Sękocin Stary, 02-11-2022 r.

Zn. spr.: DZ.270.91.2021

Wykonawcy

Dotyczy: postępowania o udzielenie zamówienia publicznego pn.: „**Zakup i wdrożenie centralnego systemu ochrony dla urządzeń końcowych funkcjonujących w PGL LP”**

Wyjaśnienia treści SWZ

Zamawiający działając na podstawie art.135 ust. 2 ustawy z dnia 11 września 2019 roku Prawo Zamówień Publicznych (t.j. Dz. U z 2022 r., poz. 1710), zwanej dalej Pzp, w związku ze złożonymi wnioskami Wykonawców, przekazuje wyjaśnienia:

Pytanie nr 1:
Dotyczy Punkt 2.3 – Czy zamawiający może uszczegółowić dla jakich platform mobilnych system AV musi oferować pełne wsparcie?
Odpowiedź Zamawiającego:
Definicja urządzenia mobilnego została opisana w słowniku I.15.

Pytanie nr 2:
Dotyczy Punkt 4.4 - Czy zamawiający wymaga aby dostęp do konsoli zarządzającej z punktu widzenia bezpieczeństwa był realizowany na zasadzie 2FA? Podejście takie stanowczo podnosi poziom bezpieczeństwa na wypadek wycieku poświadczeń jednego z administratorów.
Odpowiedź Zamawiającego:
Zamawiający nie wymaga dostępu do konsoli przy pomocy rozwiązań 2FA.

Pytanie nr 3:
Dotyczy Punkt 4.10 – Czy Zamawiający może sprecyzować w oparciu o jakie filtry należy tworzyć statyczne i dynamiczne grupy urządzeń? W przypadku rozwiązań AV budowanych tylko w oparciu o sygnaturowy model grupy dynamiczne są potrzebne w celu izolacji stacji i wykonania aktualizacji sygnatur gdyż standardowe silniki nie są w tanie ochronić sieci przed nieznanymi zagrożeniami.
Odpowiedź Zamawiającego:
Tylko grupy dynamiczne będą tworzone na podstawie filtrów. Grupy dynamiczne tworzone są na podstawie atrybutów (filtrów) zdefiniowanych przez producenta oprogramowania np. urządzenia z systemem Windows 10.

Pytanie nr 4:
Dotyczy Punkt 5.5 - Czy zamawiający może sprecyzować o jakich mechanizmach rozmawiamy pod terminem heurystyki? Czy mechanizm ten powinien chronić stacje klienckie przed zagrożeniami typu 0day, exploit oraz ransomware?
Odpowiedź Zamawiającego:
Zamawiający pod terminem heurystyki rozumie mechanizmy stosowane w wykrywaniu szkodliwego oprogramowania (ang. malware) tj. heurystyka statyczna, dynamiczna, analiza behawioralna itp.
Mechanizm ten powinien chronić stacje klienckie przed zagrożeniami typu 0day, exploit oraz ransomware.

Pytanie nr 5:
Dotyczy Punkt 5.6 - Czy zamawiający może sprecyzować czy ochrona przed szkodliwym oprogramowaniem ma być realizowana w sieci zamawiającego? Niektórzy producenci zapewnia tylko ochronę sygnaturową a ochrona przed oprogramowaniem ransomware jest realizowana przez zewnętrzne mechanizmy sandbox co przy np. braku dostępu do internetu może narażać zamawiającego na zagrożenie. Czy zamawiający wymaga aby ewentualne mechanizmy sandbox były realizowane

wewnątrz sieci czy na serwerach producenta? Czy jeżeli mechanizmy sandboxing mają być realizowane na zewnętrznych serwerach producenta czy zamawiający wymaga aby zgodnie z RODO istniała możliwość określenia lokalizacji znajdującej się w ramach UE detonacji nieznanych zagrożeń?

Odpowiedź Zamawiającego:

Ochrona przed szkodliwym oprogramowaniem powinna być realizowana w ramach dostarczonego oprogramowania dla komputerów i serwerów z systemem Windows. Dlatego niedopuszczalnym jest rozwiązanie, które realizuje ochronę systemów bazując jedynie na sygnaturach a dodatkowe wymagania (np. 5.5, 5.6) realizuje jedynie w chmurze.

