracy w trybie pasywnym (IDS),
    c. możliwość wykrywania i blokowania szerokiej gamy zagrożeń, w tym:
        i. złośliwe oprogramowanie,
        ii. skanowanie sieci,
        iii. ataki na usługę VoIP,
        iv. próby przepełnienia bufora,
        v. ataki na aplikacje P2P,
        vi. zagrożenia dnia zerowego, itp.
    d. możliwość wykrywania modyfikacji znanych ataków (sygnatury), jak i nowo powstałych, które nie zostały jeszcze dogłębnie opisane (analiza behawioralna),
    e. wiele sposobów wykrywania zagrożeń, w tym:
        i. sygnatury ataków opartych na exploitach,
        ii. reguły oparte na zagrożeniach,
        iii. mechanizm wykrywania anomalii w protokołach,
        iv. mechanizm wykrywania anomalii w ogólnym zachowaniu ruchu sieciowego,
    f. możliwość inspekcji nie tylko warstwy sieciowej i informacji zawartych w nagłówkach pakietów, ale również szerokiego zakres protokołów na wszystkich warstwach modelu sieciowego włącznie z możliwością sprawdzania zawartości pakietu,
    g. mechanizm minimalizujący liczbę fałszywych alarmów, jak i niewykrytych ataków (ang. false positives i false negatives),
    h. możliwość detekcji ataków/zagrożeń złożonych z wielu elementów i korelacji wielu, pozornie niepowiązanych zdarzeń
    i. wiele możliwości reakcji na zdarzenia, w tym takie, jak:
        i. tylko monitorowanie,
        ii. blokowanie ruchu zawierającego zagrożenia,
        iii. zastąpienie zawartości pakietów,
        iv. zapisywanie pakietów,
    j. możliwość detekcji ataków i zagrożeń opartych na protokole IPv6
    k. możliwość pasywnego zbierania informacji o urządzeniach sieciowych oraz ich aktywności w celu wykorzystania tych informacji do analizy i korelacji ze zdarzeniami bezpieczeństwa, eliminowania fałszywych alarmów oraz tworzenia polityki zgodności – zbierane są informacje o:
        i. systemach operacyjnych,
        ii. serwisach,
        iii. otwartych portach, aplikacjach,
        iv. zagrożeniach,
    l. możliwość pasywnego gromadzenia informacji o przepływach ruchu sieciowego ze wszystkich monitorowanych hostów włączając w to czas początkowy i końcowy, porty, usługi oraz ilość przesłanych danych,
    m. możliwość pasywnej detekcji predefiniowanych serwisów takich jak FTP, HTTP, POP3, Telnet, itp.
    n. możliwość automatycznej inspekcji i ochrony dla ruchu wysyłanego na niestandardowych portach używanych do komunikacji,

o. możliwość obrony przed atakami skonstruowanym tak, aby uniknąć wykrycia przez IPS. W tym celu stosowany najodpowiedniejszy mechanizm defragmentacji i składania strumienia danych w zależności od charakterystyki hosta docelowego,
p. mechanizm bezpiecznej aktualizacji sygnatur. Zestawy sygnatur/reguł muszą być pobierane z serwera w sposób uniemożliwiający ich modyfikację przez osoby postronne,
q. możliwość definiowania wyjątków dla sygnatur z określeniem adresów IP źródła, przeznaczenia lub obu jednocześnie,
r. obsługę reguł Snort,
s. możliwość wykorzystania informacji o sklasyfikowanych aplikacjach do tworzenia reguł IPS,
t. mechanizmy automatyzacji w zakresie wskazania hostów skompromitowanych (ang. Indication of compromise),
u. mechanizmy automatyzacji w zakresie automatycznego dostrojenia polityk bezpieczeństwa

