**URZĄD MIEJSKI W KONINIE**
Wydział Informatyki

62-500 Konin, plac Wolności 1
63 2401111 (tel.)
63 2429920 (fax)

sekretariat@konin.um.gov.pl
www.konin.pl

IN.1333.42.2022

Konin, 19 maj 2022r.

## Dotyczy Publicznego Konkursu Ofert z dnia 10.05.2022 r. na:

*Zakup systemu bezpieczeństwa typu UTM dla Urzędu Miejskiego w Koninie" w ramach projektu* **„Cyfrowa Gmina"** Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia

W dniu 18.05.2022 r. firma it partners security sp. z o. o.
ul. Paderewskiego 35, 40-282 Katowice zwróciła się z następującymi pytaniami:

1. **Wymagania ogólne OPZ**

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji

*Pytanie. Czy zamawiający zaakceptuje rozwiązanie, które będzie miało możliwość budowy dwóch instancji – fizycznej i logicznej na tej samej platformie?*

**Odpowiedzi na zadane pytanie:**

Zamawiający podtrzymuje wymóg OPZ

2. **Punk 4. 2 OPZ**

System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.

*Pytanie. Czy zamawiający zaakceptuje rozwiązanie, które umożliwia podłączenie routera z funkcjonalnością modemu 3G/4G poprzez połączenie sieciowe Rj45, zamiast modemu USB? Z punktu działania tej funkcjonalności,będzie ono spełniało takie same wymagania.*

**Odpowiedzi na zadane pytanie:**

Zamawiający akceptuje możliwość podłączenia routera z funkcjonalnością modemu 3G/4G, ale zarówno port konsoli szeregowej jak i gniazdo USB również są wymagane.

3. **Punkt 5.2 OPZ**

Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 8 Gbps.

*Pytanie: Producenci stosują różne modele testowe dla deszyfrowania ruchu SSL. Proszę o wskazanie modelu testowego dla ruchu SSL w celu dobrania odpowiedniej modelu o podanej przepustowości SSL w NGFW.*

**Odpowiedzi na zadane pytanie:**

Testowy model ruchu SSL powinien być oparty o TLS v1.2 z algorytmem nie słabszym niż AES128-SHA256

4. **Punkt 6.10 OPZ**

Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.

*Pytanie. Czy niezamawiający dopuści rozwiązanie, które jako token programowy może wykorzystywać np. Google Autoanalizator lub token wysyłany przez email/sms w celu dwu-składnikowego uwierzytelniania*?

**Odpowiedzi na zadane pytanie:**

Zamawiający podtrzymuje wymóg OPZ

5. **Punkt 6.12 Analiza ruchu szyfrowanego protokołem SSH.**

*Pytanie: Czy zamawiający zaakceptuje rozwiązanie, które umożliw inspekcję RDPs i FTPS, które z punktu widzenia oceny bezpieczeństwa, są częściej używanymi niż analiza SSH. Pozwoli to niezamawiającemu na dogłębna analizę ruchu w tym protokołach.*

**Odpowiedzi na zadane pytanie:**

Zamawiający dopuszcza takie rozwiązanie

6. **Punkt 6.13 OPZ**

Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system

*Pytanie: Czy zamawiający akceptuje rozwiązanie, które zamiast lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH), będzie mógł wykrywać algorytm DGA oraz posiadać funkcjonalność DNS Sinkhole?*

**Odpowiedzi na zadane pytanie:**

Zamawiający podtrzymuje wymóg OPZ

7. **Punkt 7.6 OPZ**

Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.

- Amazon Web Services (AWS).
- Microsoft Azure
- Cisco ACI.
- Google Cloud Platform (GCP).
- Nuage Networks VSP.
- OpenStack.

- VMware vCenter (ESXi).
- VMware NSX
- VMware NSX.Nutanix
- VMware NSX.IBM Cloud

*Pytanie: Wyżej wymienione rozwiązania SDN, są pełną listą wspieranych przez rozwiązanie firmy Fortinet. Proszę o usunięcie wymagania, które nie jest odzwierciedleniem realnych potrzeb zamawiającego a jedynie ograniczeniem konkurencyjności.*

**Odpowiedzi na zadane pytanie:**

Zamawiający podtrzymuje wymóg, ale ogranicza listę rozwiązań SDN do posiadanego VM Ware vCenter.

**8. Punkt 12.5 OPZ**

System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.

*Pytanie: Usuwana aktywna zawartość w plikach PDF Microsoft Office bez konieczności blokowania transferu całych plików powoduje usunięcie częstsi składowych dokumentów, powodując niemożność ich otworzenia lub błędów dokumentów. Czy zamawiający uzna za spełnione, jeżeli rozwiązanie będzie miało możliwość analizy i blokowanie takich plików przez rozwiązanie Sandbox, pozwalające na wykrycie podejrzanego pliku w symulowanym, realnym środowisku systemu operacyjnego oraz poprzez analizę kodu plików i dokumentów.*

**Odpowiedzi na zadane pytanie:**

Zamawiający nie wyraża zgody na zastąpienie funkcji usuwania aktywnego kodu przez rozwiązanie sandbox i jednocześnie podtrzymuje wymóg dostawy systemu sandbox.

**9. Punkt 16.4 OPZ**

Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

*Pytanie. Użyte wymaganie, nie odzwierciedla realnych potrzeb zamawiającego. Czy zamawiający zaakceptuje rozwiązanie ,które zamiast Uwierzytelniania w oparciu o protokół SAML, będzie miało możliwość integracji z AD, LDAP, Radius, Tacacs + oraz Agile?*

**Odpowiedzi na zadane pytanie:**

Zamawiający akceptuje zaproponowane rozwiązanie.

**10. Punkt 18.1 OPZ**

Elementy systemu bezpieczeństwa muszą realizować logowanie do posiadanego przez zamawiającego urządzenia FortiAnalyzer-400E z możliwością raportowania

*Pytanie: Czy zamawiające zaakceptuje rozwiązanie, które będzie miało dedykowane rozwiązanie tego samego producenta w formie wirtualnej maszyny pozwalające realizowanie logowania oraz długie przechowywanie i analizy logów z proponowanego rozwiązania NGFW?*

**Odpowiedzi na zadane pytanie:**

Zamawiający dopuszcza, aby w ramach postępowania została dostarczona inna platforma logowania pod warunkiem, że będzie to platforma tego samego producenta co zaproponowane urządzenia UTM z tożsamą do nich gwarancją, a także będzie ona nie gorsza od obecnie posiadanej tj. będzie to platforma fizyczna, z przestrzenią dyskową co najmniej 12TB opartą o co najmniej 4 dyski twarde z możliwością konfiguracji RAID 0/1/5/10