Norway
grants

ZP.271.2.7.2024 Jarosław 06.03.2024 r.

Wykonawcy biorący udział w postępowaniu

dotyczy: przetargu nieograniczonego na zadanie

Dostawa serwerów, macierzy, urządzeń typu UTM i oprogramowania systemowego oraz świadczenie usług wdrożenia i szkolenia.
Zamówienie realizowane jest w ramach projektu „JarosLove – z miłości do ludzi" finansowanego ze środków Norweskiego Mechanizmu Finansowego 2014-2021 (85%) oraz budżetu państwa (15%), realizowanego w ramach programu „Rozwój Lokalny"

Działając na podstawie art. 135 ustawy z dnia ustawy z dnia 11 września 2019r. Prawo zamówień publicznych (*Dz. U. z 2023r., poz. 1605 tj*) – dalej „ustawa Pzp", **Zamawiający**: Gmina Miejska Jarosław, ul. Rynek 1, 37-500 Jarosław, **przekazuje treść zapytań dotyczących Specyfikacji Warunków Zamówienia** (SWZ), **wraz z udzielonymi odpowiedziami.**

1. **Zapis: Firewall musi umożliwiać uwierzytelnianie użytkowników z wykorzystaniem: ActiveDirectory, LDAP, Radius, SecureID oraz wewnętrznej bazy użytkowników. Czy rozważyliby Państwo możliwość zastosowania wirtualnego urządzenia uwierzytelniającego, które mogłoby być elastycznie dostosowane do infrastruktury wewnętrznej lub zewnętrznej? Taka opcja mogłaby oferować szerokie spektrum metodyk uwierzytelniania, zwiększając bezpieczeństwo i efektywność..**

   Odp. *Nie zgadzamy się z proponowanym rozwiązaniem zastosowania wirtualnego urządzenia uwierzytelniającego z następujących powodów:*

1. ***Złożoność konfiguracji i zarządzania:*** *Dodanie dodatkowego wirtualnego urządzenia uwierzytelniającego może wprowadzić złożoność zarządzania infrastrukturą, zwłaszcza jeśli istnieje już wiele różnych systemów uwierzytelniania. Konfiguracja, integracja i utrzymanie takiego rozwiązania mogą wymagać dodatkowych zasobów ludzkich i finansowych.*

2. ***Podatność na błędy i awarie:*** *Każda dodatkowa warstwa wirtualnego urządzenia wprowadza potencjalne punkty awarii i błędów. W przypadku awarii tego urządzenia użytkownicy mogą stracić dostęp do zasobów sieciowych, co negatywnie wpłynie na produktywność i działanie organizacji.*

3. ***Ryzyko związane z bezpieczeństwem:*** *Wprowadzenie kolejnego punktu uwierzytelniania może zwiększyć powierzchnię ataku i ryzyko naruszenia bezpieczeństwa. Każde dodatkowe oprogramowanie lub urządzenie staje się potencjalnym celem dla ataków hakerskich.*

4. ***Zwiększony koszt:*** *Implementacja dodatkowego wirtualnego urządzenia uwierzytelniającego może generować dodatkowe koszty związane zarówno z zakupem, jak i utrzymaniem tego rozwiązania. Koszty te mogą obejmować licencje, szkolenia personelu oraz utrzymanie infrastruktury IT.*

Norway
grants

2. **Zapis: Urządzenie musi umożliwiać uwierzytelnianie i rozpoznawanie użytkowników korzystających z Microsoft Terminal Services i CitrixXenApp. Rozumiemy, że Państwa potrzeby mogą ewoluować. Czy istnieje możliwość skupienia się na uwierzytelnianiu użytkowników przez Microsoft Terminal Services, jeśli obecnie nie wykorzystują Państwo funkcjonalności CitrixXenApp? To dostosowanie mogłoby przynieść korzyści w zakresie uproszczenia infrastruktury.**

   Odp. *Nie zgadzamy się z proponowanym podejściem skupienia się jedynie na uwierzytelnianiu użytkowników poprzez Microsoft Terminal Services, z pominięciem funkcjonalności Citrix XenApp, z następujących powodów:*

