Warszawa dnia 31.07.2020 r.

Strona WWW

Dotyczy postępowania: COI-ZAK.262.20.2020

WYJAŚNIENIA I ZMIANA SIWZ NR 1

Centralny Ośrodek Informatyki, działając jako Zamawiający, w postępowaniu na **rozbudowę infrastruktury systemów nadzoru i bezpieczeństwa (5 części),** na podstawie art. 38 ust. 2 i 4 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tj. Dz. U. z 2019 r., poz. 1843 z późn. zm.), przedstawia poniżej treść pytań Wykonawców wraz z udzielonymi odpowiedziami oraz zmianę treści SIWZ:

Dotyczy Część I: Dostawa i wdrożenie systemu NGFW

PYTANIE NR 1:

Nr	Treść	Pytanie
3.2	NGFW musi dostarczać mechanizm szyfrowania danych, który będzie posiadał certyfikacje FIPS 140-2 lub równoważny.	Prosimy o dopuszczenie rozwiązania, którego proces certyfikacji FIPS 140-2 jest prowadzony, a przewidywany czas ukończenia to Q1 2021, a system operacyjny oferowanego urządzenia pozwala na uzyskanie certyfikatu ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN.

Odpowiedź:

Zamawiający podtrzymuje zapisy SIWZ, jednocześnie Zamawiający wyjaśnia, że zgoda na zaproponowane rozwiązanie byłaby zgodą na nierówne traktowanie Wykonawców.

PYTANIE NR 2:

Nr	Treść	Pytanie
3.4	Zgodność sprzętu z profilem zabezpieczeń Common Criteria – „collaborative Protection Profile for Stateful Traffic Filter Firewalls” lub równoważnym	Prosimy o dopuszczenie rozwiązania, którego proces certyfikacji Common Criteria jest prowadzony, a przewidywany czas ukończenia to Q3 2020, a system operacyjny oferowanego urządzenia we wcześniejszych wersjach uzyskiwał już wymagany certyfikat CC oraz pozwala na uzyskanie certyfikatu ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN.

Odpowiedź:

Zamawiający podtrzymuje zapisy SIWZ, jednocześnie Zamawiający wyjaśnia, że zgoda na zaproponowane rozwiązanie byłaby zgodą na nierówne traktowanie Wykonawców.

PYTANIE NR 3:

Nr	Treść	Pytanie
10	NGFW musi być wyposażony w co najmniej dwa dyski twarde (na system) w konfiguracji redundantnej (min. RAID1) każdy o pojemności nie mniejszej niż 240GB.	W punkcie III.1.2 SZCZEGÓŁOWE WYMAGANIA DLA DOSTAWY NGFW podpunkt 10 Zamawiający pisze: *NGFW musi być wyposażony w co najmniej dwa dyski twarde (na system) w konfiguracji redundantnej (min. RAID1) każdy o pojemności nie mniejszej niż 240GB.* Jednocześnie Zamawiający wymaga dostawy konsoli NFGW, która jest wyposażona w dyski zapewniające co najmniej 1,6TB użytecznej przestrzeni na przechowanie danych na dyskach zestawionych w RAID1. O ile Konsola NGFW będzie w postaci redundantnej, a jednocześnie każda oddzielna konsola posiada dyski w postaci redundantnej, dodatkowa redundancja dysków na urządzeniu NFGW wydaje się nadmiarowa, i przyczyni się w podniesienie ceny oferowanych urządzeń. Prosimy zatem o dopuszczenie alternatywnego rozwiązania NGWF, które posiada pojedynczy dysk o pojemności 480GB.

Odpowiedź:

Zamawiający podtrzymuje zapisy SIWZ i nie dopuszcza sytuacji, aby nie było redundancji na poziomie dysków w urządzeniu NGFW.

PYTANIE NR 4:

Nr	Treść	Pytanie
14.4	Producent systemu NGFW musi umożliwić aktualizowanie kategorii typu TOR, C&C, proxy anonimizujące, złośliwe strony typu Phishing	Zwracamy uwagę, iż połączenia do sieci TOR oraz serwerów C&C możliwe jest nie tylko z poziomu przeglądarki z wykorzystaniem protokołu http, lecz tez innymi metodami i protokołami. Prosimy o dopuszczenie rozwiązania, które umożliwia wykrywanie i blokowanie ruchu do sieci TOR i serwerów C&C nie w module „Kategoryzacji www" lecz w module kontroli aplikacji i/lub w module IPS.

