UNIWERSYTET ŚLĄSKI
ul. Bankowa 12,
40- 007 KATOWICE
NIP 634-019-71-34;
REGON 000001347

Katowice, dnia 03.06.2015 r.

UCZESTNICY POSTĘPOWANIA NR DZP.381.60.2015.DW

WYJAŚNIENIA DO TREŚCI SPECYFIKACJI ISTOTNYCH WARUNKÓW ZAMÓWIENIA (DOTYCZY CZĘŚCI „C")

Dotyczy: postępowania o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego nr **DZP.381.60.2015.DW** o wartości zamówienia równej lub przekraczającej kwotę 207.000 € pn. **„Dostawa urządzeń sieciowych aktywnych".**

Do Zamawiającego wpłynęły zapytania dotyczące ww. postępowania – **część „C"**.

Zgodnie z art. 38 ust. 1 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tekst jedn. Dz. U. z 2013r. poz. 907 z późn. zm.), zwanej dalej *„ustawą Pzp",* Zamawiający jest obowiązany udzielić wyjaśnień niezwłocznie, jednak nie później niż na 6 dni przed upływem terminu składania ofert. Zgodnie z ust. 2 przedmiotowego artykułu treść zapytań wraz z wyjaśnieniami Zamawiający przekazuje Wykonawcom, którym przekazał specyfikację istotnych warunków zamówienia, bez ujawniania źródła zapytania, a jeżeli specyfikacja jest udostępniana na stronie internetowej, zamieszcza na tej stronie. Wobec powyższego Zamawiający udziela następujących wyjaśnień:

Pytanie 1:

Pkt 3. Urządzenie powinno być wyposażone w redundantną macierz dysków typu RAID z możliwość wymiany dysków podczas pracy urządzenia (hot swap).

Czy Zamawiający dopuści rozwiązanie które nie będzie wyposażone w redundantną macierz dysków typu RAID z możliwością wymiany dysków podczas pracy urządzenia (hot swap) ?

Odpowiedź:

Nie. Bezpieczne przechowywanie wiadomości w miejscu niezależnym od infrastruktury wirtualizacyjnej i szybki do nich dostęp (czyli w urządzeniu) są dla Zamawiającego istotne.

Pytanie 2:

Pkt 19. Możliwość nadania użytkownikom uprawnień do zmiany własnych ustawień:

a. włączenie/wyłączenie kwarantanny,
b. włączenie/wyłączenie skanowania antyspamowego,
c. zmiany języka i częstotliwości wysyłanych powiadomień kwarantanny,
d. dodawania adresów do osobistej białej/czarnej listy,
e. zmiany ustawień osobistych klasyfikatora Bayesa,
f. zmiany punktacji wiadomości.

Czy Zamawiający dopuści rozwiązanie umożliwiające zarządzanie zawartością własnej kwarantanny? Pozostałe wymagania są właściwe dla trybu serwera, w przypadku wymaganego trybu gateway'a ingerowanie użytkownika w polityki bezpieczeństwa może okazać się mało skalowalne oraz zmniejszające stopień bezpieczeństwa.

Odpowiedź:
Nie. Dla Zamawiającego jest istotna funkcjonalność zarządzania przez użytkownika ze środowiska akademickiego osobistymi ustawieniami kwarantanny.

Pytanie 3:
Pkt 39. Produkt powinien rozróżniać co najmniej 11 różnych zestawów znaków, różnych narodowości używanych do kodowania wiadomości mailowych. Wiadomości zawierające takie znaki mogą być blokowane, przesłane do kwarantanny lub oznaczone jako spam.
Czy Zamawiający zaakceptuje rozwiązanie wyszukujące treści wyspecyfikowane z użyciem kodowania UTF-8 ?

Odpowiedź:
Tak. Zamawiający wymaga jednak rozpoznawania kodowania także w innych zestawach znaków niż UTF-8. Takie zestawy znaków są nadal stosowane w praktyce.

Pytanie 4:
Pkt 40. Możliwość konfiguracji ilości miejsca na dysku urządzenia przeznaczonego na kwarantannę każdego użytkownika. Niezależnie od tego ustawienia urządzenie nie powinno usuwać wiadomości młodszych niż 3 dni.
Czy dopuszczalne jest rozwiązanie, gdzie ograniczenia co do wielkości dysku obowiązują tylko dla globalnej kwarantanny systemowej, a wiadomości w personalnej kwarantannie są kasowane po określonej liczbie dni?

Odpowiedź:
Nie. Użytkownicy ze środowiska akademickiego charakteryzują się różnymi wymaganiami względem obsługi poczty i należy im stworzyć jak najdalej idące możliwości obsługi własnej korespondencji.

Pytanie 5:
Pkt 49. Urządzenie ma zapewniać skanowanie antywirusowe poczty przychodzącej za pomocą minimum 3 różnych silników antywirusowych działających jednocześnie.
Czy możliwe jest zastosowanie jednego silnika AV pochodzącego od producenta całego systemu ocenianego wysoko przez niezależne testy np. VB100?

