WOJEWODA MAZOWIECKI

Warszawa, 31 sierpnia 2026 r.
Znak sprawy: BOU-V.272.55.2026
11033400.36880531.37871002

Dotyczy: postępowania o udzielenie zamówienia publicznego pn. Świadczenie usług w zakresie przeprowadzenia dwuobszarowego audytu Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).

WYJAŚNIENIA TREŚCI SWZ

Działając na podstawie art. 284 ust. 2 i 6 oraz art. 286 ust. 1 ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych, Zamawiający udziela wyjaśnień treści Specyfikacji Warunków Zamówienia (dalej SWZ).

Zamawiający przekazuje treść pytań otrzymanych w dniu 22.08.2026 r. oraz 25.08.2026 r. bez ujawniania ich źródła zapytania:

Pytanie nr 1

Prosimy o doprecyzowanie zakresu prac w obszarze inwentaryzacji środowiska IT. Czy Wykonawca ma przeprowadzić pełną inwentaryzację zasobów, czy zakres obejmuje wyłącznie audyt obecnie funkcjonującego procesu inwentaryzacji oraz ocenę kompletności, aktualności i sposobu prowadzenia istniejącej ewidencji aktywów?

Odpowiedź

Zamawiający wyjaśnia, że zakres zamówienia nie obejmuje wykonania przez Wykonawcę pełnej, niezależnej inwentaryzacji fizycznej wszystkich zasobów od podstaw.

Zgodnie z OPZ, w ramach obszaru „Inwentaryzacja i analiza środowiska IT", Wykonawca zobowiązany jest do przeprowadzenia czynności audytowych obejmujących w szczególności identyfikację i klasyfikację systemów, aplikacji, zasobów i usług IT, weryfikację kompletności i aktualności istniejącej ewidencji aktywów oraz ocenę zgodności udokumentowanego środowiska IT ze stanem faktycznym.

Punktem wyjścia do przeprowadzenia audytu będzie dokumentacja oraz ewidencja aktywów prowadzona przez Zamawiającego. Wykonawca powinien dokonać jej

Kontakt:
telefon: (+48) 22 695 60 61
adres e-mail: bou@mazowieckie.pl
strona www: www.gov.pl/web/uw-mazowiecki

Adresy do doręczeń:
plac Bankowy 3/5, 00-950 Warszawa
ePUAP: /t6j4ljd68r/skrytka
e-doręczenia: AE:PL-96129-72086-CJUVW-29

weryfikacji, a w przypadku stwierdzenia rozbieżności, braków lub aktywów nieuwzględnionych w istniejącej ewidencji — wskazać je w wynikach audytu wraz z odpowiednimi rekomendacjami.

Identyfikacja nowych aktywów odbywa się zatem w ramach prowadzonych czynności audytowych i służy ocenie kompletności oraz aktualności istniejącej ewidencji, nie stanowi natomiast odrębnego zadania polegającego na przeprowadzeniu pełnej inwentaryzacji wszystkich zasobów Zamawiającego.

Pytanie nr 2

Prosimy o podanie orientacyjnej liczby zasobów objętych audytem, w szczególności:

a) stacji roboczych,

b) serwerów fizycznych i wirtualnych,

c) urządzeń sieciowych,

d) systemów i aplikacji biznesowych,

e) pozostałych urządzeń i systemów IT.

Odpowiedź

Zamawiający informuje, że dla Mazowieckiego Urzędu Wojewódzkiego orientacyjna skala środowiska IT przedstawia się następująco:

- **stacje robocze – ok. 2400,**
- **serwery fizyczne – ok. 80,**
- **serwery wirtualne – ok. 400,**
- **urządzenia sieciowe – ok. 200,**
- **systemy i aplikacje biznesowe – ok. 130,**
- **pozostałe urządzenia i systemy IT – ok. 80.**

Powyższe wartości mają charakter orientacyjny i szacunkowy oraz służą określeniu przybliżonej skali środowiska objętego audytem. Nie stanowią zamkniętej ani zweryfikowanej inwentaryzacji zasobów.

Zakres podmiotowy audytu został określony w Załączniku nr 1 do OPZ i obejmuje Mazowiecki Urząd Wojewódzki oraz 13 Jednostek Administracji Zespolonej.

W odniesieniu do pozostałych 13 jednostek Zamawiający wskazuje, że są one istotnie mniejsze organizacyjnie i infrastrukturalnie od Mazowieckiego Urzędu Wojewódzkiego. Na podstawie obecnie dostępnych danych można przyjąć, że skala środowiska pojedynczej jednostki mieści się orientacyjnie w następujących przedziałach:

- **stacje robocze – w większości jednostek od ok. 20 do 100, natomiast w największych jednostkach do ok. 300–350 urządzeń,**
- **serwery fizyczne i wirtualne – co do zasady od pojedynczych serwerów do kilku serwerów w jednostce; w części jednostek środowiska serwerowe są bardziej rozbudowane,**

• urządzenia sieciowe – od kilku do ok. 30 urządzeń podstawowej infrastruktury sieciowej w jednostce, zależnie od jej wielkości i liczby lokalizacji,

• systemy i aplikacje biznesowe – najczęściej od kilku do ok. 10 systemów i aplikacji w jednostce,

• pozostałe urządzenia i systemy IT – od pojedynczych do kilku lub kilkunastu urządzeń i systemów, zależnie od organizacji i specyfiki danej jednostki.

Wskazane wartości mają charakter orientacyjny. Zamawiający nie dysponuje obecnie kompletną i zweryfikowaną inwentaryzacją wszystkich kategorii zasobów dla każdej z 13 jednostek.

Dla zobrazowania skali organizacyjnej Zamawiający wskazuje, że największa z pozostałych jednostek zatrudnia do ok. 300 osób, kolejna do ok. 170 osób, natomiast pozostałe jednostki co do zasady zatrudniają do ok. 100 osób.

Szczegółowe informacje dotyczące środowisk poszczególnych jednostek zostaną ustalone i zweryfikowane w toku realizacji audytu na podstawie dostępnej dokumentacji, informacji przekazanych przez daną jednostkę oraz przeprowadzonych czynności audytowych.

Jednocześnie Zamawiający wyjaśnia, że zgodnie z OPZ zadaniem Wykonawcy nie jest przeprowadzenie pełnej inwentaryzacji wszystkich zasobów od podstaw. Audyt powinien obejmować weryfikację istniejących ewidencji, dokumentacji i informacji oraz ocenę ich kompletności i zgodności ze stanem faktycznym.

Pytanie nr 3

Ile lokalizacji fizycznych oraz odrębnych środowisk IT obejmuje przedmiot zamówienia?

Odpowiedź

Zamawiający informuje, że przedmiot zamówienia obejmuje 21 lokalizacji fizycznych Mazowieckiego Urzędu Wojewódzkiego.

Zakres podmiotowy zamówienia obejmuje Mazowiecki Urząd Wojewódzki oraz 13 JAR wskazanych w Załączniku nr 1 do OPZ. Liczba podmiotów objętych audytem nie jest zatem równoznaczna z liczbą lokalizacji fizycznych, w których mogą być prowadzone czynności audytowe.

W odniesieniu do 13 JAR Zamawiający wskazuje, że większość jednostek funkcjonuje w jednej lokalizacji fizycznej, natomiast spośród pozostałych:

- **jedna jednostka funkcjonuje w 2 lokalizacjach,**
- **jedna jednostka funkcjonuje w 6 lokalizacjach,**
- **jedna jednostka funkcjonuje w 7 lokalizacjach.**

Powyższe dane mają charakter orientacyjny i służą określeniu skali realizacji audytu w poszczególnych podmiotach.