1. ***Zapewnienie elastyczności i skalowalności:*** *Choć obecnie może nie być potrzeby korzystania z funkcjonalności Citrix XenApp, przyszłe zmiany w potrzebach biznesowych mogą wymagać jego wdrożenia. Utrzymywanie zdolności do uwierzytelniania i rozpoznawania użytkowników dla obu platform umożliwi łatwiejszą adaptację do ewentualnych zmian w infrastrukturze IT.*
2. ***Uniknięcie blokady możliwości:*** *Skoncentrowanie się wyłącznie na jednym rodzaju usługi uwierzytelniania może ograniczyć możliwości rozwoju infrastruktury IT w przyszłości. Wprowadzenie wsparcia dla Citrix XenApp, nawet jeśli nie jest obecnie używane, umożliwi elastyczną reakcję na zmieniające się potrzeby organizacji.*
3. ***Zapewnienie spójności w obsłudze użytkowników:*** *Utrzymywanie jednolitej metodyki uwierzytelniania dla wszystkich użytkowników, niezależnie od tego, czy korzystają z Microsoft Terminal Services czy Citrix XenApp, ułatwi zarządzanie infrastrukturą i zapewni spójne doświadczenie dla użytkowników.*

3. **Zapis: Firewall musi obsługiwać minimum 4 400 000 jednoczesnych połączeń TCP oraz przyjmować nowe połączenia z wydajnością minimalną 95 000 nowych połączeń na sekundę. Czy Zamawiający zgodzi się 3 000 000 połączeń, co pozwoliłoby na optymalizację wydajności i kosztów?**

   Odp. *Zamawiający nie wyraża zgody na obniżanie parametrów do wskazanych w pytaniu, tj. 3 000 000 połączeń, z uwagi na następujące powody:*

1. ***Zachowanie minimalnych standardów wydajnościowych:*** *Określone w zapisie minimalne parametry wydajnościowe są wynikiem analizy potrzeb organizacji oraz uwzględniają przyszłe możliwości rozwoju infrastruktury. Obniżenie tych parametrów może prowadzić do niewystarczającej wydajności i ograniczenia możliwości rozwoju systemu w przyszłości.*
2. ***Zapewnienie bezpieczeństwa:*** *Wysoka liczba jednoczesnych połączeń oraz szybkość obsługi nowych połączeń są kluczowe dla zapewnienia niezawodności i bezpieczeństwa sieci. Obniżenie tych parametrów może zwiększyć ryzyko przeciążenia systemu, co może prowadzić do utraty danych lub nieautoryzowanego dostępu.*
3. ***Zachowanie konkurencyjności:*** *Zapewnienie wysokiej wydajności i niezawodności systemu może być kluczowe dla zachowania konkurencyjności na rynku. Obniżenie*

parametrów poniżej oczekiwań może skutkować utratą zaufania klientów i stratą konkurencyjności na rynku.

4. **Zapis: Urządzenie musi obsługiwać Perfect Forward Secrecy (PFS) z wykorzystaniem algorytmów Diffie-Hellman do wymiany kluczy przez email i web. Biorąc pod uwagę potencjalne ryzyko związane z PFS, czy Zamawiający zgodzi się na wykreślenie tego punktu z OPZ?**

Odp. *Zamawiający nie może wykreślić tego punktu z uwagi na istotność zapewnienia bezpieczeństwa wymiany kluczy przez email i web przy użyciu Perfect Forward Secrecy (PFS) z algorytmami Diffie-Hellman. Oto uzasadnienie:*