Odpowiedź:
Nie. Z doświadczenia Zamawiającego wynika, że różne programy antywirusowe różnią się zakresem wykrywanego szkodliwego oprogramowania i rozwiązanie oparte na kilku programach antywirusowych jest bardziej efektywne, niż oparte na jednym silniku.

Pytanie 6:

Pkt 50. Weryfikacja odcisku wiadomości lub wirusa z bazą danych producenta, jeżeli informacje na temat tej wiadomości lub wirusa nie zostały odnalezione w lokalnej bazie na urządzeniu.

Czy dopuszczalna jest opcjonalna integracja z systemem sandbox w celu osiągnięcia tej funkcjonalności? Ochrona przed zaawansowanymi atakami wymusza zastosowanie technologii sandbox w celu oszacowania poziomu szkodliwości próbki, sprawdzenie jedynie odcisku wiadomości nie daje szansy uniknięcia wycelowanego ataku.

Odpowiedź:

Tak. Zamawiający dopuszcza opcjonalne funkcjonalności, których zadaniem jest zwiększenie wykrywalności niechcianego oprogramowania.

Pytanie 7:

Pkt 55. Interfejs administratora powinien być dostępny co najmniej w dwóch językach: polskim i angielskim.

Czy dopuszczalne jest rozwiązanie, gdzie język polski zastosowany jest tylko na użytek dostępu do webmaila?

Odpowiedź:

Nie. Z praktyki Zamawiającego wynika, że w środowisku akademickim pożądany i niezbędny jest co najmniej dwujęzyczny dostęp do całości oprogramowania systemu, tak dla administratora, jak i dla użytkownika.

Pytanie 8:

Pkt 62. Urządzenie powinno mieć możliwość przeprowadzenia diagnostyki poprzez interfejs graficzny przy użyciu narzędzi takich jak: ping, telnet, dig, tcpdump i traceroute.

Czy dopuszczalne jest zastosowanie nslookup zamiast dig.?

Odpowiedź:

Nie. Zdaniem Zamawiającego narzędzie dig jest prostsze w użytkowaniu i nasi administratorzy są wdrożeni do jego wykorzystania. Nie jest także jasne, jak długo jeszcze narzędzie nslookup będzie wspierane przez ISC (w ostatnich latach sytuacja w tej sprawie zmieniała się i nie ma pewności, czy znów się nie zmieni).

Pytanie 9:

Pkt 64. Urządzenie ma mieć możliwość tworzenia kopii zapasowej konfiguracji urządzenia, ustawień wszystkich lub wybranych użytkowników.

Czy z uwagi na fakt, że urządzenie ma pracować w trybie gateway'a, wystarczający jest backup całego systemu oraz wszystkich użytkowników?

Odpowiedź:

Nie. Ponieważ Zamawiający zamierza zróżnicować konfiguracje dla różnych użytkowników, możliwość archiwizacji konfiguracji wybranych użytkowników (po zmianie) jest istotna.

Pytanie 10:

Pkt 65. Kopie zapasowe mają być tworzone na żądanie lub eksportowane zgodnie z harmonogramem na zdefiniowany serwer ftp i smb.

Czy zdalny backup można wykonywać na serwer ftp lub sftp?

Odpowiedź:

Tak. Jednak pod warunkiem, że będzie także można wykorzystywać mechanizm SMB. Zamawiający wykorzystuje (i zamierza wykorzystywać) ten protokół w praktyce.

Pytanie 11:

Pkt 66. Możliwość określenia maksymalnej liczby plików kopii zapasowej przechowywanej na serwerze ftp i smb.

Czy powyższe wymaganie może być realizowane za pomocą skryptu po stronie serwera?

Odpowiedź:

Nie. Zamawiający zdaje sobie sprawę, że takie rozwiązanie mogłoby działać, jednak wymaga ono większego nakładu pracy ze strony administratorów, co nie jest pożądane.

Pytanie 12:

Pkt 67. Możliwość tworzenia kopii zapasowej baz danych filtrów Bayesa, dla całego systemu lub dla poszczególnych użytkowników.

Czy akceptowalne jest wykonywanie kopii filtrów Bayesa dla całego systemu bez rozróżnienia na użytkowników?

Odpowiedź:

Nie. Podobnie jak w pkt 19 i 40 dla Zamawiającego istotna jest możliwość zróżnicowania obsługi użytkowników pod względem administracji konfiguracją ich ustawień obsługi poczty.

POWYŻSZE WYJAŚNIENIA SĄ WIĄŻĄCE DLA WYKONAWCÓW I NALEŻY JE UWZGLĘDNIĆ PRZY SPORZĄDZANIU OFERTY.

Z-ca Przewodniczącego Komisji Przetargowej:

mgr inż. Artur Baran

Przewodniczący Komisji Przetargowej:

mgr Ewa Słowik