Załącznik nr 3 do Zapytania Ofertowego nr 16/2023

Szczegółowy opis przedmiotu zamówienia
przeprowadzenie audytu bezpieczeństwa systemu informatycznego

Spis treści

1. Ogólny opis przedmiotu zamówienia

Usługa obejmuje przeprowadzenie kompleksowego audytu bezpieczeństwa systemów informatycznych Prototypu opartego o hybrydową infrastrukturę cloudową.

1.1. Opis infrastruktury Prototypu

Działanie prototypu oparte jest o następujące zasoby, które będą podlegały sprawdzeniu:

a. zasoby chmurowe (private cloud w Data Center) - zarządzane w modelu IaaS,
b. zasoby chmurowe w środowisku AZURE w tym web serwisy obsługujące algorytmy oparte m.in. o technologię AI i ML - zarządzane w modelu On Premises,
c. aplikacja webowa.

1.2. Cele audytu

Celem głównym audytu jest weryfikacja bezpieczeństwa systemów informatycznych oraz zaproponowanie rozwiązań pozwalających na poprawę bezpieczeństwa w zakresie Cyber Security.

Cele szczegółowe objęte zakresem zamówienia:

1. wysokopoziomowa ocena architektury bezpieczeństwa;
2. weryfikacja zabezpieczeń systemów IT i określenie szczegółowych podatności:
    a. infrastruktury sieci lokalnej w siedzibie Zamawiającego (w Międzychodzie),
    b. środowiska serwerowego (private cloud) i sieci domenowej oraz środowiska Azure (public cloud),
    c. aplikacji webowej z interfejsem użytkownika (do poziomu zalogowanego użytkownika, bez analizy kodu),
3. ocena ryzyka dla bezpieczeństwa informacji oraz ciągłości działania,
4. określenie rekomendacji w celu mitygowania ryzyka w tym propozycja rozwiązań, które pozwolą wyeliminować lub ograniczyć prawdopodobieństwo wykorzystania wykazanych w audycie podatności.

Z wyłączeniem zakresu, o którym mowa w pkt 2, lit. a) realizacja przedmiotu zamówienia może odbywać się zdalnie.

2. Wysokopoziomowa ocena architektury bezpieczeństwa

Wykonawca musi ocenić system zarządzania cyberbezpieczeństwem w zakresie dotyczącym audytowanego Prototypu. W zakres czynności sprawdzających wchodzi weryfikacja następujących obszarów:

a) Ogólna metoda zarządzania cyberbezpieczeństwem: Analiza SWAT modelu zarządzania systemami IT w zakresie bezpieczeństwa informacji oraz ciągłości działania systemów, w tym sposób dysponowania zasobami, podział odpowiedzialności, zastępowalność, redundancja, zaangażowanie i wsparcie kierownictwa.
b) Organizacja i struktura: Ocena struktury organizacyjnej, funkcji i odpowiedzialności związanych z zarządzaniem cyberbezpieczeństwem, w celu sprawdzenia, czy są wyraźnie określone i efektywne.
c) Zarządzanie ryzykiem: Przegląd procesów zarządzania ryzykiem związanym z cyberbezpieczeństwem, w tym identyfikacji, oceny, monitorowania i redukcji ryzyka.
d) Kontrola dostępu: Przegląd mechanizmów uwierzytelniania, autoryzacji i zarządzania tożsamościami, weryfikacja czy dostęp do zasobów jest odpowiednio ograniczony i monitorowany.
e) Monitorowanie: Ocena procesów monitorowania bezpieczeństwa, w tym weryfikacja, czy narzędzia i systemy monitorowania są właściwie skonfigurowane.
f) Procesy obrony i reagowania na cyber-zagrożenia: Ocena zdolności do reakcji na zmaterializowane zagrożenia w tym ocena stosowanych narzędzi i procedur, a także zdolności organizacji do przewidywania i przygotowania się na ewentualne przyszłe zmaterializowane zagrożenia.

