Warszawa, dnia 26 października 2016 r.

RZĄDOWE CENTRUM LEGISLACJI
BIURO ADMINISTRACYJNE

RCL.BA.2711.12/2016

Wykonawcy biorący udział
w zapytaniu

Dotyczy: **Zapytania ofertowego na „Sprzedaż, dostawę, instalację i konfigurację systemu zapobiegania i wykrywania zagrożeń zamaskowanych, nierozpoznanych i zagrożeń typu zero-day"**

W związku z wpłynięciem pytań do Załącznika nr 1 przedmiotowego Zapytania ofertowego - Szczegółowy opis przedmiotu zamówienia, zwanego dalej „OPZ", Rządowe Centrum Legislacji, zwane dalej „Zamawiającym", poniżej udziela wyjaśnień:

Pytanie 1)
Dotyczy: pkt I.2 OPZ.
Czy zamawiający wymaga, aby wszystkie moduły chłodzenia znajdujące się w urządzeniu podlegały wymianie?

Odpowiedź:
Nie. Zamawiający wymaga, by wymianie podlegały moduły zasilania wraz z wentylatorami, jeśli są one wbudowane w te moduły.

Pytanie 2)
Dotyczy: pkt I.2 OPZ.
Czy zamawiający dopuszcza rozwiązanie, w którym w appliance sprzętowym wykrywającym zamaskowane zagrożenia, będzie możliwość bezprzerwowej wymiany zasilaczy? (Bez możliwości bezprzerwowej wymiany wszystkich modułów chłodzenia)?

Odpowiedź:
Zamawiający dopuszcza powyższe rozwiązanie.

Pytanie 3)

Dotyczy: pkt. I.3 OPZ.

Jakie skutki analizy otwarcia pliku powinny wywoływać podjęcie akcji „zablokuj/prześlij do odbiorcy" i dla jakich protokołów ma być wykonywana każda z w.w akcji?

Odpowiedź:

System „zablokuje" plik w przypadku gdy po weryfikacji uzna go za niebezpieczny lub „prześle dalej" jeżeli sklasyfikuje go jako nie stanowiący zagrożenia. Akcje mają być wykonywana dla protokołów wymienionych w pkt. I.5 OPZ.

Pytanie 4)

Dotyczy pkt I.10 OPZ.

Co Zamawiający dokładnie rozumie przez „wyłączenie wysyłania informacji przez Internet"?

Czy chodzi o zablokowanie wysyłania próbek pozyskanych na podstawie analizy protokołów do chmury producenta zajmującej się analizą?

Prośba o sprecyzowanie, jakie informacje nie mogą być wysyłane do Internetu a, gdyż np. zablokowanie dostępu do sieci Internet, dla próbek wykonujących się na systemach wirtualnych może uniemożliwiać wykrycie złośliwego oprogramowania (np. w przypadku pobierania złośliwego kodu z Internetu, dopiero po uruchomieniu się próbki).

Odpowiedź:

Pliki skanowane przez system nie mogą być wysyłane przez internet. Dodatkowo system musi posiadać możliwość wyłączenia wysłania wszystkich informacji o plikach przez internet (w tym próbek, hashy).

Pytanie 5)

Dotyczy pkl I.11 OPZ.

Co zamawiający rozumie przez obsługę 700 użytkowników?

Odpowiedź:

System musi być przystosowany do pracy w ruchu generowanym przez co najmniej 700 użytkowników, dla protokołów wymienionych w pkt I.5 OPZ.

Pytanie 6)

Dotyczy pkl I.11 OPZ.

Co zamawiający rozumie przez obsługę 700 skrzynek pocztowych?

Odpowiedź:

System musi być przystosowany do pracy w ruchu generowanym przez co najmniej 700 skrzynek pocztowych, dla ruchu SMTP.

Pytanie 7)

Dotyczy pkl I.11 OPZ.