Zamawiający nie określa jednej zbiorczej liczby odrębnych środowisk IT rozumianych np. jako odrębne domeny, infrastruktury serwerowe, serwerownie lub wydzielone

środowiska sieciowe. Organizacja i stopień wydzielenia środowisk IT mogą różnić się pomiędzy poszczególnymi podmiotami i będą podlegały ustaleniu oraz weryfikacji w toku audytu na podstawie dostępnej dokumentacji, informacji przekazanych przez audytowane podmioty oraz przeprowadzonych czynności audytowych.

Pytanie nr 4

Czy zakres obejmuje również środowiska chmurowe i usługi SaaS, w szczególności Microsoft 365, Entra ID, Azure lub inne usługi chmurowe?

Odpowiedź

Zamawiający potwierdza, że w Mazowieckim Urzędzie Wojewódzkim, w środowisku objętym audytem, wykorzystywane są usługi chmurowe, w tym Microsoft 365. Również w części pozostałych jednostek objętych zamówieniem wykorzystywane są usługi chmurowe i usługi typu SaaS, w tym Microsoft 365. Zakres oraz sposób wykorzystania tych usług mogą różnić się pomiędzy poszczególnymi jednostkami. Zakres audytu obejmuje wykorzystywane przez Zamawiającego i jednostki usługi chmurowe oraz usługi typu SaaS, jeżeli są one wykorzystywane do przetwarzania informacji lub realizacji procesów objętych zakresem audytu. Dotyczy to odpowiednio Microsoft 365 oraz innych wykorzystywanych usług chmurowych, w zakresie pozostającym pod kontrolą danego podmiotu.

Zakres audytu nie obejmuje audytowania infrastruktury technicznej dostawcy usługi chmurowej, do której Zamawiający lub audytowana jednostka nie posiada dostępu ani uprawnień audytowych.

Pytanie nr 5

Czy Zamawiający posiada aktualną ewidencję aktywów oraz aktualną dokumentację architektury systemowej i sieciowej, która zostanie udostępniona Wykonawcy?

Odpowiedź

Zamawiający informuje, że nie posiada jednej kompletnej, aktualnej i scentralizowanej ewidencji aktywów ani kompletnej dokumentacji architektury systemowej i sieciowej obejmującej całe środowisko objęte audytem.

Zamawiający posiada natomiast częściową dokumentację oraz ewidencje, które mają charakter rozproszony, są prowadzone przez różne komórki organizacyjne lub osoby i mogą różnić się pod względem kompletności oraz aktualności.

Posiadana dokumentacja, ewidencje aktywów, diagramy, zestawienia oraz inne informacje dotyczące środowiska IT zostaną udostępnione Wykonawcy w zakresie, w jakim są dostępne i niezbędne do realizacji audytu.

Analogicznie, w odniesieniu do pozostałych jednostek objętych zamówieniem Wykonawcy zostanie udostępniona posiadana przez daną jednostkę dokumentacja i ewidencja, przy czym Zamawiający nie gwarantuje ich kompletności ani aktualności. Ocena kompletności, aktualności, spójności oraz zgodności dokumentacji ze stanem faktycznym stanowi element przedmiotu audytu określonego w OPZ.

Pytanie nr 6

Czy zadaniem Wykonawcy jest wyłącznie wskazanie rozbieżności pomiędzy dokumentacją a stanem faktycznym, czy również aktualizacja lub przygotowanie dokumentacji, ewidencji aktywów i diagramów środowiska?

Odpowiedź

Zamawiający wyjaśnia, że zadaniem Wykonawcy jest przeprowadzenie audytu, w tym ocena zgodności stanu faktycznego z obowiązującą dokumentacją, identyfikacja niezgodności, braków, luk oraz rozbieżności, a następnie przedstawienie odpowiednich ustaleń i rekomendacji działań naprawczych lub usprawniających. Zgodnie z OPZ zakres ten obejmuje w szczególności identyfikację brakujących, nieaktualnych lub niespójnych dokumentów, ocenę spójności środowiska technicznego z dokumentacją oraz opracowanie rekomendacji działań naprawczych i usprawniających.

Przedmiot zamówienia nie obejmuje natomiast obowiązku samodzielnego przygotowania, aktualizacji ani uzupełnienia przez Wykonawcę wewnętrznej dokumentacji Zamawiającego, dokumentacji architektury systemowej i sieciowej ani diagramów środowiska.

Rezultatem prac Wykonawcy mają być dokumenty i raporty określone w OPZ, zawierające wyniki audytu, zidentyfikowane niezgodności i braki oraz rekomendacje dotyczące sposobu ich usunięcia.

Pytanie nr 7

Czy systemy krytyczne zostały już przez Zamawiającego zidentyfikowane i sklasyfikowane, czy ich identyfikacja i klasyfikacja ma zostać wykonana w ramach audytu?

Odpowiedź

Zamawiający wyjaśnia, że identyfikacja systemów krytycznych oraz punktów styku z systemami zewnętrznymi stanowi element zakresu prac Wykonawcy określony w OPZ w ramach obszaru „Inwentaryzacja i analiza środowiska IT".

Wykonawca powinien w pierwszej kolejności wykorzystać posiadane przez Zamawiającego oraz jednostki objęte audytem informacje, dokumentację i istniejące klasyfikacje dotyczące systemów i ich znaczenia dla realizowanych procesów, a następnie dokonać ich weryfikacji w toku audytu.

W przypadku stwierdzenia, że istniejąca identyfikacja jest niepełna, nieaktualna lub niewystarczająca, Wykonawca powinien wskazać dodatkowe systemy wymagające zakwalifikowania jako krytyczne oraz odpowiednio przedstawić wyniki tej oceny w dokumentacji audytowej.
Wyniki identyfikacji i klasyfikacji systemów krytycznych powinny zostać uwzględnione przy planowaniu dalszych czynności audytowych, w szczególności przy określaniu zakresu i głębokości weryfikacji konfiguracji oraz zabezpieczeń poszczególnych systemów i urządzeń.

Pytanie nr 8
Czy weryfikacja konfiguracji i zabezpieczeń ma obejmować wszystkie systemy i urządzenia, czy dopuszczalne jest przeprowadzenie audytu na reprezentatywnej próbie?
Odpowiedź
Zamawiający wyjaśnia, że zakres audytu powinien obejmować całe środowisko IT w zakresie niezbędnym do jego oceny, natomiast szczegółowa weryfikacja konfiguracji i zabezpieczeń poszczególnych systemów oraz urządzeń może zostać przeprowadzona z wykorzystaniem odpowiednio dobranej próby.
Dla zasobów niezakwalifikowanych jako krytyczne Zamawiający określa następujący minimalny zakres szczegółowej weryfikacji w ramach każdej jednorodnej grupy zasobów:

- **grupa obejmująca od 1 do 10 zasobów – wszystkie zasoby,**
- **od 11 do 50 zasobów – co najmniej 5 zasobów,**
- **od 51 do 200 zasobów – co najmniej 10 zasobów,**
- **od 201 do 500 zasobów – co najmniej 20 zasobów,**
- **powyżej 500 zasobów – co najmniej 30 zasobów.**

Przez jednorodną grupę należy rozumieć zasoby o porównywalnym przeznaczeniu, technologii, sposobie zarządzania i konfiguracji.
Niezależnie od powyższych wartości próba powinna obejmować:

- **wszystkie systemy i zasoby zidentyfikowane jako krytyczne, jeżeli ich liczba i charakter uzasadniają indywidualną weryfikację,**
- **wszystkie istotne rodzaje wykorzystywanych technologii,**
- **istotnie odmienne warianty konfiguracji,**
- **zasoby o podwyższonym poziomie ryzyka,**
- **kluczowe elementy infrastruktury bezpieczeństwa.**

Jeżeli wyniki analizy ryzyka albo ustalenia dokonane podczas audytu wskazują, że minimalna próba nie jest wystarczająca do uzyskania wiarygodnej oceny, Wykonawca zobowiązany jest odpowiednio rozszerzyć zakres szczegółowej weryfikacji.
Sposób doboru próby powinien zostać przedstawiony przez Wykonawcę w metodyce audytu i uzgodniony z Zamawiającym.