3. Weryfikacja zabezpieczeń systemów IT i określenie szczegółowych podatności

3.1. infrastruktura sieci lokalnej w siedzibie Zamawiającego (w Międzychodzie)

Wykonawca musi ocenić ogólne bezpieczeństwo sieci oraz dokonać analizy podatności na cyberzagrożenia. Zakres analizy obejmuje do 150 prywatnych adresów IP wewnątrz sieci (głównie stacje robocze, a także urządzenia infrastruktury sieciowej, urządzenia sieciowe peryferyjne - drukarki) oraz dwa publiczne adresy IP.

W szczegółowy zakres oceny wchodzą poniższe czynności.

a. analiza architektury sieciowej:

a) weryfikacja sieci LAN na strefy sieciowe (w tym wykorzystanie urządzeń typu firewall oraz VLAN),
b) określenie usług działających w wybranych podsieciach,

c) poszukiwanie podatności w wybranych podsieciach (do 15 podsieci),
d) weryfikacja mechanizmów ochronnych w warstwie 2 i 3 modelu OSI w tym mechanizmów ochronnych przeciwko atakom ARP spoofing oraz nieautoryzowanego dostępu do sieci, a także weryfikacja zabezpieczeń routingu przed atakami man-in-the-middle,
e) ocena zdolności sieci do zapewnienia ciągłości działania.
f) analiza poprawności konfiguracji infrastruktury sprzętowo-sieciowej pod kątem bezpieczeństwa na podstawie udostępnionych przez Zamawiającego informacji oraz udzielonego dostępu nadzorowanego przez Zamawiającego.

b. analiza brzegu sieci:

a) badanie topologii/architektury sieci,
b) testy szczelności systemów klasy firewall,
c) ogólna analiza komunikacji sieciowej z poziomu sieci Internet,
d) skanowanie portów różnymi technikami, w celu wykrycia potencjalnych luk bezpieczeństwa w udostępnianych usługach,
e) wykrywanie usług sieciowych udostępnionych w sieci Internet,
f) próba detekcji wersji oraz typu oprogramowania systemowego zainstalowanego na urządzeniach dostępnych z sieci Internet,
g) testowanie co najmniej 2 metodami odporności usług wystawionych do sieci Internet na ataki „Denial of Service”,
h) testowanie odporności usług wystawionych do sieci Internet, za pomocą narzędzi wykrywających typowe luki bezpieczeństwa.

3.2. środowisko serwerowe (private cloud) i sieć domenowa oraz środowisko Azure (public cloud)

Wykonawca musi ocenić ogólne bezpieczeństwo środowiska serwerowego oraz dokonać analizy podatności na cyber-zagrożenia. Audytem zostanie objęte nie więcej niż 20 serwerów wirtualnych wykorzystujących systemy operacyjne Windows Server 2016-2022, 3CX, Docker Linux.

W szczegółowy zakres oceny wchodzą poniższe czynności.

a) weryfikacja udostępnionych usług sieciowych,
b) weryfikacja zbędnych usług wraz ze wskazaniem ich podatności,
c) weryfikacja zaimplementowanych systemów aktualizacji,
d) weryfikacja zaimplementowanych systemów kopii zapasowych
e) weryfikacja zaimplementowanych systemów logowania zdarzeń,
f) weryfikacja mechanizmów administracji zdalnej,
g) weryfikacja przypisania użytkowników do właściwych grup,
h) weryfikacja uprawnień zgodnie z pryncypium jak najmniejszych uprawnień (ang. „least privilige”),
i) przeprowadzenie próby obejścia uprawnień i uzyskania nieautoryzowanego dostępu do danych chronionych przetwarzanych przez serwery,
j) identyfikacja ewentualnych słabych punktów w konfiguracji usług wykorzystywanych na platformie Azure, z wyłączeniem usługi Entra ID,

k) weryfikacja bezpieczeństwa endpointów API integratorów danych funkcjonujących w ramach usług platformy Azure.