Czy 250 000 tysięcy plików to poprawna liczba, biorąc pod uwagę, fakt, że sandboxing to pełne uruchomienie danej próbki w maszynie wirutalnej (zakładana ilość to 8 maszyn), a uruchomienie próbki to ok 3-4 minuty, wartość wydaje się być nieadekwatna?

Odpowiedź:

W tej liczbie Zamawiający nie wymaga, aby system przeprowadzał pełny sandboxing. Liczba ta obejmuje także weryfikację plików przy pomocy innych mechanizmów (np. hash pliku, innych mechanizmów umożliwiających ocenę pliku nie wykorzystując pełnego sandboxingu) i na tej podstawie podjęcie akcji „zablokuj/prześlij dalej".

Pytanie 8)

Dotyczy pkl I.11 OPZ.

Czy Zamawiający dopuszcza rozwiązanie, które w ciągu godziny potrafi wykonać pełen sandboxing dla 160 plików (wynika to z prostego obliczenia 60 minut przez 3 minuty to ok 20 plików per maszyna razy 8 maszyn VM) oraz 6 000 plików skanowanych AV na godzinę?

Odpowiedź:

Zamawiający nie definiuje wymagania dotyczącego ilości plików, które podlegać mają pełnemu sandboxingowi.

Pytanie 9)

Dotyczy pkl I.12 OPZ.

Czy Zamawiający dopuszcza rozwiązanie, w którym zarządzanie konfiguracją, polityką skanowania, profilami maszyn wirtualnych oraz przeglądanie logów znajduje się na urządzeniu wykonującym analizę zamaskowanych zagrożeń?

Odpowiedź:

Tak. Zamawiający dopuszcza powyższe rozwiązanie.

Pytanie 10)

Dotyczy pkl I.13 OPZ.

Czy współpraca w postaci wysyłania informacji o zagrożeniach za pomocą protokołu SYSLOG do Checkpoint SmartEvent jest wystarczająca?

Odpowiedź:

Nie, oprogramowanie SamartEvent musi rozpoznawać nadesłane logi, czyli posiadać niezbędne parsery umożliwiające właściwą korelację oraz prawidłowe tworzenie dashbordów i raportów.

Pytanie 11)

Dotyczy pkl I.13 OPZ.

Jakich korelacji musi dokonywać dostarczony system?

Odpowiedź:

System musi dokonywać korelacji, które są możliwe do przeprowadzenia w systemie SmartEvent.

Pytanie 12)

Dotyczy pkl I.6 OPZ.

Co dokładnie Zamawiający rozumie przez „obsługę plików"?

Odpowiedź:

Zamawiający poprzez „obsługę plików" rozumie rozpoznanie i możliwość emulacji w środowisku sandboxing.

Pytanie 13)

Dotyczy pkl I.14 OPZ.

W jakim trybie docelowo mają być wpięte te urządzenia?

Odpowiedź:

Zamawiający nie definiuje w jakim trybie docelowo mają być podłączone urządzenia. Wszystkie wymagane tryby pracy muszą być wspierane przez dostarczone urządzenia.

Pytanie 14)

Dotyczy pkl I.14 OPZ.

Czy urządzenia mają być redundantne lub zapewniać obejście na wypadek awarii?

Odpowiedź:

Nie. Urządzenia nie muszą być redundantne ani zapewniać obejścia na wypadek awarii.

Pytanie 15)

Dotyczy pk1 I.14 OPZ.

Czy Zamawiający dopuszcza rozwiązanie, w którym scentralizowane zarządzanie dla wymienionych urządzeń będzie polegało na zarządzaniu polityką analizy zamaskowanego oprogramowania na urządzeniu dokonującym właściwej analizy (sandboxing)?

Odpowiedź:

Zamawiający nie dopuszcza powyższego rozwiązania.

Jednocześnie, Zamawiający informuje, iż termin składania ofert ulega zmianie i upływa w dniu 27 października 2016 r. o godz. 12:00.

DYREKTOR
Biura Administracyjnego
Wiesław Zarzecki