Pytanie nr 9

Prosimy o wskazanie rodzajów i liczby systemów operacyjnych, serwerów, aplikacji oraz systemów biznesowych, które mają zostać objęte szczegółową analizą konfiguracji.

Odpowiedź

Zamawiający informuje, że środowisko IT Mazowieckiego Urzędu Wojewódzkiego obejmuje w szczególności następujące rodzaje systemów operacyjnych:

- **Windows 10 i Windows 11,**
- **Windows Server w wersjach od 2012 do 2025,**
- **Linux, w szczególności Debian i Ubuntu, w różnych wersjach,**
- **pojedyncze systemy Windows XP funkcjonujące w odizolowanych środowiskach,**
- **nieliczne urządzenia wykorzystujące system macOS.**

Orientacyjna skala środowiska Mazowieckiego Urzędu Wojewódzkiego, zgodnie z informacjami przekazanymi w odpowiedzi na wcześniejsze pytanie, obejmuje ok. 80 serwerów fizycznych, ok. 400 serwerów wirtualnych oraz ok. 130 systemów i aplikacji biznesowych.

Zamawiający wskazuje, że w pozostałych jednostkach objętych zamówieniem wykorzystywane są co do zasady zbliżone kategorie systemów operacyjnych, systemów serwerowych oraz aplikacji i systemów biznesowych. Poszczególne jednostki mogą jednak różnić się pod względem liczby wykorzystywanych rozwiązań, ich wersji, konfiguracji, funkcji oraz skali zastosowania. Szczegółowy stan środowiska poszczególnych jednostek będzie podlegał weryfikacji w toku audytu.

Zamawiający nie określa z góry zamkniętej liczby systemów, serwerów i aplikacji, które mają zostać poddane szczegółowej analizie konfiguracji. Ich dobór powinien zostać dokonany przez Wykonawcę w ramach przyjętej metodyki audytu, z uwzględnieniem analizy ryzyka, krytyczności systemów, rodzaju wykorzystywanej technologii, różnic konfiguracyjnych oraz znaczenia danego zasobu dla bezpieczeństwa informacji i realizowanych procesów.

Szczegółowa analiza konfiguracji może być prowadzona na odpowiednio dobranej próbie, zgodnie z minimalnymi zasadami doboru próby wskazanymi w odpowiedzi na pytanie nr 8.

Próba powinna być dobierana odrębnie dla istotnych grup technologicznych i konfiguracyjnych. W szczególności należy zapewnić, aby szczegółową analizą objęty został co najmniej jeden zasób reprezentujący każdy istotny wykorzystywany system operacyjny, jego istotnie odmienną wersję lub rolę systemową, jeżeli ma ona znaczenie dla poziomu bezpieczeństwa.

W przypadku serwerów dobór próby powinien dodatkowo uwzględniać ich role, w szczególności serwery realizujące usługi uwierzytelniania i katalogowe, plikowe, bazodanowe, aplikacyjne, infrastrukturalne oraz związane z bezpieczeństwem. Systemy i aplikacje zidentyfikowane jako krytyczne powinny zostać objęte szczegółową analizą niezależnie od minimalnej liczebności próby. W przypadku nielicznych lub unikalnych technologii, dla których liczba zasobów nie przekracza 10, szczegółowej weryfikacji powinny zostać poddane wszystkie takie zasoby.

Pytanie nr 10

Względem jakich standardów lub benchmarków ma być oceniany poziom hardeningu systemów, np. wewnętrznych standardów Zamawiającego, CIS Benchmarks, Microsoft Security Baselines lub zaleceń producentów?

Odpowiedź

Zamawiający wyjaśnia, że OPZ nie wskazuje jednego obligatoryjnego benchmarku technicznego, takiego jak CIS Benchmarks czy Microsoft Security Baselines, względem którego ma zostać przeprowadzona ocena poziomu hardeningu wszystkich systemów.

Podstawę oceny stanowią wymagania określone w OPZ, w szczególności wynikające z KRI, KSC oraz normy PN-EN ISO/IEC 27001:2023 – w odniesieniu do jednostek objętych audytem zgodności z tą normą – a także obowiązujące u Zamawiającego polityki, procedury, standardy bezpieczeństwa i zasady konfiguracji, jeżeli zostały określone dla danego rodzaju systemu lub urządzenia.

Szczegółową metodykę technicznej oceny poziomu hardeningu powinien zaproponować Wykonawca, z uwzględnieniem rodzaju, wersji, funkcji i krytyczności badanego systemu oraz właściwych dla niego dobrych praktyk bezpieczeństwa. W tym celu Wykonawca może posługiwać się w szczególności zaleceniami producentów, Microsoft Security Baselines, CIS Benchmarks lub innymi równoważnymi i uznanymi źródłami dobrych praktyk technicznych.

Analogicznie do przewidzianego w OPZ mechanizmu oceny dojrzałości SZBI, dla którego zastosowany ma zostać model zaproponowany przez Wykonawcę i zaakceptowany przez Zamawiającego, szczegółowa metodyka oraz przyjęte punkty odniesienia dla oceny poziomu hardeningu powinny zostać przedstawione przez Wykonawcę i uzgodnione z Zamawiającym w ramach przygotowania metodyki i organizacji prac audytowych.

Pytanie nr 11

Czy Zamawiający zapewni Wykonawcy dostęp typu read-only lub eksporty konfiguracji niezbędne do technicznej weryfikacji zabezpieczeń?

Odpowiedź

Zamawiający zapewni Wykonawcy, w zakresie niezbędnym do realizacji audytu oraz technicznie możliwym dla danego systemu lub urządzenia, dostęp do informacji i konfiguracji wymaganych do przeprowadzenia technicznej weryfikacji zabezpieczeń. W zależności od możliwości danego rozwiązania może to obejmować w szczególności dostęp z uprawnieniami ograniczonymi do odczytu, udostępnienie eksportów konfiguracji, raportów lub innych danych technicznych, a także prezentację wymaganych ustawień przez administratora danego systemu.
Sposób oraz termin udostępnienia dostępu lub danych zostaną uzgodnione w ramach organizacji i harmonogramu prac audytowych, z uwzględnieniem zasad bezpieczeństwa obowiązujących u Zamawiającego oraz w jednostkach objętych audytem.