Odpowiedź:

Zamawiający nie precyzuje jaki moduł ma realizować przedmiotowe wymaganie. Zamawiający dopuszcza zaproponowane rozwiązanie pod warunkiem dostarczenia odpowiednich licencji.

PYTANIE NR 5:

Nr	Treść	Pytanie
15.4	Musi umożliwiać automatyczne dodawanie Feed-ów z zewnętrznych serwerów oraz bezpośrednio z plików CSV zawierających listy adresów IP, domen, URL.	Czy Zamawiający dopuści rozwiązanie, które umożliwia wykorzystanie skryptów API dostarczonych przez dostawcę do konwersji plików csv w celu implementacji zmian w konfiguracji?

Odpowiedź:

Zamawiający dopuszcza zaproponowane rozwiązanie, ale przy założeniu pełnej automatyzacji.

PYTANIE NR 6:

Nr	Treść	Pytanie
15.6	Ochrona przed atakami typu flood: SYN (w tym TCP) floods, UDP (w tym DNS query) floods, IP floods, ICMP floods, HTTP floods Anomalie dot. floods związanymi z niestandardowymi pakietami.	Czy Zamawiający dopuści rozwiązanie równoważne zapewniające ochronę przed DDoS: tcp_syn_flood tcp_port_scan tcp_src_session tcp_dst_session udp_flood udp_scan udp_src_session udp_dst_session icmp_flood icmp_sweep icmp_src_session icmp_dst_session sctp_flood sctp_scan sctp_src_session sctp_dst_session

Odpowiedź:

Zamawiający podtrzymuje zapisy SIWZ oraz dopuszcza dostarczenie dodatkowych funkcjonalności.

PYTANIE NR 7:

Nr	Treść	Pytanie
15.11	Musi umożliwić ochronę (np. „virtual patching” na poziomie sieci) przed próbami wykorzystania podatności (luk) w chronionych systemach	Czy Zamawiający uzna wymaganie za spełnione, jeże dostarczone rozwiązanie umożliwi utworzenie dedykowanego profilu IPS do ochrony określonych usług ze

		względu na cel (klient / server), severity, protokół, system operacyjny, aplikację?

Odpowiedź:

Zamawiający podtrzymuje zapisy SIWZ. Funkcjonalność musi być zapewniona bezpośrednio przez moduł IPS w NGFW.

PYTANIE NR 8:

Nr	Treść	Pytanie
18	Dwie Konsole NGFW muszą działać na fizycznych urządzeniach (ang. hardware appliance)	Czy Zamawiający dopuszcza dostarczenie oddzielnej pary konsol do zarządzania oraz oddzielnej do logowania i raportowania?

Odpowiedź:

Zamawiający podtrzymuje zapisy SIWZ.

PYTANIE NR 9:

Nr	Treść	Pytanie
19.5	Musi umożliwiać sprawdzenie wpływu na chroniony ruch sieciowy, nowo pobranych sygnatur IPS przed ich zatwierdzeniem.	Sygnatury są aktualizowane kiedy wykryte są nowe ataki, powinny być aktywowane bez zbędnej zwłoki, prosimy o usunięcie wymagania lub jego zmianę dopuszczającą rozwiązanie, gdzie filtry w profilach ochronnych IPS są tworzone w oparciu o cel (klient / server), severity, protokół, system operacyjny, aplikację.

Odpowiedź:

Zamawiający podtrzymuje zapisy SIWZ.

Zamawiający nie dopuszcza sytuacji, aby były aktywowane nowe sygnatury bez możliwości ich wcześniejszej weryfikacji na zasadzie sprawdzenia czy i jaki ruch byłby zablokowany.

PYTANIE NR 10:

Nr	Treść	Pytanie
20.2	Konsola NGFW nie może być w żaden sposób limitowana, jeśli chodzi o ilość danych. Może ją jedynie ograniczać ilość zasobów dyskowych Konsoli NGFW.	Producenci często podają ograniczenia wydajnościowe na ilość przetwarzanych danych dziennie. Również Zamawiający w punkcie 19.12 dopuszcza rozwiązanie posiadające ograniczenie wydajnościowe. Czy Zamawiający uzna warunek za spełniony dla rozwiązania które posiada ograniczenie wydajnościowe na przetwarzanie 150GB logów dziennie.