Wykaz usług wykorzystywanych w ramach platformy Azure oraz lista usług wykorzystywanych w ramach środowiska serwerowego, stanowią tajemnicę przedsiębiorstwa i zostaną przekazane oferentowi, którego oferta zostanie uznana za najkorzystniejszą, na etapie podpisywania Umowy, po uprzednim zabezpieczeniu poufności przekazywanych danych lub w trakcie trwania postępowania, wyłącznie na wyraźną prośbę oferenta. W ocenie Zamawiającego tak szczegółowe dane nie są niezbędne dla przygotowania oferty.*

- Na potrzeby weryfikacji zgodności konfiguracji usług MS Azure wykonawcy zostanie udostępnione konto z rolą Reader na wszystkich zasobach, które podlegają weryfikacji.
- Audyt musi być przeprowadzony z wykorzystaniem narzędzi i metod, umożliwiających ocenę konfiguracji i identyfikację problemów bez konieczności bezpośredniego dostępu do systemu operacyjnego na poziomie administratora umożliwiającym zmiany (zarezerwowane dla tego poziomu). Zamawiający umożliwi przegląd ustawień konfiguracyjnych wyłącznie w ramach wywiadu z działem IT oraz dostępu nadzorowanego.

3.3. detekcja błędów aplikacyjnych – testy penetracyjne i symulowane ataki

Wykonawca musi przeprowadzić testy w celu wykrycia błędów bezpieczeństwa i podatności na ataki. Wykonawca musi wykorzystać zarówno manualne i automatyczne metody prowadzenia audytu.

Próba ataku w ramach pentestu musi polegać na symulacji kontrolowanego ataku na punkty końcowe Prototypu, której celem jest identyfikacja potencjalnych podatności oraz ocena odporności systemu na rzeczywiste zagrożenia.

Testy penetracyjne muszą być wykonane w dwóch etapach.

Etap 1 – testy w modelu black-box. Wykonawca musi wykonać testy penetracyjne symulujące atak zewnętrzny, bez wykorzystania wiedzy na temat kodu źródłowego oraz infrastruktury Zamawiającego.

Etap 2 – testy z dostępem do systemu przy użyciu danych logowania.

W ramach etapu 1 Wykonawca musi przeprowadzić łącznie co najmniej 1000 kontrolowanych i zróżnicowanych prób wykorzystania potencjalnych podatności w celu sprawdzenia, czy system jest bezpieczny i czy reaguje w odpowiedni sposób na próby ataków. Ataki muszą być ukierunkowane na osiągnięcie poniższych celów:

a) wykradzenie danych z chronionej bazy danych,
b) instalacja złośliwego oprogramowania,
c) modyfikacja algorytmów, w tym algorytm utworzonych przy pomocy technologii AI,
d) pozyskanie informacji na temat krytycznych luk.

- Testy penetracyjne będą odbywać się w środowisku produkcyjnym Zamawiającego z uruchomioną usługą Azure Web Application Firewall.

Kluczowe cechy aplikacji stanowią tajemnicę przedsiębiorstwa i zostaną przekazane oferentowi, którego oferta zostanie uznana za najkorzystniejszą, na etapie podpisywania Umowy, po uprzednim zabezpieczeniu poufności przekazywanych danych lub w trakcie trwania postępowania, wyłącznie na wyraźną prośbę oferenta. W ocenie Zamawiającego tak szczegółowe dane nie są niezbędne dla przygotowania oferty.*

- Zamawiający nie przewiduje udostępnienia kodu źródłowego aplikacji.

W ramach etapu 2 Wykonawca musi przeprowadzić poniższe testy i sprawdzenia w celu wykrycia podatności i błędów aplikacyjnych:

a. SQL injection – „błędy wstrzyknięcia"

Wykonawca musi zweryfikować czy Prototyp jest podatny na ataki typu SQL injection, które mogą pozwolić nieautoryzowanemu użytkownikowi na wykonywanie zapytań SQL w bazie danych, manipulowanie danymi lub uzyskanie dostępu do wrażliwych informacji.

