



Zastępca Prezesa
Aneta Burghardt

Wykonawcy

Wasze pismo znak:

Data:

Nasz znak:

Data:

ZP.253 .DPiZP.2619.6.2023.IW

12.10.2023 r.

Dotyczy: postępowania o udzielenie zamówienia publicznego prowadzonego w trybie podstawowym na „Zakup usług konsultingowych z dziedziny cyberbezpieczeństwa”.

I. Działając na podstawie art. 284 ust. 2 ustawy z dnia 11 września 2019 roku Prawo zamówień publicznych (Dz. U. 2022 r. poz. 1605 ze zm.; dalej: „ustawa Pzp”) Agencja Restrukturyzacji i Modernizacji Rolnictwa z siedzibą w Warszawie przy Al. Jana Pawła II nr 70, zwana w dalszej treści pisma „Zamawiającym”, udziela odpowiedzi na pytania zgłoszone w przedmiotowym postępowaniu.

Pytanie 1

Co Zamawiający ma na myśli pisząc, że scenariusz powinien przedstawiać w postaci graficznej zarówno wektor ataku, jak i taktykę defensywną?

Odpowiedź:

Zamawiający wyjaśnia, że graficzna reprezentacja dotyczy poszczególnych faz ataków dla konkretnych scenariuszy wymaganych przez Zamawiającego. Jak wiadomo, realizacja ataku typu ransomware może przebiegać według różnych scenariuszy. Można wykorzystać np. technikę phishingu lub wiele innych technik związanych np. z przełamaniem aplikacji webowych. Wspomniane techniki dotyczą tak zwanej fazy dostarczania, która zwykle jest poprzedzana innymi fazami (np. faza rekonesansu, uzbrajania). Zamawiający wymaga opracowania konkretnych scenariuszy i przedstawienia poszczególnych faz w formie graficznej.

Graf taktyki defensywnej to zamodelowanie działań, które należy podjąć w ramach infrastruktury/systemów bezpieczeństwa przeciwdziałając atakowi ze scenariusza.

Pytanie 2

Jaki jest cel opracowania scenariuszy i procedur jeśli mają one być niepowiązane bezpośrednio z systemami ARiMR (wpisywanie narzędzi jest jedynie "dopuszczalne")?

Odpowiedź:

Zamawiający nie określił, że scenariusze oraz procedury mają być niepowiązane bezpośrednio z systemami ARiMR, tylko że muszą być uniwersalne. Dopuszczalność wpisania/zawarcia narzędzi, którymi dysponuje Zamawiający jest jedynie zezwoleniem na swobodną analizę środowiska ARiMR wymaganą do prawidłowej realizacji usługi. Zamawiający wymaga uniwersalnych scenariuszy, które łatwo mapują się na znane taktyki, techniki i procedury (TTP) wykorzystywane podczas zaawansowanych ataków w kontekście infrastruktury bezpieczeństwa Zamawiającego.

Pytanie 3

Warianty procedur są uzależnione od systemów IT i ITSec wykorzystywanych przez Zamawiającego. Czy wskazana maksymalna liczba wariantów może być ograniczona do 1?

Odpowiedź:

Zamawiający wyjaśnia, że procedura musi obejmować wszystkie systemy IT i IT-Sec będące w gestii Zamawiającego, jak również będące poza jego zarządzaniem. W wypadku systemów administrowanych/hostowanych przez osoby trzecie, gdzie procedura musiałaby objąć rekomendację dla ich konfiguracji np. polityka WAF, Anty-DDoS, powinna ona uwzględniać możliwe warianty działania jako pod-procedury dla głównej procedury, pod kątem rozpatrywanego scenariusza.

W związku z powyższym, liczba wariantów nie może być ograniczona do 1.

Pytanie 4

Czy wskazany zakres detekcji oznacza opis w jaki osoba obsługująca alarm ma dokonać jego weryfikacji? Czyli dla konkretnego scenariusza jakie sprawdzenia trzeba wykonać w powiązanych systemach IT ARiMR?

Odpowiedź:

Zamawiający potwierdza, że wskazany zakres detekcji oznacza opis w jaki osoba obsługująca alarm ma dokonać jego weryfikacji.

Pytanie 5

Co Zamawiający rozumie pod pojęciem "zautomatyzowane reagowanie oparte o analizę ryzyka"? Czy Wykonawca ma opisać istniejące automatyzacje odpowiedzi w powiązanych systemach ARiMR? Dokonać analizy możliwości takich automatyzacji? Czy może je wdrożyć?

Odpowiedź:

Zamawiający wyjaśnia, że użycie sformułowania „zautomatyzowane reagowanie oparte o analizę ryzyka” w tym wypadku polega w tym, że analiza ryzyka ma na celu ograniczenie negatywnego wpływu danej automatyzacji na procesy biznesowe. Można to uczynić np. poprzez wzbogacenie informacji o zdarzeniu w kolejnych systemach lub usługach typu threat intelligence. Wykonawca powinien dokonać analizy możliwości określonych automatyzacji oraz je wdrożyć w formie odpowiednich rekomendacji, bazując na posiadanej infrastrukturze Zamawiającego i swojej najlepszej wiedzy.