Odpowiedź:

Zamawiający podtrzymuje zapisy SIWZ. Zamawiający nie jest w stanie na obecną chwilę oszacować skali przetwarzanych logów dziennie stąd zapisany (w wymaganiu 19.12) limit wydajnościowy odnosi się do ilości zasobów dyskowych oraz zasobów tj. CPU i RAM.

PYTANIE NR 11:

5. Wydajność:

Całkowita wydajność pojedynczego NGFW w trybie ochrony FW (ang. FireWall), IPS (ang. Intrusion Prevention system) i kontroli aplikacji – nie mniejsza niż 20Gbps

Czy wskazana wydajność 20Gbps jest wydajnością, którą producenci podają w swojej dokumentacji „data sheet" osiąganą w warunkach laboratoryjnych przy stałej wielkości pakietów z reguły 1024 bajty, czy jest to wydajność urządzenia dla warunków zbliżonych do rzeczywistych przykładowo:

10% pakietów 128 Bajtów

35% pakietów 450 Bajtów

55% pakietów 1024 Bajty

Odpowiedź:

Zamawiający będzie polegał na deklaracjach producentów NGFW i nie określa wielkości pakietów.

PYTANIE NR 12:

7. Niezawodność:

NGFW musi mieć możliwość stworzenia klastra typu active/active i active/standby

Czy Zamawiający wymaga, aby klaster typu active/active miał możliwość zastosowania więcej niż dwóch urządzeń NGFW w celu przyszłej rozbudowy systemu?

Odpowiedź:

Zamawiający dopuszcza, ale nie wymaga, możliwości zastosowania więcej niż dwóch urządzeń NGFW w celu przyszłej rozbudowy systemu.

PYTANIE NR 13:

9. Asymetryczność ruchu:

9.1 Ruch pomiędzy dwoma ośrodkami przetwarzania danych jest asymetryczny i dwa NGFW muszą mieć możliwość zachowania stanu sesji (musi być możliwość skonfigurowania klastra w drugiej warstwie modelu OSI).

Czy poprzez ten punkt Zamawiający rozumie, że dwa urządzenia mają działać w klastrze w taki sposób, że jedno z urządzeń NGFW ma pełną informację o całej pojedynczej sesji w obu kierunkach i na tej podstawie podejmuje decyzje o blokowaniu lub przepuszczeniu ruchu a nie każde urządzenie z osobna analizujące jedynie połowę pojedynczej sesji w jednym kierunku?

Odpowiedź:

Zamawiający musi otrzymać możliwość (funkcjonalność + odp. ew. licencje) ochrony ruchu sieciowego w przypadku, gdy występuje asymetryczność ruchu pomiędzy dwoma DC i przy założeniu, że w każdym z tych DC będzie NGFW.

PYTANIE NR 14:

10. Pamięć wewnętrzna na OS:

NGFW musi być wyposażony w co najmniej dwa dyski twarde (na system) w konfiguracji redundantnej (min. RAID1) każdy o pojemności nie mniejszej niż 240GB.

Czy Zamawiający dopuści rozwiązanie oferujące pojedynczy dysk SSD o pojemności 400 GB?

Odpowiedź:

Zamawiający podtrzymuje zapisy SIWZ dot. wymaganej redundancji na poziomie dysków twardych.

PYTANIE NR 15:

14. Kategoryzacja www:

14.1. System musi obsługiwać mechanizm filtrowania stron WWW w zależności od kategorii treści (min. 10 kategorii).

14.4. Producent systemu NGFW musi umożliwić aktualizowanie kategorii typu TOR, C&C, proxy anonimizujące, złośliwe strony typu Phishing.

Czy Zamawiający wymaga kategoryzacji stron WWW tylko w odniesieniu do bezpieczeństwa i takich kategorii jak TOR, C&C, proxy anonimizujace, złośliwe strony typu Phishing, czy wymaga również filtrowania w oparciu o bazy takich kategorii jak: treści dla dorosłych, hazard, strony typu Social Networks?