Niezależnie od tego, ochrona z użyciem technologii sandbox może stanowić dodatkową linię ochrony, jedynie w przypadku, gdy rozwiązanie:

- spełnienia wszystkie wymagania zgodności z obowiązującym prawem, w szczególności z RODO (w szczególności, w zakresie możliwości określenia lokalizacji znajdującej się w ramach UE detonacji nieznanych zagrożeń);
- będzie miało możliwość tworzenia przez administratorów polityk określających zasady przesyłania plików do chmury, definiowanych co najmniej w oparciu o rodzaj plików, użytkownika, chronione urządzenie;
- zostanie określony maksymalny czas wymagany do ocen przesłanego pliku;

Pytanie nr 6:

Dotyczy Punkt 5.18 - Czy zamawiający może doprecyzować iż na pewno chodzi o rozwiązanie IDS (Intrusion Detection System) i nie nastąpiła literówka? Rozwiązania klasy IPS (Intrusion Protection System) są odpowiedzialne za ochronę stacji przez zagrożeniami płynącymi z sieci.

Odpowiedź Zamawiającego:

Zamawiający wymaga rozwiązania pozwalającego na **aktywną** ochronę przed atakami sieciowymi. Akceptowalne są rozwiązania zarówno IDS jak i IPS spełniające powyższy warunek.

Pytanie nr 7:

Dotyczy Punkt 5.21 – Czy zmawiający może określić dla jakich aplikacji ma być realizowana ochrona przed atakami brute force? Od jakiego poziomu błędnie podanych loginów/haseł atak należy zaklasyfikować jako brute force?

Odpowiedź Zamawiającego:

Zamawiający przewiduję ochronę usług tj. RDP, SMB. Zamawiający nie definiuje poziomu błędnie podanych loginów/haseł.

Pytanie nr 8:

Dotyczy Punkt 5.24 – Czy zamawiający może określić w jaki sposób ma być realizowana funkcja ochrony przed skanowaniem portów? Czy przeskanowanie np. czy port 80 jest otwarty ma już być raportowane jako złośliwe działanie, czy alert ma się pojawić w chwili przeskanowania większej liczby portów. Czy skanowanie tyczy się tylko portów TCP, czy także UDP, oraz jaka jest minimalna wartość od jakiej alert ma zostać podniesiony?

Odpowiedź Zamawiającego:

Zamawiający nie definiuje sposobu w jaki ma być realizowana ochrona przed skanowaniem portów.

Pytanie nr 9:

Dotyczy Punkt 6.1 – Czy zmawiający wymaga aby na poziomie ochrona w czasie rzeczywistym były raportowane także próby wykonywania aktywnej exploitacji kernela chronionej stacji?

Odpowiedź Zamawiającego:

Zamawiający nie wymaga raportowania prób wykonania aktywnej eksploatacji kernela chronionej stacji.

Pytanie nr 10:

Dotyczy Punkt 7.1 – Czy zmawiający może uszczegółowić informację o systemach wykorzystywanych na urządzeniach mobilnych?

Odpowiedź Zamawiającego:

Definicja urządzenia mobilnego została opisana w słowniku I.15.

Pytanie nr 11:
Dotyczy Punkt 8.5 – Czy zamawiający wymaga żeby przeszukiwanie incydentów i zebranych danych z urządzeń chronionych pod kątem wektorów ataków była realizowana na wszystkich platformach wspomnianych w punkcie 2.3?
Odpowiedź Zamawiającego:
Zamawiający wymaga, żeby przeszukiwanie incydentów i zebranych danych z urządzeń chronionych pod kątem wektorów ataków była realizowana przynajmniej na urządzeniach klasy PC, serwerach fizycznych i wirtualnych (VMware, Hyper-v).