Pytanie nr 12
Jakie rozwiązania do zarządzania aktualizacjami i podatnościami są obecnie wykorzystywane przez Zamawiającego?
Odpowiedź
Zamawiający informuje, że zarządzanie aktualizacjami nie jest obecnie realizowane za pomocą jednego, jednolitego centralnego rozwiązania obejmującego całe środowisko IT. Wykorzystywane są mechanizmy i narzędzia właściwe dla poszczególnych systemów, platform i środowisk.
W obszarze identyfikacji i monitorowania podatności Zamawiający jest obecnie w trakcie szerszego wdrażania rozwiązania klasy SIEM / monitorowania bezpieczeństwa, posiadającego również funkcjonalności związane z identyfikacją podatności w systemach objętych monitoringiem.
Wcześniej funkcjonowało pilotażowe wdrożenie tego rodzaju rozwiązania, obejmujące ograniczoną część środowiska, w szczególności wybrane serwery. Aktualnie zakres wdrożenia jest rozszerzany.
Zamawiający zaznacza, że rozwiązanie wykorzystywane do identyfikacji i monitorowania podatności nie jest samo w sobie centralnym systemem dystrybucji i instalowania aktualizacji.
Szczegółowa ocena funkcjonującego procesu zarządzania aktualizacjami i podatnościami, w tym stosowanych mechanizmów, zakresu ich wykorzystania, sposobu reagowania na wykryte podatności oraz skuteczności procesu, stanowi element audytu.

Pytanie nr 13
Czy Zamawiający posiada wyniki wcześniejszych skanów podatności oraz dokumentację dotyczącą procesu obsługi wykrytych podatności, które zostaną udostępnione Wykonawcy?

Odpowiedź

Zamawiający wyjaśnia, że OPZ przewiduje analizę wyników wcześniejszych skanów podatności wyłącznie w przypadku, gdy są one dostępne. Zapis „analiza wyników skanów podatności (jeśli dostępne)" oznacza, że Zamawiający nie gwarantuje posiadania kompletnych ani aktualnych wyników skanów dla wszystkich systemów i jednostek objętych audytem.

Jeżeli takie wyniki lub raporty są dostępne, zostaną udostępnione Wykonawcy w zakresie niezbędnym do realizacji audytu.

Analogicznie, posiadana dokumentacja dotycząca procesu identyfikacji, rejestrowania, oceny, priorytetyzacji oraz usuwania podatności zostanie udostępniona Wykonawcy, o ile istnieje i pozostaje w dyspozycji Zamawiającego lub jednostki objętej audytem.

Brak wcześniejszych wyników skanów lub kompletnej dokumentacji procesu nie zwalnia Wykonawcy z obowiązku oceny funkcjonowania procesu zarządzania podatnościami w zakresie określonym w OPZ.

Pytanie nr 14

Z jakiego okresu ma zostać przeprowadzona analiza procesu patch managementu i reakcji na wykryte podatności?

Odpowiedź

Zamawiający wyjaśnia, że analiza procesu zarządzania aktualizacjami (patch management) oraz reakcji na wykryte podatności powinna obejmować okres 12 miesięcy poprzedzających rozpoczęcie czynności audytowych w danej jednostce, a także ocenę aktualnego stanu funkcjonowania tego procesu na dzień przeprowadzania audytu.

Analiza powinna obejmować, w zakresie dostępnych danych i dokumentacji, w szczególności sposób identyfikacji i oceny podatności, podejmowania decyzji o wdrażaniu aktualizacji, terminowość ich instalowania, obsługę wyjątków i przypadków, w których aktualizacja nie mogła zostać wdrożona, oraz sposób dokumentowania i monitorowania podjętych działań.

W przypadku gdy dla części analizowanego okresu nie są dostępne kompletne dane lub dokumentacja, Wykonawca powinien przeprowadzić ocenę na podstawie dostępnych materiałów oraz wskazać stwierdzone braki w dokumentacji lub możliwości odtworzenia przebiegu procesu.

Pytanie nr 15

Jakie rozwiązania bezpieczeństwa i monitorowania są obecnie wykorzystywane, w szczególności SIEM, EDR/XDR, IDS/IPS, NDR oraz systemy centralnego logowania?

Odpowiedź

Zamawiający informuje, że wykorzystywane obecnie rozwiązania bezpieczeństwa i monitorowania należą w szczególności do następujących klas:

- **IDS/IPS,**
- **centralne gromadzenie i analiza logów,**
- **NAC (Network Access Control).**

Jednocześnie obecnie trwa wdrażanie rozwiązania klasy:

- **SIEM / centralnego monitorowania bezpieczeństwa.**

Rozwiązanie klasy SIEM jest zatem obecnie w trakcie wdrażania i rozszerzania zakresu jego wykorzystania, natomiast wskazane wyżej mechanizmy IDS/IPS, centralnego logowania oraz NAC są rozwiązaniami już funkcjonującymi w środowisku.
Zamawiający nie wskazuje obecnie odrębnych rozwiązań klasy NDR jako jednolicie wdrożonych w całym środowisku. Rozwiązania klasy EDR/XDR, jeżeli występują w poszczególnych obszarach lub jednostkach, również nie są wskazywane jako jednolite rozwiązanie obejmujące całe środowisko objęte zamówieniem.
Szczegółowa identyfikacja wykorzystywanych mechanizmów i narzędzi, ich konfiguracji, integracji, zakresu wdrożenia, pokrycia monitorowanego środowiska oraz skuteczności działania stanowi element czynności audytowych.

Pytanie nr 16

Czy zakres obejmuje techniczną analizę konfiguracji systemu SIEM, w tym reguł detekcyjnych, korelacji, alterowania i źródeł logów, czy wyłącznie ocenę organizacyjnego procesu monitorowania?

Odpowiedź

Zamawiający wyjaśnia, że zakres audytu obejmuje zarówno ocenę organizacyjnego procesu monitorowania bezpieczeństwa, jak i technicznych aspektów funkcjonowania wykorzystywanych systemów monitorowania i logowania.
Zgodnie z OPZ ocenie podlegają w szczególności systemy monitorowania, w tym SIEM i systemy logowania, zakres gromadzonych logów, ich retencja i integralność, zdolność wykrywania incydentów oraz procesy reagowania i eskalacji.
W przypadku gdy w czasie prowadzenia audytu system SIEM będzie funkcjonował w środowisku objętym audytem, Wykonawca powinien objąć oceną również jego konfigurację w zakresie niezbędnym do oceny skuteczności monitorowania bezpieczeństwa, w szczególności:

- **źródła i zakres pozyskiwanych logów,**
- **mechanizmy detekcji i korelacji zdarzeń,**
- **zasady generowania i obsługi alertów,**
- **retencję i integralność danych,**
- **pokrycie monitorowanego środowiska,**
- **powiązanie mechanizmów detekcji z procesem reagowania na incydenty.**

OPZ nie wymaga natomiast przeprowadzenia wyczerpującego, indywidualnego przeglądu każdej reguły detekcyjnej, korelacyjnej lub alertowej funkcjonującej w systemie SIEM. Szczegółowość analizy technicznej powinna być adekwatna do skali i sposobu wykorzystania systemu oraz umożliwiać ocenę jego skuteczności w zakresie określonym w OPZ.
W przypadku rozwiązania klasy SIEM, które obecnie znajduje się w trakcie wdrażania, zakres jego oceny będzie uzależniony od rzeczywistego stanu wdrożenia i wykorzystania systemu w momencie prowadzenia czynności audytowych.

