

Warszawa, 27.01.2014r.

Krajowe Biuro Wyborcze

Postępowanie ZP-3710-2/14: „Symetryczne łącze internetowe na 24 miesiące do siedziby Krajowego Biura Wyborczego”

Pytanie 1

Proponujemy uzupełnienie zapisu pkt I.5.2 SIWZ o sformułowanie dopuszczające przesyłanie ruchu pomiędzy sieciami Wykonawcy i Zamawiającego, w następującej formie: „Ruch z danymi podczas ataku DDoS nie może być wysyłany poza sieć Wykonawcy (zakaz nie dotyczy ruchu pomiędzy siecią wykonawcy i siecią Zamawiającego)”.

Odpowiedź:

Zakaz nie dotyczy ruchu między siecią Wykonawcy a siecią Zamawiającego.

Pytanie 2

W punkcie I.6. Zamawiający użył zwrotu „netflow”, który jest nazwą związaną z firmą CISCO Systems. Prosimy o wyjaśnienie, czy Zamawiający użył tej nazwy w rozumieniu zwyczajowym (jako odmiany protokołu sieciowego)? Oferent wnosi o dopuszczenie usług bazujących na rozwiązaniach równoważnych, na przykład Jflow, cflowd (Juniper Networks), NetStream (3Com/HP/Huawei), Cflowd (Alcatel-Lucent), Rflow (Ericsson), AppFlow (Citrix), Slow (wielu dostawców).

Odpowiedź:

Zamawiający dopuszcza usługi bazujące na ww. równoważnych protokołach sieciowych.

Pytanie 3

W punkcie IV.3. Zamawiający wymaga posiadania „procedur jakościowych równoznacznych z normą ISO 27001”. Prosimy o wyjaśnienie, według jakich kryteriów Zamawiający będzie oceniał równoznaczność procedur jakościowych

Odpowiedź:

Będzie oceniał na podstawie oświadczenia Wykonawcy, że posiada procedury jakościowe równoznaczne z normą ISO 27001, pozwalającą na wykonanie przedmiotu zamówienia.

Pytanie 4

Czy Zamawiający dopuszcza posiadanie przez wykonawcę nieaktualnego certyfikatu ISO 27001?

Odpowiedź:

Zamawiający nie żąda posiadania certyfikatu ISO 27001 przez Wykonawcę.
Żąda jedynie „posiadania procedur jakościowych równoznacznych z normą ISO 27001, pozwalających na wykonanie przedmiotu zamówienia”.

Pytanie 5

W punkcie IV.4 Zamawiający wymaga posiadania „certyfikatów dostawców platformy ochrony przed DDoS: ANCE (Arbor Networks Certified Engineer), OSCP (Offensive Security Certified Professional) lub/i OSCE (Offensive Security Certified Expert)”. Ze względu na zachowanie konkurencyjności w rozumieniu Ustawy wnioskujemy o dopuszczenie rozwiązań równoważnych (na przykład Incapsula, Radware, Verisign, ATMAN anti-DDoS, Akamai, Wanguard, Prolexic, CISCO, Juniper). Wnosimy o wprowadzenie zapisu umożliwiającego zastosowanie powyższych rozwiązań.

- a. W związku z wnioskiem opisanym powyżej wnosimy o dopuszczenie równoważnych certyfikatów w przypadku gdy oferent będzie wykorzystywał system ochrony przed atakami DDoS innego dostawcy niż Arbor Networks (na przykład Incapsula, Radware, Verisign, ATMAN anti-DDoS, Akamai, Wanguard, Prolexic, CISCO, Juniper).
- b. Jednocześnie, oferent proponuje wykreślenie z powyższego zapisu certyfikatów OSCP oraz OSCE gdyż dotyczą głównie umiejętności przełamywania zabezpieczeń serwerów i sieci, wykorzystywania luk w oprogramowaniu, tworzeniu ataków na zasoby sieciowe, natomiast nie zawierają żadnych elementów związanych z ochroną sieci i serwerów, zapobieganiu włamaniom, ani ochronie przed atakami DDoS.

Wyjaśnienie oferenta: Oczywiście jest konieczność dopasowania wymaganych certyfikatów do rozwiązań stosowanych przez oferenta. Proponujemy więc zastąpić wymóg posiadania certyfikatów ANCE, OSCP lub/i OSCE wymogiem oświadczenia oferenta o posiadaniu przez osoby przeznaczone do ochrony przed DDoS kompetencji związanych z ochroną przed atakami DDoS i kompetencji związanych ze stosowanym rozwiązaniem technicznym; alternatywnie - wymogiem posiadania certyfikatów związanych ze stosowanym rozwiązaniem technicznym ochrony przed atakami DDoS. Dodatkowo oferent wnosi o o opisanie wymagania stawianego przez Zamawiającego w rozumieniu Rozporządzenia Prezesa Rady Ministrów z dnia 19.02.2013 r. w sprawie rodzajów dokumentów, jakich może żądać zamawiający od wykonawcy, oraz form, w jakich te dokumenty mogą być składane, a także z uwzględnieniem Art. 22 pkt 4 ustawy PZP.

Odpowiedź:

Zamawiający dopuszcza ochronę przed atakiem DDoS podług innych certyfikatów, równoważnych certyfikatom ANCE (Arbor Networks Certified Engineer) i OSCP (*Offensive Security Certified Professional*) lub/i OSCE (*Offensive Security Certified Expert*).

Udokumentowanie – oświadczeniem Wykonawcy lub innym sposobem dokumentowania.

Pytanie 6

W punkcie VII.4.a.ostatni podpunkt Zamawiający wymaga podania czasu reakcji na atak DDoS w minutach. Prosimy o wyjaśnienie w jaki sposób stosowany będzie wzór z punktu XI.5.2) dla niecałkowitej ilości minut (na przykład 5,6 minuty lub 10,4 minuty).

Odpowiedź:

Należy podać czas reakcji z dokładnością 1 minuty.