Pytanie 6

Jaki ma być konkretny zakres szkoleń, o których mowa w par. 4 ust 7 projektu umowy? Omówienie i zaprezentowanie raportu nie wymaga 40 roboczogodzin spotkań.

Odpowiedź:

Zamawiający wyjaśnia, że Szkolenie musi obejmować szeroki zakres taktyk i technik wykorzystywanych do klasyfikowania ataków, reagowania na nie oraz oceny ryzyka z tym związanego. Można zrealizować je w oparciu o MITRE ATT&CK w kontekście zaproponowanych scenariuszy i infrastruktury Zamawiającego.

Pytanie 7

Jeśli ww szkolenia mają być zrealizowane przed przekazaniem Raportu, a co za tym idzie odbiorem jego finalnej wersji, to oznacza, że realny czas na przygotowanie raportu skraca się do 10 roboczodni, co jest czasem niewystarczającym na realizację prac i niezgodnym z terminem realizacji. W jaki sposób Zamawiający zamierza zapewnić Wykonawcy 21 dni roboczych na realizację i wykonanie raportu końcowego?

Odpowiedź:

Zamawiający działając na podstawie przepisu art. 286 ust. 1 ustawy zmienia treść SWZ w następujący sposób.

1. W Rozdz. II SWZ, pkt 1 przyjmuje brzmienie:

„1. Część 1 zamówienia – Wykonawca zobowiązany jest do realizacji Usługi i wykonania Raportu końcowego spełniającego wymagania określone w ppu w terminie **28 Dni Roboczych** od dnia zawarcia Umowy, przy czym przez wykonanie Raportu końcowego rozumie się dostarczenie Raportu końcowego zaakceptowanego przez Zamawiającego poprzez podpisanie bez zastrzeżeń Protokołu Odbioru wg wzoru stanowiącego Załącznik nr 3 do ppu. Wykonawca przedstawi harmonogram wykonania Umowy terminie do 5 Dni Roboczych od podpisania Umowy.”

2. W Rozdz. II SWZ, pkt 2 przyjmuje brzmienie:



Zastępca Prezesa
Aneta Burghardt

„2. Część 2 zamówienia – Wykonawca zobowiązany jest do realizacji Usługi i wykonania Raportu końcowego spełniającego wymagania określone w ppu w terminie **28 Dni Roboczych** od dnia zawarcia Umowy, przy czym przez wykonanie Raportu końcowego rozumie się dostarczenie Raportu końcowego zaakceptowanego przez Zamawiającego poprzez podpisanie bez zastrzeżeń Protokołu Odbioru wg wzoru stanowiącego Załącznik nr 3 do ppu. Wykonawca przedstawi harmonogram wykonania Umowy terminie do 5 Dni Roboczych od podpisania Umowy.”

3. W Załączniku nr 10.1 do SWZ *projektowane postanowienia umowy*, § 4 pkt 1 przyjmuje brzmienie:

„1. Wykonawca zobowiązany jest do realizacji Usługi i wykonania Raportu końcowego spełniającego wymagania określone w Umowie w terminie **28 Dni Roboczych** od dnia zawarcia Umowy, przy czym przez wykonanie Raportu końcowego rozumie się dostarczenie Raportu końcowego zaakceptowanego przez Zamawiającego poprzez podpisanie bez zastrzeżeń Protokołu Odbioru wg wzoru stanowiącego Załącznik nr 3 do Umowy.”

4. W Załączniku nr 10.2 do SWZ *projektowane postanowienia umowy*, § 4 pkt 1 przyjmuje brzmienie:

„1. Wykonawca zobowiązany jest do realizacji Usługi i wykonania Raportu końcowego spełniającego wymagania określone w Umowie w terminie **28 Dni Roboczych** od dnia zawarcia Umowy, przy czym przez wykonanie Raportu końcowego rozumie się dostarczenie Raportu końcowego zaakceptowanego przez Zamawiającego poprzez podpisanie bez zastrzeżeń Protokołu Odbioru wg wzoru stanowiącego Załącznik nr 3 do Umowy.”

Ponadto działając na podstawie art. 286 ust. 1 ustawy, Zamawiający wprowadza następujące zmiany w treści SWZ:

ZMIANA NR 1

W Rozdziale IX.1 SWZ „Sposób oraz termin składania ofert i otwarcia ofert”, pkt. 2 i 3 otrzymują brzmienie:

„2. Termin składania ofert upływa w dniu **19 października 2023 r.** o godzinie 11.00

3. Otwarcie ofert odbędzie się w dniu **19 października 2023 r.** o godzinie 12.00”

ZMIANA NR 2

Rozdział VII SWZ „Termin związania ofertą”, otrzymuje brzmienie:

„Wykonawcy pozostają związani złożoną ofertą do dnia **17 listopada 2023 r.** Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.”

p.o. ZASTĘPCA PREZESA

Aneta Burghardt