1. ***Ochrona danych:*** *PFS z algorytmami Diffie-Hellman zapewnia dodatkową warstwę ochrony danych poprzez uniemożliwienie potencjalnym atakującym odtworzenia poprzednich kluczy, nawet jeśli zostanie złamana jedna z kluczy sesji. W konsekwencji, utrzymanie tego punktu zabezpiecza wymianę kluczy, co pomaga chronić poufność i integralność przesyłanych danych.*
2. ***Zgodność z przepisami i regulacjami:*** *Wiele regulacji i standardów bezpieczeństwa, takich jak GDPR w Europie lub HIPAA w Stanach Zjednoczonych, wymaga zastosowania zaawansowanych mechanizmów ochrony danych, w tym PFS. Wykreślenie tego punktu mógłoby prowadzić do naruszenia wymagań związanych z ochroną danych osobowych i wiązać się z konsekwencjami prawnymi.*
3. ***Zachowanie bezpieczeństwa sieciowego:*** *W dzisiejszych czasach, kiedy zagrożenia związane z cyberbezpieczeństwem stale rosną, istotne jest utrzymanie najwyższych standardów bezpieczeństwa sieciowego. Wykreślenie tego punktu mogłoby otworzyć lukę w systemie, co zwiększyłoby ryzyko ataków i naruszeń bezpieczeństwa.*
4. ***Wzmacnianie zaufania:*** *Zachowanie PFS z algorytmami Diffie-Hellman w procesie wymiany kluczy przez email i web przyczynia się do wzmocnienia zaufania klientów i partnerów do organizacji. Wykreślenie tego punktu mogłoby zaszkodzić reputacji urzędu jako odpowiedzialnego i bezpiecznego partnera.*

5. **Zapis: Dla połączeń IPSec client-to-site musi być możliwość zestawienia połączenia VPN przed zalogowaniem się użytkownika do systemu? Chcielibyśmy zrozumieć, jak duża część Państwa użytkowników korzysta z VPN przed logowaniem. Ta informacja pomoże nam zaproponować rozwiązanie dopasowane do rzeczywistych potrzeb.**

Odp. *Funkcjonalność umożliwiająca zestawienie połączenia VPN przed zalogowaniem się użytkownika jest kluczowa, ponieważ równolegle prowadzimy działania mające na celu zainstalowanie urządzeń UTM (Unified Threat Management) w naszych jednostkach podległych. Oto uzasadnienie:*

1. ***Zapewnienie ciągłości działania:*** *Wdrożenie urządzeń UTM w jednostkach podległych ma na celu zwiększenie bezpieczeństwa sieci poprzez skuteczniejszą ochronę przed zagrożeniami zewnętrznymi. Funkcjonalność VPN przed logowaniem pozwala użytkownikom zdalnie łączyć się z siecią firmową, nawet przed zalogowaniem się do systemu, co zapewnia ciągłość dostępu do zasobów sieciowych.*

2. ***Optymalizacja działań użytkowników:*** *Wdrażając urządzenia UTM, możemy spodziewać się, że korzystanie z VPN przed logowaniem stanie się częstsze wśród użytkowników, którzy będą chcieli szybko i bezpiecznie uzyskać dostęp do zasobów sieciowych.*
3. ***Przyszłe potrzeby i skalowalność:*** *Przewidywane około 30 użytkowników docelowych w przyszłości wymaga elastycznego i skalowalnego podejścia do zarządzania dostępem do sieci. Funkcjonalność VPN przed logowaniem umożliwia dostęp do zasobów sieciowych w sposób bezpieczny i wydajny, niezależnie od lokalizacji użytkownika.*
   W związku z powyższym, umożliwienie zestawienia połączenia VPN przed zalogowaniem się użytkownika jest kluczowe dla zapewnienia ciągłości działania, optymalizacji działań użytkowników oraz przygotowania się na przyszłe potrzeby i wzrost liczby użytkowników.

6. **Zapis: Antyspam ma zapewnić możliwość kwarantanny e-mail. Czy wirtualne urządzenie do zarządzania kwarantanną e-mail, zainstalowane w Państwa infrastrukturze, mogłoby być dla Państwa akceptowalnym rozwiązaniem? Chcielibyśmy zapewnić elastyczność przy jednoczesnym zachowaniu wysokiego poziomu bezpieczeństwa.**

   Odp. *Zamawiający nie wyraża zgody na proponowane rozwiązanie, które zakładałoby zastosowanie wirtualnego urządzenia do zarządzania kwarantanną e-mail. Powodem takiej decyzji jest konieczność zapewnienia kompleksowej funkcjonalności antyspamu, która obejmuje także możliwość kwarantanny e-mail. Dodatkowo, wirtualizacja mogłaby wprowadzić dodatkowe problemy i koszty. Uzasadnienie dotyczące wirtualizacji znajduje się już w odpowiedzi do pytania 1.*