Pytanie nr 17
Jakie typy i orientacyjna liczba źródeł logów są obecnie objęte centralnym monitorowaniem?
Odpowiedź
Zamawiający informuje, że w środowisku Mazowieckiego Urzędu Wojewódzkiego centralnym gromadzeniem i monitorowaniem logów objętych jest obecnie orientacyjnie około 200 źródeł.
Źródła te obejmują w szczególności:

- **część serwerów,**
- **większość przełączników sieciowych,**
- **część urządzeń UPS,**
- **większość urządzeń firewall.**

Powyższa liczba ma charakter orientacyjny i odzwierciedla aktualny stan środowiska. Zakres centralnego monitorowania może ulegać zmianom, m.in. w związku z prowadzonym wdrożeniem i rozwojem narzędzi monitorowania bezpieczeństwa.
W odniesieniu do pozostałych jednostek objętych zamówieniem zakres centralnego gromadzenia i monitorowania logów jest zróżnicowany i co do zasady istotnie mniejszy niż w Mazowieckim Urzędzie Wojewódzkim. W części jednostek centralne monitorowanie nie jest obecnie realizowane albo ma bardzo ograniczony zakres, obejmujący pojedyncze urządzenia lub systemy, np. urządzenia brzegowe, serwery lub systemy ochrony stacji roboczych.
W jednostkach posiadających bardziej rozbudowane mechanizmy monitorowania liczba źródeł obejmowanych centralnym zbieraniem logów wynosi od kilku do około 30 urządzeń infrastrukturalnych. W pojedynczych przypadkach dodatkowo centralnym monitoringiem bezpieczeństwa objętych może być do około 300 stacji roboczych za pośrednictwem rozwiązania klasy EDR.
W niektórych jednostkach zamiast ciągłego centralnego gromadzenia logów prowadzone są okresowe przeglądy lub analizy alertów generowanych przez wykorzystywane rozwiązania bezpieczeństwa. Zamawiający nie dysponuje obecnie jednolitym, zweryfikowanym zestawieniem liczby wszystkich źródeł logów dla każdej jednostki.

Zgodnie z OPZ jednym z elementów audytu technicznego jest weryfikacja zakresu, retencji i integralności logów. Do zadań Wykonawcy będzie zatem należała również ocena rzeczywistego zakresu źródeł objętych centralnym logowaniem i monitorowaniem, identyfikacja ewentualnych braków w pokryciu oraz ocena adekwatności monitorowania z punktu widzenia bezpieczeństwa środowiska.

Pytanie nr 18

Czy Zamawiający posiada formalne procedury reagowania na incydenty, eskalacji i raportowania oraz czy zostanie udostępniona dokumentacja przykładowych incydentów?

Odpowiedź

Zamawiający informuje, że w Mazowieckim Urzędzie Wojewódzkim procedura dotycząca zarządzania incydentami, obejmująca zasady reagowania, eskalacji i raportowania, jest obecnie w trakcie procedowania i nie stanowi jeszcze obowiązującej regulacji wewnętrznej.

Na potrzeby audytu Wykonawcy zostaną udostępnione posiadane dokumenty i materiały dotyczące reagowania na incydenty, w tym procedowane projekty regulacji, w zakresie niezbędnym do przeprowadzenia audytu.

W odniesieniu do pozostałych jednostek objętych zamówieniem zakres i stopień sformalizowania dokumentacji dotyczącej reagowania na incydenty mogą być zróżnicowane. Posiadane przez poszczególne jednostki procedury, instrukcje lub inne regulacje w tym zakresie zostaną udostępnione Wykonawcy, o ile są dostępne.

Wykonawcy zostanie również udostępniona, o ile jest dostępna, dokumentacja dotycząca przykładowych, rzeczywiście obsłużonych incydentów, w szczególności zgłoszenia, rejestry lub raporty, w zakresie niezbędnym do przeprowadzenia audytu oraz z uwzględnieniem wymagań dotyczących ochrony informacji, poufności i bezpieczeństwa.

W przypadku braku formalnie obowiązującej procedury, braku materiałów dotyczących incydentów lub ich niekompletności Wykonawca powinien uwzględnić ten fakt w ocenie dojrzałości i skuteczności procesu zarządzania incydentami.

Pytanie nr 19

Prosimy o wskazanie konkretnych wymagań KSC, względem których ma zostać przeprowadzona weryfikacja procesu raportowania incydentów.

Odpowiedź

Zamawiający wyjaśnia, że weryfikacja procesu raportowania incydentów powinna zostać przeprowadzona względem wymagań ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, w aktualnym brzmieniu, z uwzględnieniem zmian

wprowadzonych ustawą z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (Dz.U. z 2026 r. poz. 252).

Weryfikacja powinna obejmować wymagania właściwe dla statusu prawnego danej jednostki objętej audytem, w szczególności dotyczące:

- **identyfikowania i klasyfikowania incydentów, w tym kwalifikowania incydentów jako poważnych;**
- **terminowości i sposobu dokonywania wymaganych zgłoszeń;**
- **zakresu informacji przekazywanych w zgłoszeniach;**
- **przekazywania, odpowiednio do statusu podmiotu, wczesnych ostrzeżeń, zgłoszeń incydentów poważnych, sprawozdań okresowych, sprawozdań z postępu obsługi oraz sprawozdań końcowych;**
- **współpracy z właściwymi CSIRT oraz przekazywania wymaganych informacji;**
- **wykorzystywania właściwego systemu teleinformatycznego do realizacji obowiązków związanych ze zgłaszaniem incydentów;**
- **organizacji wewnętrznego procesu eskalacji i zapewnienia terminowego przekazywania informacji niezbędnych do realizacji obowiązków ustawowych.**

W szczególności należy uwzględnić wymagania wynikające z art. 11–12c ustawy o KSC, a w przypadku podmiotów publicznych również inne właściwe przepisy regulujące sposób realizacji tych obowiązków.

Szczegółowy zakres wymagań podlegających ocenie powinien zostać ustalony przez Wykonawcę z uwzględnieniem statusu danej jednostki w krajowym systemie cyberbezpieczeństwa oraz przepisów przejściowych określających terminy rozpoczęcia realizacji poszczególnych obowiązków.

Pytanie nr 20

Prosimy o podanie orientacyjnej liczby:

a) firewalli,

b) routerów,

c) przełączników,

d) kontrolerów Wi-Fi,

e) punktów dostępowych,

f) innych urządzeń sieciowych objętych audytem.

Odpowiedź

Zamawiający informuje, że orientacyjna liczba urządzeń sieciowych w środowisku Mazowieckiego Urzędu Wojewódzkiego przedstawia się obecnie następująco:

• firewalle – ok. 60,

• routery – Zamawiający praktycznie nie wykorzystuje odrębnych urządzeń pełniących wyłącznie funkcję routera; funkcje routingu realizowane są głównie przez inne elementy infrastruktury sieciowej,
• przełączniki sieciowe – ok. 140,
• kontrolery Wi-Fi – ok. 7, przy czym funkcjonalność kontrolera realizowana jest w wykorzystywanych urządzeniach firewall i nie są to odrębne urządzenia fizyczne,
• punkty dostępowe Wi-Fi – obecnie ok. 30.

Zamawiający planuje rozbudowę infrastruktury bezprzewodowej, w ramach której liczba punktów dostępowych może wzrosnąć. Część planowanych urządzeń przeznaczona jest również dla innych jednostek objętych zamówieniem. Rzeczywista liczba urządzeń funkcjonujących w środowisku w momencie realizacji audytu może zatem różnić się od wartości wskazanych powyżej.