W ramach weryfikacji Wykonawca musi zrealizować czynności co najmniej takie jak:

- mapowanie aplikacji: Przeprowadzenie analizy aplikacji, identyfikując funkcje i obszary, które korzystają z baz danych i są narażone na potencjalne ataki SQL injection, takie jak pola formularzy, parametry URL, czy wartości cookies.

- testowanie na różnych wejściach: testowanie aplikacji, podając różne dane wejściowe, zawierające potencjalnie złośliwe zapytania SQL, aby sprawdzić, czy aplikacja reaguje w odpowiedni sposób na te dane.

- analiza odpowiedzi aplikacji: Analiza odpowiedzi aplikacji na wprowadzone zapytania SQL, sprawdzenie, czy odpowiedzi te wskazują na obecność podatności na SQL injection, takie jak błędy wynikające z nieprawidłowych zapytań SQL czy wyświetlanie chronionych lub niewłaściwych danych.

b. XSS (Cross-Site Scripting)

Weryfikacja podatności na atak typu XSS (Cross-Site Scripting). Wykonawca musi sprawdzić, czy aplikacja webowa jest narażona na ataki XSS, które pozwalają atakującemu na wstrzyknięcie(osadzenie) i wykonanie złośliwego kodu JavaScript (lub innego skryptowego języka) w przeglądarce ofiary oraz obejście mechanizmów kontroli dostępu do danych użytkownika.

W ramach weryfikacji Wykonawca musi zrealizować czynności co najmniej takie jak:

- mapowanie aplikacji: Wykonawca musi przeprowadzić analizę aplikacji, identyfikując funkcje i obszary, które mogą być narażone na potencjalne ataki XSS, takie jak pola formularzy, parametry URL, czy wartości cookies.

- testowanie na różnych wejściach: Wykonawca musi poddać testom aplikację, podając różne dane wejściowe, zawierające potencjalnie złośliwe skrypty, aby sprawdzić, czy aplikacja reaguje w odpowiedni sposób na te dane.

- analiza odpowiedzi aplikacji: Wykonawca musi przeanalizować odpowiedzi aplikacji na wprowadzone złośliwe skrypty, sprawdzając, czy odpowiedzi te wskazują na obecność podatności na XSS, takie jak wykonywanie nieoczekiwanego kodu skryptowego czy wyświetlanie chronionych danych.

c. CSRF (Cross-Site Request Forgery)

W ramach weryfikacji Wykonawca musi zrealizować czynności co najmniej takie jak:

- mapowanie aplikacji: Wykonawca musi przeprowadzić analizę aplikacji, identyfikując funkcje i obszary, które mogą być narażone na potencjalne ataki CSRF, takie jak formularze, operacje modyfikujące dane, czy akcje wymagające autoryzacji.

- analiza mechanizmów zabezpieczających: Wykonawca musi sprawdzić, czy aplikacja implementuje mechanizmy zabezpieczające przed atakami CSRF, takie jak tokeny anty-CSRF, techniki "same-origin" czy "double-submit" cookies. Weryfikacja czy jest możliwy scenariusz przeprowadzenia ataku.

- symulacja ataków CSRF: wWykonawca musi przeprowadzić testy, próbując wymusić na aplikacji wykonanie nieautoryzowanych działań za pomocą technik CSRF, aby sprawdzić, czy zabezpieczenia są skuteczne.

d. Code Execution

Wykonawca musi zweryfikować, czy aplikacja lub system jest podatny na ataki, które pozwalają atakującemu na zdalne wykonanie nieautoryzowanego kodu.

W ramach weryfikacji Wykonawca musi zrealizować czynności co najmniej takie jak:

- analiza aplikacji: Identyfikacja obszarów w aplikacji, które mogą być potencjalnie podatne na ataki Code Execution, takie jak formularze, funkcje przesyłania plików, interfejsy API czy funkcje przetwarzające dane wejściowe od użytkownika.

- sprawdzanie filtracji danych: Testowanie, czy aplikacja prawidłowo filtruje, waliduje i sankcjonuje dane wejściowe, aby zapobiec wykonaniu nieautoryzowanego kodu.