24. System filtracji URL musi zapewniać:
    a. kategoryzację stron – w co najmniej 70 kategoriach,
    b. bazę URL o wielkości nie mniejszej niż 250 mln URL,
25. Urządzenie musi zapewniać możliwość wykrywania i śledzenia transferu następujących kategorii plików w ruchu sieciowym:
    a. pliki systemowe,
    b. pliki graficzne,
    c. pliki PDF,
    d. pliki wykonywalne,
    e. pliki multimedialne,
    f. pliki pakietu Office,
    g. pliki skompresowane.
26. Urządzenie musi posiadać możliwość monitorowania jak i kontrolowania transferu plików w następujących protokołach: HTTP, SMTP, FTP, IMAP, POP3, NetBIOS (SMB) w danym kierunku – upload/download.
27. Urządzenie musi posiadać wbudowany podsystem wykrywania oprogramowania złośliwego (malware) i jego propagacji w strefie chronionej poprzez:
    a. sprawdzenie reputacji plików w systemie globalnym,
    b. sprawdzenie plików w sandbox (realizowanym lokalnie lub w chmurze,)
    c. statyczną analizę struktury całego pliku pod kątem charakterystycznych elementów używanych w złośliwym oprogramowaniu.
28. Urządzenie musi zapewniać możliwość zapisania na dysk twardy kopii analizowanych plików o następujących charakterystykach:
    a. pliki wolne od złośliwego kodu,
    b. pliki zawierające złośliwy kod,
    c. pliki podejrzane,
    d. pliki o własnej, zdefiniowanej przez użytkownika kategorii
29. Urządzenie musi posiadać podsystem wykrywania oprogramowania złośliwego zawiera narzędzia analizy historycznej dla plików przesłanych w przeszłości, a rozpoznanych jako oprogramowanie złośliwe (analiza retrospektywna).
30. Oprogramowanie urządzenia/urządzenie musi posiadać funkcję weryfikacji aplikacji bez rozszyfrowania sesji TLS, informacje pozyskanie w trakcie nawiązywania sesji TLS muszą posłużyć do wykrywania aplikacji oraz podejmowania działań.

31. Urządzenie musi być objęte 5-letnim serwisem świadczonym bezpośrednio przez producenta w reżimie 8x5xNBD uprawniającym do wymiany sprzętu w przypadku zdiagnozowania awarii urządzenia, wsparcia telefonicznego i mailowego w zakresie konfiguracji urządzenia oraz do aktualizacji oprogramowania urządzenia. Dostęp do aktualizacji sygnatur IPS, mechanizmów filtrowania webowego i aktualizacji filtrów antymalware'owych przez okres 5 lat.

Firewall typ3 – lokalizacja: Wrocław, ul. Braniborska 59

1. Urządzenie musi być dedykowaną platformą sprzętową – nie dopuszcza się rozwiązań „serwerowych" bazujących na ogólnodostępnych na rynku podzespołach PC ogólnego przeznaczenia.
2. Urządzenie musi pełnić rolę ściany ogniowej (firewall) typu stateful inspection i ściany ogniowej nowej generacji (NG Firewall).
3. Urządzenie musi być wyposażone w 8 portów 1 Gigabit Ethernet oraz 4 porty SFP.
4. Urządzenie musi obsługiwać interfejsy VLAN (802.1Q) na interfejsach fizycznych – minimum 1.000 sieci VLAN.
5. Urządzenie musi być wyposażone w dedykowany port konsoli oraz dedykowany port Gigabit Ethernet do zarządzania Out-of-Band.
6. Urządzenie musi być wyposażone w port USB 2.0.
7. Urządzenie musi mieć możliwość montażu w szafie rack 19" (należy dołączyć niezbędne elementy montażowe).
8. Maksymalna wysokość urządzenia 1RU.
9. Wymagana jest przepustowość teoretyczna urządzenia dla uruchomionych modułów firewall'a oraz kontroli aplikacji (AVC) na poziomie 3.2Gb/s, a dla modułów AVC oraz systemu IPS na poziomie 3.2Gb/s.
10. Wymagana maksymalna liczba sesji (z kontrolą aplikacji) na poziomie 350 000 z możliwością zestawiania co najmniej 20 000 nowych połączeń na sekundę.
11. Wymagane wsparcie dla VPN IPSec na poziomie 1.3 Gb/s.
12. Urządzenie nie może posiadać ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej.
13. Urządzenie musi mieć możliwość uruchomienia urządzenia w trybie firewall'a L3, jak i w trybie transparentnym.
14. Urządzenie musi obsługiwać routing statyczny i dynamiczny (RIP, OSPF, BGP).
15. Urządzenie musi posiadać możliwości konfiguracji reguł filtrowania ruchu w oparciu o tożsamość. użytkownika, zapewniając integrację z usługą katalogową Microsoft Active Directory.
16. Urządzenie musi obsługiwać funkcjonalność Network Address Translation (NAT oraz PAT).
17. Urządzenie musi zapewniać mechanizmy redundancji w tym możliwość konfiguracji urządzeń w układ zapasowy (failover) działający w trybie wysokiej dostępności (HA) active/standby.
18. Urządzenie musi zapewniać funkcjonalność tzw. Firewall'a Next-Generation w zakresie:
    a. systemu automatycznego wykrywania i klasyfikacji aplikacji (Application Visibility and Control),
    b. systemu IPS (Intrusion Prevention System).
19. System musi posiadać możliwość kontekstowego definiowania reguł z wykorzystaniem informacji pozyskiwanych o hostach na bieżąco poprzez pasywne skanowanie. System ma tworzyć kontekst z wykorzystaniem co najmniej poniższych parametrów:
    a. Wiedza o użytkownikach – uwierzytelnienie,
    b. Wiedza o urządzeniach – pasywne skanowanie ruchu,
    c. Wiedza o urządzeniach mobilnych,
    d. Wiedza o aplikacjach wykorzystywanych po stronie klienta,