W odniesieniu do pozostałych 13 jednostek objętych zamówieniem infrastruktura sieciowa jest istotnie mniejsza niż w Mazowieckim Urzędzie Wojewódzkim. Na podstawie obecnie dostępnych danych Zamawiający szacuje, że w jednostkach tych funkcjonuje łącznie co najmniej ok. 170 urządzeń infrastruktury sieciowej.

W poszczególnych jednostkach liczba urządzeń jest zróżnicowana i wynosi od kilku do kilkudziesięciu urządzeń. Dla części jednostek Zamawiający nie dysponuje obecnie kompletnymi i zweryfikowanymi danymi, dlatego wskazana wartość stanowi orientacyjny dolny poziom wynikający z dostępnych informacji, a rzeczywista łączna liczba urządzeń może być wyższa.

Struktura infrastruktury poszczególnych jednostek jest zróżnicowana i może obejmować w szczególności firewalle lub urządzenia wielofunkcyjne realizujące funkcje firewall/router, przełączniki sieciowe, kontrolery i punkty dostępowe Wi-Fi oraz inne elementy infrastruktury sieciowej. Szczegółowa liczba, rodzaj, funkcja i konfiguracja urządzeń zostaną zweryfikowane w toku audytu.

Powyższe dane mają charakter orientacyjny i służą określeniu skali środowiska. Nie stanowią zamkniętej ani zweryfikowanej inwentaryzacji infrastruktury sieciowej.

Zakres audytu obejmuje również inne urządzenia i komponenty infrastruktury sieciowej, jeżeli występują w środowisku i mają znaczenie dla bezpieczeństwa przetwarzania informacji. Ich identyfikacja oraz ocena stanowią element czynności prowadzonych przez Wykonawcę w ramach „Inwentaryzacji i analizy środowiska IT" oraz „Audytu infrastruktury sieciowej", zgodnie z OPZ.

Pytanie nr 21

Czy audyt konfiguracji urządzeń sieciowych ma obejmować wszystkie urządzenia, czy reprezentatywną próbę?

Odpowiedź

Zamawiający wyjaśnia, że audyt powinien obejmować całość infrastruktury sieciowej w zakresie niezbędnym do oceny jej bezpieczeństwa, natomiast szczegółowa weryfikacja konfiguracji poszczególnych urządzeń może zostać przeprowadzona na odpowiednio dobranej próbie.

Minimalna liczebność próby dla jednorodnej grupy urządzeń wynosi:

- **od 1 do 10 urządzeń – wszystkie urządzenia,**
- **od 11 do 50 urządzeń – co najmniej 5 urządzeń,**
- **od 51 do 200 urządzeń – co najmniej 10 urządzeń,**
- **od 201 do 500 urządzeń – co najmniej 20 urządzeń,**
- **powyżej 500 urządzeń – co najmniej 30 urządzeń.**

Dobór próby powinien być przeprowadzony odrębnie dla istotnych kategorii i grup urządzeń, z uwzględnieniem ich producenta, modelu, wersji oprogramowania, funkcji, lokalizacji oraz różnic konfiguracyjnych.

Niezależnie od minimalnej liczebności próba powinna obejmować wszystkie istotnie odmienne warianty konfiguracji oraz urządzenia o szczególnym znaczeniu dla bezpieczeństwa, w tym urządzenia brzegowe, urządzenia zabezpieczające dostęp do sieci zewnętrznych, elementy infrastruktury DMZ oraz inne urządzenia o podwyższonej krytyczności.

W przypadku wielu urządzeń o jednolitej konfiguracji, zarządzanych centralnie lub wykorzystujących wspólny szablon konfiguracyjny, Wykonawca może uwzględnić ten fakt przy doborze próby, pod warunkiem zweryfikowania również mechanizmu centralnego zarządzania i zgodności urządzeń z przyjętym wzorcem konfiguracji.

Jeżeli wyniki audytu wskazują na nieprawidłowości o charakterze systemowym, Wykonawca powinien odpowiednio rozszerzyć próbę.

Pytanie nr 22

Czy analiza firewalli ma obejmować szczegółową weryfikację wszystkich reguł firewall, ACL i NAT, czy ocenę architektury, polityk bezpieczeństwa i wybranej próby reguł?

Odpowiedź

Zamawiający wyjaśnia, że analiza firewalli powinna obejmować ocenę architektury zabezpieczeń, stosowanych polityk bezpieczeństwa, zasad kontroli dostępu oraz konfiguracji urządzeń, w tym reguł ACL i NAT.

W odniesieniu do firewalli objętych szczegółową weryfikacją zgodnie z zasadami wskazanymi w odpowiedzi na pytanie nr 21 Zamawiający nie wymaga każdorazowo ręcznej analizy wszystkich istniejących reguł, jeżeli ich liczba jest znaczna.

Szczegółowej analizie powinny jednak podlegać w 100% reguły o podwyższonym znaczeniu lub ryzyku, w szczególności:

- **dotyczące ruchu przychodzącego z sieci zewnętrznych,**
- **związane z publikacją usług i translacją NAT,**
- **umożliwiające dostęp administracyjny,**
- **zawierające szerokie lub nieograniczone zakresy źródeł, celów, portów lub usług,**
- **dotyczące systemów i segmentów krytycznych,**
- **reguły wyjątkowe, tymczasowe lub niestandardowe,**
- **reguły potencjalnie nadmiarowe, nieużywane, zdublowane lub niespójne z polityką bezpieczeństwa.**

Spośród pozostałych reguł Wykonawca powinien poddać szczegółowej analizie próbę obejmującą co najmniej 10% reguł, jednak nie mniej niż 20 reguł na analizowane urządzenie. Jeżeli urządzenie posiada nie więcej niż 50 reguł, szczegółowej analizie powinny zostać poddane wszystkie reguły.

W przypadku urządzeń posiadających bardzo dużą liczbę reguł dopuszcza się ograniczenie minimalnej próby pozostałych reguł do 100 reguł na urządzenie, pod warunkiem objęcia pełną analizą wszystkich reguł zakwalifikowanych jako reguły o podwyższonym znaczeniu lub ryzyku.

Jeżeli w analizowanej próbie zostaną stwierdzone istotne lub powtarzające się nieprawidłowości, Wykonawca powinien odpowiednio rozszerzyć zakres analizy, a w uzasadnionych przypadkach przeprowadzić analizę całego zestawu reguł danego urządzenia.

Pytanie nr 23

Ile podsieci, VLAN-ów i stref bezpieczeństwa funkcjonuje w środowisku objętym audytem?

Odpowiedź

Zamawiający informuje, że w środowisku Mazowieckiego Urzędu Wojewódzkiego funkcjonuje orientacyjnie:

- **ok. 180 VLAN-ów,**
- **ok. 200 podsieci,**
- **ok. 10 stref bezpieczeństwa.**

Powyższe wartości mają charakter orientacyjny i odzwierciedlają aktualny stan środowiska. W przypadku stref bezpieczeństwa ich liczba może różnić się w zależności od przyjętej definicji i sposobu klasyfikacji poszczególnych segmentów środowiska sieciowego.