Pytanie nr 12:
Dotyczy Punkt 8.8 - Czy zamawiający wymaga, aby integracja z bazą MITRE raportowała podejrzane zdarzenia tak dla systemów Windows jak i Linux?
Odpowiedź Zamawiającego:
Zamawiający wymaga, aby integracja z bazą MITRE raportowała podejrzane zdarzenia zarówno dla systemów Windows jak i Linux.

Pytanie nr 13:
Dotyczy Punkt 1.2 – Czy zamawiający dopuszcza rozwiązanie, które w zamian pozwala na wykorzystanie klastra Windows Failover Cluster do zapewnienia wysokiej dostępności konsoli centralnego zarządzania? Rozwiązanie które proponujemy ma możliwość wykorzystywania jednego serwera centralnego zarządzania obsługującego do 250 tysięcy urządzeń i ich podział wewnątrz konsoli na odpowiednie grupy zarządzania a dodatkowo do zapewnienia wysokiej dostępności konsoli centralnego zarządzania wykorzystany zostanie klaster Windows Failover Cluster. Takie rozwiązanie daje możliwość centralizacji całego rozwiązania, możliwość tworzenia wielu użytkowników i przypisania im odpowiednich ról (np. zarządzanie oddziałem, generowanie raportów, dostęp tylko do odczytu). Takie rozwiązanie jest bardziej granularne i z punktu widzenia Zamawiającego jest ono bardziej efektywne dając o wiele więcej możliwości zarządzania całym środowiskiem np.:

- *Tworzenie nowych użytkowników,*
- *Nadawanie oraz kontrolowanie uprawnień dla użytkowników,*
- *Nadawanie uprawnień w sytuacjach kryzysowych,*
- *Audyt uprawnień,*
- *Audyt całego środowiska pod względem zagrożeń,*
- *Generowanie raportów z całego środowiska,*
- *Monitorowanie uprawnień,*
- *Badanie zgodności posiadanych przez użytkowników uprawnień pod kątem spełnienia polityk i zasad funkcjonujących w centrali i oddziałach.*

Windows Failover Cluster to grupa niezależnych serwerów fizycznych lub maszyn wirtualnych (węzły klastra), która zapewnia wysoką dostępność i skalowalność ról klastrowanych. Węzły klastra umożliwiają konfigurację oprogramowania i sprzętu, która umożliwia działanie usług na zachowanych węzłach w przypadku awarii jednego lub większej liczby węzłów klastra. Role klastra są również aktywnie monitorowane, aby zapewnić płynne działanie aplikacji. W razie potrzeby role są automatycznie lub pod kontrolą użytkownika przenoszone do lepiej działających węzłów. Klastry pracy awaryjnej udostępniają również funkcję CSV (Cluster Shared Volume), która zapewnia spójną, rozproszoną przestrzeń nazw, z której role klastra mogą korzystać w celu uzyskania dostępu do współdzielonego magazynu we wszystkich węzłach.
Odpowiedź Zamawiającego:
Zamawiający dopuszcza zaproponowane rozwiązanie pod warunkiem spełnienia warunków zawartych w punkcie 1.2 OPZ.

Pytanie nr 14:
Dotyczy Punkt 2.3 - Czy zamawiający dopuszcza rozwiązanie, które w zamian wspiera systemy operacyjne: Windows 7 i nowsze, Windows Server 2012 R2 i nowsze, Red Hat Enterprise Linux 7 i nowszy, Debian 10 i nowszy, Android 8 i nowsze oraz Apple IOS 10 i nowsze?
Odpowiedź Zamawiającego:
Zamawiający dopuszcza powyższe rozwiązanie.

Pytanie nr 15:
Dotyczy Punkt 2.4 - Czy zamawiający dopuszcza rozwiązanie, które w zamian pozwala na wdrażanie

urządzeń mobilnych za pomocą dedykowanej konsoli w trybie standardowym oraz w trybie właściciela urządzenia? W takim przypadku z jednej wdrożonej konsoli można zarządzać wszystkimi urządzeniami mobilnymi, serwerami oraz stacjami roboczymi.

Odpowiedź Zamawiającego:

Zamawiający podtrzymuje określone wymagania.