e. Wiedza o podatnościach,
f. Wiedza o bieżących zagrożeniach,
g. Baza danych URL.

20. System musi posiadać otwarte API dla współpracy z systemami zewnętrznymi w tym co najmniej z systemami SIEM.
21. Urządzenie musi umożliwiać konfigurację IPsec IKEv2 oraz SSL VPN Remote Access z możliwością uwierzytelniania w serwerze RADIUS/LDAP/AD. W ramach połączenia VPN system musi umożliwiać stworzenie, kilku różnych grup dostępowych do sieci. System musi posiadać możliwość definiowania powitalnego banneru dla połączenia VPN RA oraz możliwości tunelowania całego ruchu jak i również tzw. „Split tunelingu" (funkcja ta jest konfigurowana per grupa VPN RA).
22. System wykrywania aplikacji AVC musi zapewniać:
    a. możliwość klasyfikacji ruchu i wykrywania co najmniej 4000 aplikacji,
    b. możliwość tworzenie profili użytkowników korzystających ze wskazanych aplikacji z dokładnością co najmniej do systemu operacyjnego, z którego korzysta użytkownik oraz wykorzystywanych usług,
    c. wykorzystanie informacji geolokacyjnych dotyczących użytkownika lub aplikacji,
    d. współpracę z otwartym systemem opisu aplikacji pozwalającym administratorowi na skonfigurowanie opisu dowolnej aplikacji i wykorzystanie go do automatycznego wykrywania tejże aplikacji przez system AVC oraz na wykorzystanie profilu tej aplikacji w regułach reagowania na zagrożenia oraz w raportach.
23. System IPS musi zapewniać:
    a. możliwość pracy w trybie in-line (wszystkie pakiety, które mają być poddane inspekcji muszą przechodzić przez system)
    b. możliwość pracy w trybie pasywnym (IDS)
    c. możliwość wykrywania i blokowania szerokiej gamy zagrożeń w tym:
        i. złośliwe oprogramowanie,
        ii. skanowanie sieci,
        iii. ataki na usługę VoIP,
        iv. próby przepełnienia bufora,
        v. ataki na aplikacje P2P,
        vi. zagrożenia dnia zerowego, itp.
    d. możliwość wykrywania modyfikacji znanych ataków (sygnatury), jak i nowo powstałych, które nie zostały jeszcze dogłębnie opisane (analiza behawioralna)
    e. wiele sposobów wykrywania zagrożeń, w tym:
        i. sygnatury ataków opartych na exploitach,
        ii. reguły oparte na zagrożeniach,
        iii. mechanizm wykrywania anomalii w protokołach,
        iv. mechanizm wykrywania anomalii w ogólnym zachowaniu ruchu sieciowego
    f. możliwość inspekcji nie tylko warstwy sieciowej i informacji zawartych w nagłówkach pakietów, ale również szerokiego zakres protokołów na wszystkich warstwach modelu sieciowego włącznie z możliwością sprawdzania zawartości pakietu,
    g. mechanizm minimalizujący liczbę fałszywych alarmów, jak i niewykrytych ataków (ang. false positives i false negatives),
    h. możliwość detekcji ataków/zagrożeń złożonych z wielu elementów i korelacji wielu, pozornie niepowiązanych zdarzeń,
    i. wiele możliwości reakcji na zdarzenia, w tym takie, jak:
        i. tylko monitorowanie,
        ii. blokowanie ruchu zawierającego zagrożenia,