W odniesieniu do pozostałych 13 jednostek objętych zamówieniem struktura segmentacji sieci jest istotnie mniej rozbudowana niż w Mazowiecki Urząd Wojewódzki. Na podstawie obecnie dostępnych danych w poszczególnych

jednostkach funkcjonuje najczęściej od ok. 2 do 10 podsieci, VLAN-ów lub innych logicznie wydzielonych segmentów sieci, natomiast w najbardziej rozbudowanych środowiskach liczba ta wynosi do ok. 15.
Łącznie, na podstawie dostępnych informacji, w jednostkach zidentyfikowano co najmniej ok. 45–50 podsieci, VLAN-ów lub innych wydzielonych segmentów sieciowych. Dla części jednostek Zamawiający nie dysponuje obecnie kompletnymi i zweryfikowanymi danymi, dlatego rzeczywista liczba może być wyższa.
Zakres stosowania formalnie wydzielonych stref bezpieczeństwa jest zróżnicowany. W części jednostek funkcjonują pojedyncze strefy bezpieczeństwa lub uproszczona segmentacja sieci, natomiast w innych podział realizowany jest przede wszystkim poprzez podsieci i VLAN-y. Szczegółowa liczba oraz sposób organizacji stref bezpieczeństwa zostaną zweryfikowane w toku audytu.

Pytanie nr 24
Czy Zamawiający udostępni aktualne diagramy LAN/WAN/Wi-Fi, informacje o segmentacji oraz konfiguracje urządzeń sieciowych?
Odpowiedź
Zamawiający informuje, że nie posiada kompletnego i aktualnego zestawu diagramów LAN/WAN/Wi-Fi oraz dokumentacji segmentacji obejmujących całe środowisko objęte audytem. Posiadana dokumentacja ma charakter częściowy i rozproszony, a jej aktualność i kompletność mogą być zróżnicowane.
Wykonawcy zostaną udostępnione posiadane przez Zamawiającego oraz jednostki objęte audytem diagramy, dokumentacja sieciowa i informacje dotyczące segmentacji, w zakresie, w jakim są one dostępne.
W zakresie konfiguracji urządzeń sieciowych Zamawiający umożliwi pozyskanie informacji niezbędnych do przeprowadzenia audytu. W zależności od możliwości technicznych danego rozwiązania może to nastąpić w szczególności poprzez udostępnienie eksportów konfiguracji, dostęp z uprawnieniami ograniczonymi do odczytu lub prezentację konfiguracji przez administratora danego systemu lub urządzenia.
Sposób oraz termin udostępnienia konfiguracji i pozostałych danych technicznych zostaną uzgodnione w ramach organizacji i harmonogramu prac audytowych.
Ocena kompletności i aktualności dokumentacji sieciowej oraz jej zgodności ze stanem faktycznym, jak również weryfikacja rzeczywistej topologii i segmentacji środowiska, stanowią element czynności audytowych określonych w OPZ.

Pytanie nr 25

Czy środowisko obejmuje systemy OT/ICS lub inne specjalistyczne urządzenia, które również mają zostać objęte audytem?

Odpowiedź

Zamawiający informuje, że środowisko objęte przedmiotem zamówienia nie obejmuje systemów OT/ICS ani innych specjalistycznych urządzeń przemysłowych tego typu. Zakres audytu obejmuje systemy teleinformatyczne, infrastrukturę sieciową oraz procesy i rozwiązania IT wykorzystywane do przetwarzania informacji, zgodnie z zakresem określonym w OPZ.

Pytanie nr 26

Prosimy o podanie orientacyjnej liczby adresów IP/hostów oraz zakresów sieci, które mają zostać objęte skanowaniem podatności.

Odpowiedź

Zamawiający informuje, że orientacyjna liczba wykorzystywanych adresów IP/hostów w środowisku Mazowieckiego Urzędu Wojewódzkiego wynosi około 3500.
Środowisko wykorzystuje wiele zakresów adresacji prywatnej, a ponadto około 250 publicznych adresów IP. Powyższe wartości mają charakter orientacyjny i służą określeniu przybliżonej skali środowiska objętego audytem.
W odniesieniu do pozostałych 13 jednostek objętych zamówieniem skala środowisk jest istotnie mniejsza niż w Mazowieckim Urzędzie Wojewódzkim. Na podstawie obecnie dostępnych danych w większości jednostek liczba wykorzystywanych hostów/adresów IP wynosi od kilkudziesięciu do ok. 250–300. W pojedynczych, bardziej rozbudowanych środowiskach liczba adresów wynikająca z wykorzystywanej przestrzeni adresowej może być większa i wynosić do ok. 1500, przy czym nie oznacza to, że wszystkie adresy są przypisane do aktywnych hostów.
Na podstawie obecnie dostępnych informacji można przyjąć, że łączna liczba hostów/adresów IP w pozostałych jednostkach wynosi orientacyjnie kilka tysięcy. Dla potrzeb oszacowania skali prac Zamawiający wskazuje wartość do ok. 4000 hostów/adresów IP dla 13 jednostek, z zastrzeżeniem, że dla części z nich dane nie są obecnie kompletne ani zweryfikowane.
Wskazane wartości mają charakter orientacyjny i szacunkowy. W przypadku części jednostek dostępne dane odnoszą się do liczby aktywnych hostów, natomiast w innych do wielkości wykorzystywanych segmentów lub przestrzeni adresowej. Rzeczywista liczba aktywnych zasobów podlegających skanowaniu może być zatem niższa od wskazanej maksymalnej skali adresacji.

Szczegółowy zakres zasobów przeznaczonych do skanowania zostanie ustalony dla każdej jednostki na etapie realizacji audytu, z uwzględnieniem rzeczywistego środowiska, ograniczeń technicznych oraz uzgodnionych wyłączeń.

Pytanie nr 27

Czy skanowanie ma obejmować:

a) infrastrukturę wewnętrzną,

b) infrastrukturę dostępną z Internetu,

c) oba powyższe obszary?

Odpowiedź

Zamawiający wyjaśnia, że skanowanie podatności powinno obejmować zarówno infrastrukturę wewnętrzną, jak i zasoby i usługi dostępne z Internetu, w zakresie, w jakim stanowią one element środowiska teleinformatycznego objętego audytem. Zakres skanowania powinien zostać dobrany w sposób umożliwiający identyfikację podatności, otwartych portów, usług oraz innych istotnych słabości technicznych zarówno z perspektywy sieci wewnętrznej, jak i zewnętrznej.

Szczegółowy zakres adresowy i lista zasobów przeznaczonych do skanowania zostaną uzgodnione z Wykonawcą na etapie realizacji audytu, z uwzględnieniem architektury środowiska, krytyczności zasobów, ograniczeń technicznych oraz zasad bezpieczeństwa obowiązujących u Zamawiającego i w jednostkach objętych audytem. W przypadku zasobów dostępnych publicznie skanowanie powinno być prowadzone wyłącznie w zakresie uzgodnionym i autoryzowanym przez Zamawiającego.

Pytanie nr 28

Czy wymagane są skany:

a) nieuwierzytelnione,

b) uwierzytelnione,

c) oba rodzaje skanów?

Odpowiedź

Zamawiający wyjaśnia, że w ramach audytu wymagane jest zastosowanie obu rodzajów skanowania: nieuwierzytelnionego oraz uwierzytelnionego, przy czym ich zakres powinien być dostosowany do rodzaju badanego zasobu, jego krytyczności, możliwości technicznych oraz celu wykonywanej weryfikacji.