Odpowiedź:

Zamawiający dopuszcza, ale nie wymaga możliwości dostarczenia rozszerzonej funkcjonalności.

PYTANIE NR 16:

15. Ochrona NGFW – funkcjonalność:

15.4. Musi umożliwiać automatyczne dodawanie Feed- ów z zewnętrznych serwerów oraz bezpośrednio z plików CSV zawierających listy adresów IP, domen, URL.

Czy Zamawiający dopuści rozwiązanie pozwalające na dodawanie listy adresów IP, domen oraz URLi z plików typu TXT zamiast CSV?

Odpowiedź:

Zamawiający dopuszcza format pliku typu CSV lub TXT.

Zamawiający zmienia zapis w pkt III.1.2, wiersz 15 Ochrona NGFW – funkcjonalność, ppkt 15.4 Rozdziału II SIWZ – Opis Przedmiotu Zamówienia, nadając mu następującą treść:

„Musi umożliwiać automatyczne dodawanie Feed-ów z zewnętrznych serwerów oraz bezpośrednio z plików CSV lub TXT zawierających listy adresów IP, domen, URL."

PYTANIE NR 17:

15.6. Ochrona przed atakami typu flood:

- **SYN (w tym TCP) floods,**
- **UDP (w tym DNS query) floods,**
- **IP floods,**
- **ICMP floods,**
- **HTTP floods Anomalie dot. Floods związane z niestandardowymi pakietami.**

Czy fragment „HTTP floods Anomalie dot. Floods związane z niestandardowymi pakietami" powinien zostać rozdzielony na dwa oddzielne punkty jak poniżej?

- HTTP floods
- Anomalie dot. Floods związane z niestandardowymi pakietami

Odpowiedź:

Zamawiający zmienia zapis w pkt III.1.2, wiersz 15 Ochrona NGFW – funkcjonalność, ppkt 15.6 Rozdziału II SIWZ – Opis Przedmiotu Zamówienia, nadając mu następującą treść:

„Ochrona przed atakami typu flood:

- *SYN (w tym TCP) floods,*
- *UDP (w tym DNS query) floods,*
- *IP floods,*
- *ICMP floods,*

- *HTTP floods*
- *Anomalie dot. floods związanymi z niestandardowymi pakietami.”*

PYTANIE NR 18:

Czy zamawiający dopuszcza by tego typu ochrona przed DDOS/floods realizowana była jedynie poprzez mechanizmy ograniczania sesji połówkowych i niezakończonych oraz ograniczania wolumenu ruchu czy jednak Zamawiający wymaga by ta funkcjonalność realizowana była poprzez dedykowany do tego typu ochrony system z behawioralną detekcją tego typu ataków bazujący na specjalnych algorytmach wspomagających trafną detekcję DDOS/Floods.

Odpowiedź:

Zamawiający podtrzymuje zapisy SIWZ.

PYTANIE NR 19:

15.7. Ochrona przed atakami typu „Drive-by-download”.

Czy Zamawiający dopuści rozwiązanie oferujące zabezpieczenie przed skutkami tego typu ataków, czyli blokowanie ruchu do domen C&C i próbę uzyskania dostępu do skompromitowanego systemu, czy wymagana jest pełna analiza pliku pod kątem detekcji malware’u z możliwością przesłania do analizy dynamicznej w systemie sandbox badanego pliku?

Odpowiedź:

Zamawiający podtrzymuje zapisy SIWZ. Zamawiający nie wymaga pełnej analizy pliku pod kątem detekcji malware’u.

PYTANIE NR 20:

17. Komunikacja szyfrowana:

17.1 Musi mieć możliwość przesyłania ruchu zaszyfrowanego (co najmniej TLS/SSL) do zewn. deszyfratora.

Czy Zamawiający dopuszcza rozwiązanie z możliwością przesyłania całego ruchu na porcie 443 do zewnętrznego deszyfratora?

Odpowiedź:

Zamawiający dopuszcza rozwiązanie z możliwością przesyłania całego ruchu na porcie 443 do zewnętrznego deszyfratora.