- symulacja ataków: Próby wykorzystania znalezionych podatności poprzez wprowadzenie specjalnie spreparowanych danych wejściowych, które mają na celu wymusić wykonanie nieautoryzowanego kodu. Testy te mogą obejmować techniki takie jak wstrzykiwanie skryptów, przesyłanie złośliwych plików czy ataki typu deserializacji.

e. Broken Authentication and Session Management

Test ma na celu zidentyfikowanie słabości w systemach uwierzytelniania i zarządzania sesjami w aplikacji. Wykonawca musi zrealizować co najmniej następujące zadania:

- analiza systemu uwierzytelniania i zarządzania sesjami: Wykonawca musi sprawdzić, czy aplikacja stosuje odpowiednie mechanizmy uwierzytelniania, nie mniej niż takie jak: silne hasła, uwierzytelnianie wieloskładnikowe czy blokowanie kont po wielokrotnym wprowadzeniu nieprawidłowego hasła.

- testowanie zarządzania sesjami: Wykonawca musi sprawdzić czy aplikacja prawidłowo zarządza identyfikatorami sesji oraz czy są one losowe, odpowiednio długie i unikalne. Wykonawca musi także sprawdzić czy aplikacja stosuje odpowiednie mechanizmy wygasania sesji oraz czy chroni przed atakami typu "session fixation" czy "session hijacking".

- testowanie funkcji odzyskiwania konta: Audytorzy sprawdzają, czy funkcje odzyskiwania konta są bezpieczne i czy nie pozwalają atakującemu na przejęcie konta poprzez uzyskanie dostępu do danych niezbędnych do resetowania hasła lub zmiany adresu e-mail.

- =testowanie obsługi błędów: Sprawdzanie, czy aplikacja nie ujawnia informacji na temat swojej konfiguracji, użytkowników czy systemu uwierzytelniania poprzez komunikaty o błędach.

- próby ataków: Symulacja prób ataków na system uwierzytelniania i zarządzania sesjami, takich jak brute force, ataki słownikowe, ataki typu "session fixation" czy "session hijacking".

f. Authorization Bypass (próby dostępu bez uwierzytelnienia)

W ramach weryfikacji Wykonawca musi zrealizować czynności co najmniej takie jak:

- testowanie uprawnień: Wykonawca powinien sprawdzić, czy system autoryzacji prawidłowo ogranicza dostęp do zasobów i funkcji. Testy te obejmują próby dostępu z różnymi poziomami uprawnień oraz próby dostępu do zasobów, do których nie powinno być możliwe uzyskanie dostępu.

- testowanie funkcji administracyjnych: Wykonawca powinien sprawdzić, czy funkcje administracyjne są odpowiednio zabezpieczone przed nieautoryzowanym dostępem.

- próby ataków: Wykonawca powinien symulować próby ataków na system autoryzacji, aby zidentyfikować potencjalne luki i słabości.

g. Insecure Communications

Zadaniem Wykonawcy jest wykrycie i ocena niezabezpieczonych kanałów komunikacyjnych. W ramach tej usługi musi zostać wykonana analiza ruchu sieciowego, w celu wykrycia wszelkich niezabezpieczonych kanałów komunikacyjnych, takich jak niezabezpieczone protokoły, niezaszyfrowane połączenia, weryfikacja mechanizmów zarządzania sesją, takich jak identyfikatory sesji, niewłaściwe konfiguracje lub błędy konfiguracyjne, które mogą prowadzić do nieautoryzowanego dostępu do systemu lub przechwycenia i odczytania danych.

h. Path Traversal

Zadaniem Wykonawcy jest przeprowadzenie testów na wykrycie podatności na atak typu Path Traversal, znany również jako Directory Traversal, polegający na manipulacji ścieżkami plików w systemie, w celu uzyskania dostępu do chronionych zasobów lub wykonywania nieautoryzowanych operacji na plikach. Test musi wykazać luki w aplikacji (jeżeli takie istnieją), które pozwalają na wprowadzenie ścieżek plików, aby uzyskać dostęp do plików i folderów poza obszarem przewidzianym dla użytkowników aplikacji.