iii. zastąpienie zawartości pakietów,
iv. zapisywanie pakietów,

j. możliwość detekcji ataków i zagrożeń opartych na protokole IPv6
k. możliwość pasywnego zbierania informacji o urządzeniach sieciowych oraz ich aktywności w celu wykorzystania tych informacji do analizy i korelacji ze zdarzeniami bezpieczeństwa, eliminowania fałszywych alarmów oraz tworzenia polityki zgodności - zbierane są informacje o:
   i. systemach operacyjnych,
   ii. serwisach,
   iii. otwartych portach, aplikacjach,
   iv. zagrożeniach,
l. możliwość pasywnego gromadzenia informacji o przepływach ruchu sieciowego ze wszystkich monitorowanych hostów włączając w to czas początkowy i końcowy, porty, usługi oraz ilość przesłanych danych,
m. możliwość pasywnej detekcji predefiniowanych serwisów takich jak FTP, HTTP, POP3, Telnet, itp.
n. możliwość automatycznej inspekcji i ochrony dla ruchu wysyłanego na niestandardowych portach używanych do komunikacji,
o. możliwość obrony przed atakami skonstruowanym tak, aby uniknąć wykrycia przez IPS. W tym celu musi być zastosowany najodpowiedniejszy mechanizm defragmentacji i składania strumienia danych w zależności od charakterystyki hosta docelowego,
p. mechanizm bezpiecznej aktualizacji sygnatur. Zestawy sygnatur/reguł muszą być pobierane z serwera w sposób uniemożliwiający ich modyfikację przez osoby postronne,
q. możliwość definiowania wyjątków dla sygnatur z określeniem adresów IP źródła, przeznaczenia lub obu jednocześnie,
r. obsługę reguł Snort,
s. możliwość wykorzystania informacji o sklasyfikowanych aplikacjach do tworzenia reguł IPS
t. mechanizmy automatyzacji w zakresie wskazania hostów skompromitowanych (ang. Indication of compromise),
u. mechanizmy automatyzacji w zakresie automatycznego dostrojenia polityk bezpieczeństwa.

24. System filtracji URL musi zapewniać:
    a. kategoryzację stron – w co najmniej 70 kategoriach,
    b. bazę URL o wielkości nie mniejszej niż 250 mln URL.
25. Urządzenie musi zapewniać możliwość wykrywania i śledzenia transferu następujących kategorii plików w ruchu sieciowym:
    a. pliki systemowe,
    b. pliki graficzne,
    c. pliki PDF,
    d. pliki wykonywalne,
    e. pliki multimedialne,
    f. pliki pakietu Office,
    g. pliki skompresowane,
26. Urządzenie musi posiadać możliwość monitorowania jak i kontrolowania transferu plików w następujących protokołach: HTTP, SMTP, FTP, IMAP, POP3, NetBIOS (SMB) w danym kierunku – upload/download.
27. Urządzenie musi posiadać wbudowany podsystem wykrywania oprogramowania złośliwego (malware) i jego propagacji w strefie chronionej poprzez:

   a. sprawdzenie reputacji plików w systemie globalnym,
   b. sprawdzenie plików w sandbox (realizowanym lokalnie lub w chmurze,)
   c. statyczną analizę struktury całego pliku pod kątem charakterystycznych elementów używanych w złośliwym oprogramowaniu.
28. Urządzenie musi zapewniać możliwość zapisania na dysk twardy kopii analizowanych plików o następujących charakterystykach:
   a. pliki wolne od złośliwego kodu,
   b. pliki zawierające złośliwy kod,
   c. pliki podejrzane,
   d. pliki o własnej, zdefiniowanej przez użytkownika kategorii.
29. Urządzenie musi posiadać podsystem wykrywania oprogramowania złośliwego zawierający narzędzia analizy historycznej dla plików przesłanych w przeszłości, a rozpoznanych jako oprogramowanie złośliwe (analiza retrospektywna).
30. Oprogramowanie urządzenia/urządzenie musi posiadać funkcję weryfikacji aplikacji bez rozszywania sesji TLS, informacje pozyskanie w trakcie nawiązywania sesji TLS muszą posłużyć do wykrywania aplikacji oraz podejmowania działań.
31. Urządzenie musi być objęte 5-letnim serwisem świadczonym bezpośrednio przez producenta w reżimie 8x5xNBD uprawniającym do wymiany sprzętu w przypadku zdiagnozowania awarii urządzenia, wsparcia telefonicznego i mailowego w zakresie konfiguracji urządzenia oraz do aktualizacji oprogramowania urządzenia. Dostęp do aktualizacji sygnatur IPS, mechanizmów filtrowania webowego i aktualizacji filtrów antymalware'owych przez okres 5 lat.

Przygotował:

Administrator Systemu Informatycznego AST

mgr Witold Stępień

Zatwierdził:
Kanclerz AST

mgr inż. Leszek Bednarz

Kraków, 25 lipca 2024 r.