Pytanie nr 16:

Dotyczy Punkt 4.1 - Czy zamawiający dopuszcza rozwiązanie, które w zamian pozwala na wykorzystanie klastra Windows Failover Cluster do zapewnienia wysokiej dostępności konsoli centralnego zarządzania? Rozwiązanie które proponujemy ma możliwość wykorzystywania jednego serwera centralnego zarządzania obsługującego do 250 tysięcy urządzeń i ich podział wewnątrz konsoli na odpowiednie grupy zarządzania a dodatkowo do zapewnienia wysokiej dostępności konsoli centralnego zarządzania wykorzystany zostanie klaster Windows Failover Cluster. Takie rozwiązanie daje możliwość centralizacji całego rozwiązania, możliwość tworzenia wielu użytkowników i przypisania im odpowiednich ról (np. zarządzanie oddziałem, generowanie raportów, dostęp tylko do odczytu). Takie rozwiązanie jest bardziej granularne i z punktu widzenia Zamawiającego jest ono bardziej efektywne dając o wiele więcej możliwości zarządzania całym środowiskiem np.:

- *Tworzenie nowych użytkowników,*
- *Nadawanie oraz kontrolowanie uprawnień dla użytkowników,*
- *Nadawanie uprawnień w sytuacjach kryzysowych,*
- *Audyt uprawnień,*
- *Audyt całego środowiska pod względem zagrożeń,*
- *Generowanie raportów z całego środowiska,*
- *Monitorowanie uprawnień ,*
- *Badanie zgodności posiadanych przez użytkowników uprawnień pod kątem spełnienia polityk i zasad funkcjonujących w centrali i oddziałach.*

Windows Failover Cluster to grupa niezależnych serwerów fizycznych lub maszyn wirtualnych (węzły klastra), która zapewnia wysoką dostępność i skalowalność ról klastrowanych. Węzły klastra umożliwiają konfigurację oprogramowania i sprzętu, która umożliwia działanie usług na zachowanych węzłach w przypadku awarii jednego lub większej liczby węzłów klastra. Role klastra są również aktywnie monitorowane, aby zapewnić płynne działanie aplikacji. W razie potrzeby role są automatycznie lub pod kontrolą użytkownika przenoszone do lepiej działających węzłów. Klastry pracy awaryjnej udostępniają również funkcję CSV (Cluster Shared Volume), która zapewnia spójną, rozproszoną przestrzeń nazw, z której role klastra mogą korzystać w celu uzyskania dostępu do współdzielonego magazynu we wszystkich węzłach. (analogicznie jak w przypadku pytania do punktu 1.2)

Odpowiedź Zamawiającego:

Zamawiający dopuszcza zaproponowane rozwiązanie pod warunkiem spełnienia warunków zawartych w punkcie 4.1 OPZ.

Pytanie nr 17:

Dotyczy Punkt 7.16 - Czy zamawiający dopuszcza bezpieczniejsze rozwiązanie, które w zamian pozwala na wysyłanie poleceń blokowania, odblokowania urządzenia, przywracania ustawień fabrycznych i kasowania danych za pomocą konsoli zarządzającej? Wysyłanie poleceń przy użyciu wiadomości SMS jest metodą niebezpieczną, ze względu na możliwość nieautoryzowanego wykonania polecania przez atakującego przy użyciu techniki SMS Spoofing. Rozwiązanie polegające na wykonywaniu poleceń z poziomu dedykowanej konsoli zarządzającej jest pozbawione tego ryzyka.

Odpowiedź Zamawiającego:

Zamawiający dopuszcza proponowane rozwiązanie.