Wykonawca musi wykonać próby uzyskania dostępu do plików i folderów, do których nie powinien mieć dostępu, takich jak pliki konfiguracyjne, dane użytkowników czy inne wrażliwe dane.

i. Open Redirection

Zadaniem wykonawcy jest przeprowadzenie testów na wykrycie podatności typu Open Redirection pozwalającej na wykorzystanie aplikacji do przekierowania użytkownika na niezaufane, zewnętrzne strony internetowe. Zamawiający musi zweryfikować, czy potencjalny atakujący może manipulować parametrami przekierowania w aplikacji, aby wprowadzić własny, złośliwy adres URL.

j. Denial of Service (DoS)

Zadaniem wykonawcy jest określenie stopnia odporności na ataki typu DoS. W zakres realizacji wchodzą następujące czynności takie jak:

a) analiza architektury systemu i infrastruktury sieciowej w celu identyfikacji potencjalnych wejść i usług narażonych na atak DoS.
b) przeprowadzenie testów obciążenia i wydajności na kluczowych komponentach systemu, aby zidentyfikować możliwe wąskie gardła i obszary podatne na przeciążenie.
c) wykonanie symulacji ataków DoS, w tym ataków na warstwę aplikacji, protokołów sieciowych oraz infrastruktury serwerowej, aby ocenić ich wpływ na dostępność systemu.
d) identyfikacja i ocena potencjalnych zagrożeń oraz opracowanie strategii zarządzania ryzykiem związanym z atakami DoS.

k. File Inclusion

Wykonawca musi przeprowadzić badanie podatności na atak typu File Inclusion, polegający na wykorzystaniu błędów w aplikacjach internetowych, aby zmusić serwer do wczytywania, wykonania, plików z zewnętrznego źródła. Wykonawca musi podjąć próbę nieautoryzowanego dostępu do danych, ujawnienie wrażliwych informacji lub zdobycie uprawnień, które umożliwią zdalne wykonywanie kodu na serwerze. Testy muszą obejmować różne techniki i wektory ataku, zarówno dla LFI, jak i RFI.

l. Response Splitting

Wykonawca musi zweryfikować podatność na atak Response Splitting polegający na manipulacji danymi wejściowymi przekazywanymi do serwera, w celu wprowadzenia dodatkowych nagłówków HTTP lub innych wartości w odpowiedzi serwera. Atak ma na celu osiągnięcie różnych celów, takich jak przekierowanie ofiar na złośliwe strony, kradzież danych, wykonanie kodu JavaScript w kontekście domeny ofiary czy omijanie mechanizmów zabezpieczających.

Wykonawca musi przeprowadzić testy bezpieczeństwa, mające na celu sprawdzenie, czy możliwe jest wprowadzenie dodatkowych nagłówków HTTP lub innych wartości w odpowiedzi serwera, wykorzystując dane wejściowe aplikacji.

3.4. badanie podatności – aplikacji z wykorzystaniem listy kontrolnej OWASP

Zadaniem wykonawcy jest zbadanie podatności aplikacji i punktów końcowych z wykorzystaniem listy kontrolnej OWASP (Application Security Verification Standard) ASVS 4.0.3 lub równoważnej.

Prace muszą być realizowane z uwzględnieniem klasyfikacji OWASP ASVS Level 1 i 2 oraz wykorzystaniem własnej metodyki Wykonawcy.

3.5. Testy serwera www

a. Bezpieczeństwo skonfigurowanego mechanizmu SSL:

Wykonawca musi sprawdzić, czy serwer używa aktualnych i bezpiecznych protokołów szyfrowania, czy certyfikaty SSL są prawidłowe, ważne i pochodzą od zaufanego dostawcy, oraz czy serwer obsługuje tylko bezpieczne zestawy szyfrów.

Wykonawca musi przeprowadzić test mechanizmu SSL. Test ma na celu sprawdzenie poprawności konfiguracji certyfikatów SSL/TLS, siły szyfrowania oraz zabezpieczenia komunikacji.

b. Dostępność komunikatów o błędach:

Wykonawca musi sprawdzić, czy serwer generuje komunikaty o błędach zawierające wrażliwe informacje, takie jak dane techniczne, ścieżki plików czy informacje o strukturze bazy danych.