Skanowanie nieuwierzytelnione powinno stanowić podstawowy sposób oceny ekspozycji zasobów i powinno obejmować zasoby znajdujące się w uzgodnionym zakresie skanowania, w szczególności:

- **zasoby i usługi dostępne z sieci zewnętrznych,**
- **zasoby dostępne w sieciach wewnętrznych,**
- **otwarte porty i udostępnione usługi,**

- **podatności możliwe do zidentyfikowania bez uzyskiwania dostępu do systemu.**

Skanowanie powinno być prowadzone z uwzględnieniem uzgodnionych z Zamawiającym wyłączeń dotyczących systemów, dla których aktywne skanowanie mogłoby powodować ryzyko zakłócenia ich działania.
Skanowanie uwierzytelnione powinno zostać przeprowadzone co najmniej dla:

- **systemów i zasobów zidentyfikowanych jako krytyczne, o ile ich charakter i możliwości techniczne pozwalają na bezpieczne wykonanie takiego skanowania,**
- **co najmniej jednego zasobu reprezentującego każdą istotną grupę technologiczną lub konfiguracyjną objętą audytem,**
- **systemów, dla których skan nieuwierzytelniony nie pozwala na wystarczająco wiarygodną ocenę m.in. stanu aktualizacji, wersji zainstalowanego oprogramowania lub występowania znanych podatności.**

Dobór zasobów do skanowania uwierzytelnionego powinien uwzględniać w szczególności rodzaj i wersję systemu operacyjnego, rolę systemu, jego krytyczność, poziom ryzyka oraz występujące różnice konfiguracyjne.
W przypadku stwierdzenia w badanej próbie istotnych lub powtarzających się podatności Wykonawca powinien odpowiednio rozszerzyć zakres skanowania uwierzytelnionego.
Szczegółowy zakres skanowania oraz sposób doboru zasobów powinny zostać przedstawione przez Wykonawcę w metodyce audytu i uzgodnione z Zamawiającym przed rozpoczęciem czynności technicznych.
Niezależnie od zastosowanego rodzaju skanowania wszystkie czynności powinny mieć charakter nieinwazyjny. Zakres zamówienia nie obejmuje testów penetracyjnych, prób eksploatacji wykrytych podatności ani innych działań mogących powodować niekontrolowane zakłócenia w funkcjonowaniu systemów.

Pytanie nr 29
Czy Zamawiający wskazuje konkretne wymagane narzędzie do skanowania podatności oraz czy Wykonawca ma zapewnić we własnym zakresie wymagane licencje?
Odpowiedź
Zamawiający wyjaśnia, że OPZ nie wskazuje jednego obligatoryjnego narzędzia do skanowania podatności. Wymienione w OPZ rozwiązania, takie jak Nmap, Nessus czy OpenVAS, mają charakter przykładowy i wskazują klasę narzędzi, które mogą zostać wykorzystane do realizacji czynności audytowych.
Dobór konkretnego narzędzia lub zestawu narzędzi należy do Wykonawcy, przy czym zastosowane rozwiązania powinny umożliwiać prawidłową realizację zakresu audytu określonego w OPZ oraz zapewniać odpowiednią jakość i wiarygodność uzyskiwanych wyników.

Wykonawca zobowiązany jest zapewnić we własnym zakresie wszystkie narzędzia, licencje, subskrypcje oraz inne uprawnienia niezbędne do realizacji skanowania podatności i pozostałych czynności audytowych objętych przedmiotem zamówienia. Zamawiający nie zapewnia Wykonawcy licencji na komercyjne narzędzia wykorzystywane do realizacji audytu.
Zastosowanie narzędzi open source jest dopuszczalne, o ile umożliwiają one realizację wymagań określonych w OPZ.

Pytanie nr 30
Czy w środowisku występują systemy krytyczne lub wrażliwe na aktywne skanowanie, dla których wymagane będą specjalne profile skanowania lub wyłączenia?
Odpowiedź
Zamawiający informuje, że w środowisku występują systemy i zasoby, dla których ze względu na ich charakter, krytyczność lub wrażliwość techniczną mogą być wymagane ograniczenia w zakresie aktywnego skanowania podatności.
W szczególności niewielka liczba zasobów dostępnych z sieci publicznej zostanie wyłączona z aktywnego skanowania. Szczegółowa lista takich zasobów zostanie przekazana Wykonawcy na etapie realizacji audytu, przed rozpoczęciem czynności technicznych.
Dla pozostałych systemów krytycznych lub wrażliwych Wykonawca powinien, w razie potrzeby, zastosować odpowiednio dostosowane, nieinwazyjne profile skanowania, uwzględniające charakter systemu, jego funkcję, wykorzystywaną technologię oraz ryzyko zakłócenia jego działania.
Identyfikacja systemów krytycznych stanowi element zakresu audytu określonego w OPZ. Wyniki tej identyfikacji powinny zostać uwzględnione przy planowaniu czynności technicznych.
Szczegółowy zakres skanowania, zastosowane profile, ograniczenia oraz wyłączenia powinny zostać uzgodnione z Zamawiającym przed rozpoczęciem skanowania.
Wykonawca nie może prowadzić aktywnego skanowania zasobów wskazanych przez Zamawiającego jako wyłączone z takich czynności.

Pytanie nr 31
Czy wymagane jest wyłącznie przeprowadzenie skanu podstawowego, czy również ponowne skanowanie po przeprowadzeniu działań naprawczych?
Odpowiedź
Zamawiający wyjaśnia, że zakres przedmiotu zamówienia obejmuje przeprowadzenie skanowania podatności, analizę uzyskanych wyników, identyfikację podatności i podatnych usług oraz ich odpowiednią klasyfikację i ujęcie w wynikach audytu.

Przedmiot zamówienia nie obejmuje obowiązkowego ponownego skanowania po wdrożeniu przez Zamawiającego lub jednostki objęte audytem działań naprawczych. Wykonawca powinien w ramach raportu wskazać stwierdzone podatności, ich istotność oraz rekomendowane działania naprawcze. Ewentualna późniejsza weryfikacja skuteczności wdrożonych działań naprawczych, w tym ponowne skanowanie, nie stanowi elementu niniejszego zamówienia.

Pytanie nr 32

Czy identyfikacja podatności mogą być realizowane z jednej lokalizacji dla wszystkich podmiotów?

Odpowiedź

Zamawiający wyjaśnia, że identyfikacja podatności nie może być realizowana wyłącznie z jednej lokalizacji wspólnej dla wszystkich podmiotów objętych zamówieniem.

Czynności w tym zakresie powinny być prowadzone odrębnie dla każdej jednostki, z uwzględnieniem jej własnej infrastruktury, adresacji, segmentacji, konfiguracji zabezpieczeń oraz lokalnych uwarunkowań technicznych i organizacyjnych.

Sposób technicznej realizacji skanowania w ramach danej jednostki może zostać zaproponowany przez Wykonawcę, przy czym musi on umożliwiać wiarygodną ocenę podatności środowiska tej jednostki i zostać uzgodniony z Zamawiającym.

Udzielone wyjaśnienia mają moc wiążącą oraz stanowią integralną część dokumentacji zamówienia.

Termin składania i otwarcia ofert pozostaje bez zmian

z upoważnienia Wojewody Mazowieckiego
Kamila Kowalikowska-Stefens
Dyrektor Biura Obsługi Urzędu
/podpisano kwalifikowanym
podpisem elektronicznym/

Administratorem danych osobowych jest Wojewoda Mazowiecki. Przetwarzamy Państwa dane osobowe wyłącznie w celu wykonania zadań Administratora, które wynikają z przepisów prawa oraz zadań realizowanych w interesie publicznym. Więcej informacji znajdą Państwo na stronie https://www.gov.pl/web/uw-mazowiecki/Przetwarzanie-danych-osobowych, w zakładce „O urzędzie” – „Przetwarzanie Danych Osobowych”.