7. **Zapis: Kontroler musi mieć funkcję analizy mapy konfliktów w kanałach transmisyjnych. Czy krytyczne jest by dana funkcjonalność była zapewniona przez kontroler, czy te same wymagania mogą zostać zapewnione przez usługę? Czy Zamawiający zgodzi się na pomiar zrobiony przez wykonawcę i konfiguracje bez konieczności utrzymywania mapy live?.**

   Odp. *Zamawiający nie wyraża zgody na proponowaną zmianę, gdyż funkcjonalność analizy mapy konfliktów w kanałach transmisyjnych jest kluczowa dla utrzymania sieci. Ta funkcjonalność musi być zapewniona przez kontroler, ponieważ umożliwia dokładną diagnozę i zarządzanie ewentualnymi konfliktami w kanałach transmisyjnych w czasie rzeczywistym. Użycie usługi zamiast funkcji wbudowanej w kontroler może nie zapewnić takiej samej precyzji i dostępności w analizie i reakcji na konflikty.*
   Co do drugiej części pytania, Zamawiający nie zgodzi się na pomiar wykonany przez wykonawcę i konfiguracje bez utrzymywania mapy live. Utrzymanie aktualnej mapy konfliktów w kanałach transmisyjnych jest kluczowe dla zapewnienia ciągłości działania sieci oraz szybkiego reagowania na wszelkie problemy. Bez utrzymania mapy live, skuteczność i efektywność działań naprawczych mogą być znacznie ograniczone.

8. **Zapis: System ma posiadać możliwość stworzenia mapy sieci wewnętrznej zawierającej szczegółowe dane urządzenia (MAC, IP, System operacyjny, otwarte porty). Czy Zamawiający zgodzi się na zmianę zapisu na: "System ma posiadać możliwość stworzenia mapy sieci wewnętrznej zawierającej szczegółowe dane urządzenia (MAC, IP, System operacyjny, ilość przesyłanych danych)"**

Norway
grants

Odp. *Zamawiający nie wyraża zgody na zmianę zapisu, ponieważ informacja o otwartych portach w celu zapewnienia bezpieczeństwa sieci jest jedną z kluczowych dla jego wymagań. Monitorowanie otwartych portów pozwala na identyfikację potencjalnych luk w zabezpieczeniach sieciowych i umożliwia szybką reakcję na ewentualne zagrożenia. Wprowadzenie zmiany, która eliminuje tę informację, ograniczyłoby możliwość skutecznego monitorowania i utrzymania bezpieczeństwa sieci. Co więcej, choć informacja o ilości przesyłanych danych może być istotna, Zamawiający monitoruje ją w inny sposób, co sprawia, że nie jest ona równie krytyczna jak informacja o otwartych portach w kontekście zapewnienia bezpieczeństwa sieci.*

9. **Zapis: System zarządzania musi posiadać graficzną konsolę do zarządzania systemem VPN działającą w trybie drag-and-drop. Jedynie jeden producent spełnia ten zapis. Czy zamawiający może zmodyfikować zapis na: „System zarządzania musi posiadać graficzną konsolę do zarządzania systemem VPN działającą w trybie drag-and-drop lub wizard”?**

   Odp. *Tak, Zamawiający może przystać na propozycję pytającego i zmodyfikować zapis dotyczący trybu działania konsoli.*

10. **Zapis: W celu realizacji ochrony „Zero Day” zamawiający dopuszcza wykorzystanie dodatkowego urządzenia spełanijącego powyższe założenia. Czy zamawiający dopuści virtualny appliance instalowany w infrastrukturze w zamawiającego?**

    Odp. *Zamawiający nie wyraża zgody na wykorzystanie wirtualnego urządzenia (virtualny appliance) instalowanego w swojej infrastrukturze w celu realizacji ochrony "Zero Day". Powodem takiej decyzji jest obawa o potencjalne dodatkowe ryzyko związane z wirtualizacją w kontekście bezpieczeństwa sieciowego. Wirtualne urządzenia mogą wprowadzać dodatkowe potencjalne punkty ataku oraz komplikować proces zarządzania i monitorowania sieci. Ponadto, Zamawiający preferuje rozwiązania sprzętowe ze względu na ich dedykowaną wydajność i stabilność działania, zwłaszcza w obszarze ochrony przed zagrożeniami "Zero Day".*

BURMISTRZ
MIASTA JAROSŁAWIA

Waldemar Paluch