PYTANIE NR 21:

Czy Zamawiający dopuszcza rozwiązanie bez możliwości przesyłania ruchu zaszyfrowanego TLS/SSL do zewnętrznego deszyfratora, gdy NGFW jest w stanie zapewnić deszyfrację lokalnie zarówno dla systemów wewnętrznych poprzez zaimportowanie klucza prywatnego jak i dla systemów zewnętrznych z nieznanym kluczem prywatnym, do których dostają się użytkownicy?

Odpowiedź:

Zamawiający dopuszcza rozwiązanie bez możliwości przesyłania ruchu zaszyfrowanego TLS/SSL do zewnętrznego deszyfratora pod warunkiem utrzymania parametrów wydajnościowych przy włączonej lokalnej deszyfracji.

PYTANIE NR 22:

19. Wymagania funkcjonalne:

19.4. Musi pozwalać na automatyczne usuwanie logów i raportów przetrzymywanych na urządzeniu po upływie określonego czasu i po zarejestrowaniu problemów z miejscem na dysku.

Czy Zamawiający dopuści rozwiązanie, w którym logi są usuwane automatycznie jednak nie po upływie określonego czasu i po zarejestrowaniu problemów z miejscem na dysku, ale po wypełnieniu zdefiniowanego ręcznie obszaru pamięci na dysku dedykowanego dla danego typu logów. Takie rozwiązanie zapewnia dużo większą kontrolę nad przechowywaniem logów i nie dopuszcza do sytuacji, w której logi niektórych typów - jak np. logi z połączeń, których jest z reguły dużo więcej niż innych ważniejszych logów jak np. ze zdarzeń bezpieczeństwa - zajmą zbyt dużą przestrzeń dyskową. W takiej sytuacji czas przechowywania logów ze zdarzeń bezpieczeństwa byłby zbyt krótki.

Odpowiedź:

Dopuszcza się usuwanie logów ze względu na typ logów ale pod warunkiem, że w pierwszej kolejności będą usuwane najstarsze logi.

PYTANIE NR 23:

19.5. Musi umożliwiać sprawdzenie wpływu na chroniony ruch sieciowy, nowo pobranych sygnatur IPS przed ich zatwierdzeniem.

Czy Zamawiający dopuszcza rozwiązanie bez funkcjonalności sprawdzenia wpływu nowych sygnatur IPS na ruch przed ich zatwierdzeniem, gdy system w momencie aktualizacji reguł IPS podtrzymuje aktualne sesje do ich zakończenia.

Odpowiedź:

Zamawiający podtrzymuje zapisy SIWZ i zgadza się, że funkcjonalność nie musi dotyczyć aktualnie nawiązanych sesji.

PYTANIE NR 24:

19.12 Musi umożliwiać zbieranie zarejestrowanych zdarzeń bezpieczeństwa oraz inf. dot. połączeń (z chronionego ruchu sieciowego) przechodzących przez w/w NGFW (nie może być żadnych limitów licencyjnych z tym związanych prócz limitów dot. pojemności dyskowej /wydajnościowych) i musi być możliwość wysyłania tych informacji do systemu klasy SIEM (wraz z adresem IP zawartym w polu XForwarded-For).

Czy Zamawiający dopuści rozwiązanie, w którym automatyczna rotacja logów jest włączona stale i nie jest zależna bezpośrednio od przestrzeni dyskowej, ale od wypełnienia zdefiniowanego ręcznie obszaru pamięci na dysku dedykowanego dla danego typu logów. Takie rozwiązanie zapewnia dużo większą kontrolę nad przechowywaniem logów i nie dopuszcza do sytuacji, w której logi niektórych typów - jak np. logi z połączeń, których jest z reguły dużo więcej niż innych ważniejszych logów jak np. ze zdarzeń bezpieczeństwa - zajmą zbyt dużą przestrzeń dyskową. W takiej sytuacji czas przechowywania logów ze zdarzeń bezpieczeństwa byłby zbyt krótki.

Odpowiedź:

Dopuszcza się automatyczną rotację logów zależną od wypełnienia zdefiniowanego ręcznie obszaru pamięci, ale pod warunkiem, że będą w pierwszej kolejności usuwane najstarsze logi.

Niniejsze wyjaśnienia i zmiany stanowią integralną część SIWZ.

/-/ Katarzyna Wasilewska
Dyrektor Generalny