Pytanie nr 18:

Dotyczy Punkt 1.1 - Przy tego typu zamówieniach najczęściej to wykonawca zapewnia całość tj. sprzęt oraz oprogramowanie niezbędne do świadczenia usługi, wdraża usługę, instaluje, konfiguruje sprzęt i oprogramowanie oraz zapewnia prawidłowe świadczenie Usługi. W tym przypadku zamówienie zostało podzielone na części (hardware/software). W przypadku takiego wydzielenia, ryzyko utrudnień i komplikacji wynikających z synchronizacji świadczonej usługi i kompatybilności sprzętowej może przewyższyć korzyści i spowodować realny brak możliwości korzystania z usługi. W przypadku gdy Usługę będzie świadczył więcej niż jeden wykonawca może dojść do sytuacji, gdy usługa jako całość nie będzie funkcjonowała poprawnie, a żaden z Wykonawców nie będzie chciał wziąć odpowiedzialności za powstały błąd lub znalezienie przyczyny wystąpienia błędu i będzie to wymagało współpracy między kilkoma wykonawcami, co może znacząco przedłużyć czas usunięcia błędów. Również koordynacja prawidłowej realizacji usługi może spowodować ogromne trudności i zwiększyć ryzyko niepowodzenia.

Podzielenie zamówienia może zagrozić właściwemu wykonywaniu zamówienia oraz spowodować zwiększenie kosztów wykonywania tejże usługi. W związku z tym, że w tym przypadku Zamawiający udostępnia platformę sprzętową/wirtualną, zwracamy się do Zamawiającego z zapytaniem czy jest w stanie rozbudować infrastrukturę sprzętową do wymagań technicznych wdrażanego rozwiązania jeśli udostępnione zasoby okażą się niewystarczające? Czy wykonawca ma jednak dostarczyć /udostępnić wymagany sprzęt, aby usługa działała prawidłowo jeśli okaże się, że alokowane zasoby sprzętowe są niewystarczające?

Odpowiedź Zamawiającego:

Zamawiający udostępnia platformę sprzętową z zasobami określonymi w OPZ. Oferent powinien oszacować czy jest ona wystarczająca dla zaoferowanego rozwiązania. Jeżeli nie, w ramach pytań może wnioskować o zwiększenie przydzielonych zasobów o **konkretnie określoną wartość**, Zamawiający zweryfikuje czy posiada dostępne zasoby.

Pytanie nr 19:

Pytanie - Czy Zamawiający posiada bezpieczne, skalowalne zintegrowane rozwiązanie do zarządzania, wszystkimi swoimi urządzeniami takimi jak stacje robocze oraz serwery do wdrażania aplikacji, aktualizacji oprogramowania i systemów operacyjnych? np. Microsoft Endpoint Manager/ System Center Configuration Manager?

Odpowiedź Zamawiającego:

Zamawiający nie posiada powyższego rozwiązania.

Pytanie nr 20:

Pytanie - Prosimy o podanie ile urządzeń jest zarządzanych centralnie a ile niezarządzanych z konsoli która jest głównym punktem administracji i umożliwia zarządzanie wieloma lokacjami. Taka informacja pozwoli oszacować czas i koszt wdrożenia.

Odpowiedź Zamawiającego:

Zgodnie z przedmiotem zamówienia:

- etap nr 1 dotyczący 530 licencji będzie realizowany na urządzeniach tylko zarządzanych centralnie z konsoli,
- etap nr 2 instalacja licencji na pozostałych urządzeniach końcowych będzie realizowane przez Zamawiającego.

Pytanie nr 21:

Pytanie - Czy Zamawiający posiada jakieś licencje wieczyste lub subskrypcje do ochrony antywirusowej. Taka informacja pozwoli na oszacowanie ilości czasu potrzebnego na dezinstalację oprogramowania AV innych firm podczas wdrożenia systemu bezpieczeństwa. Prosimy o podanie:

- *Nazwy posiadanego oprogramowania antywirusowego,*
- *Ilości.*

Odpowiedź Zamawiającego:

Zamawiający samodzielnie przeprowadzi deinstalację obecnie posiadanego oprogramowania do ochrony antywirusowej.

Udzielone odpowiedzi obowiązują Wykonawców przy składaniu ofert i będą stanowić załącznik do Załącznika nr 1 do umowy.

Kierownik Zamawiającego:

Dariusz Gąsiorowski
Dyrektor Zakładu Informatyki Lasów Państwowych