Wykonawca musi przeprowadzić test, który ma na celu zidentyfikowanie przypadków, gdy serwer udostępnia nadmiarowe informacje o błędach, które mogą być wykorzystane przez atakującego do zdobycia informacji o infrastrukturze serwera lub aplikacji.

c. Analiza podatności występujących w zainstalowanej wersji serwera:

Wykonawca musi przeprowadzić test, który ma na celu zidentyfikowanie ewentualnych podatności związanych z konkretną aktualnie używaną wersją serwera WWW, które mogą być wykorzystane przez atakujących.

d. Dostępność nadmiarowych metod HTTP:

Wykonawca musi sprawdzić, które metody HTTP są obsługiwane przez serwer (np. GET, POST, PUT, DELETE, HEAD, OPTIONS, CONNECT, TRACE) i zbadać czy niektóre z nich są zbędne i w związku z tym stanowią niepotrzebny potencjalny wektor ataku.

e. Zastosowanie technik Google Hacking

Wykonawca musi przeprowadzić badanie bezpieczeństwa z zastosowaniem technik Google Hacking oraz zidentyfikować dostępne publicznie, narażone na ataki źródła informacji, takie jak: pliki, foldery, strony internetowe, urządzenia sieciowe, dane konfiguracyjne, kody źródłowe, hasła i inne.

4. Ocena ryzyka dla bezpieczeństwa informacji oraz ciągłości działania

Zadaniem Wykonawcy jest przeprowadzenie szacowania ryzyka na poziomie systemów informatycznych – poziom 3 według definicji NSC 800-30 w zakresie naruszenia poufności i integralności danych oraz utraty ciągłości działania systemów IT.

Do zadań wykonawcy należy:

a) identyfikacja źródeł zagrożeń oraz przypisanie ich do aktywów,
b) identyfikacja podatności, które mogą być wykorzystane przez źródła zagrożeń
c) inwentaryzacja zabezpieczeń,
d) ustalenie prawdopodobieństwa, że zidentyfikowane źródła zagrożeń zainicjują zdarzenia
e) określenie wielkości oddziaływania,
f) ustalenie ryzyka.

Wyniki szacowania ryzyka systemów informacyjnych muszą odnosić się do fazy powykonawczej, a w związku z tym muszą zawierać opisy podatności w istniejących systemach, ocenę ryzyka związanego z

każdą z podatności oraz rekomendowane działania naprawcze, które mogą być podjęte w celu ograniczenia ryzyka.

Cel szacowania ryzyka – dostarczenie informacji niezbędnych do podjęcia decyzji o zmianach w zakresie architektury, technologii, zabezpieczeń technicznych systemów w celu zapewnienia ochrony przetwarzanych danych oraz ciągłości działania prototypu (zwiększenie odporności systemu/Prototypu).

Opisy zdarzeń zagrożeń muszą być wyrażone w sposób szczegółowy tj. z uwzględnieniem nazw konkretnych systemów informacyjnych, technologii, podmiotów ról lub lokalizacji.

Wykonawca musi uwzględnić zagrożenia nie mniej niż takiej jak zostały przedstawione w tabeli *E- 2. Reprezentatywne przykłady zdarzeń zagrożeń o charakterze agresywnym* (NSC 800-30). Wykonawca musi przyjąć 5 stopniową skalę szacowania zgodnie z:

- tabelą F- 2. *Skale szacowania – dotkliwość podatności* (NSC 800-30) dla określenia stopnia dotkliwości podatności,
- tabelą G- 3. *Skale szacowania – Prawdopodobieństwo wystąpienia zdarzeń zagrożeń (agresywne)* dla określenia *prawdopodobieństwa materializacji zagrożenia*
- tabelą H- 3. Skala szacowania – Wpływ zdarzeń zagrożeń – dla określenia wartości skutków materializacji zagrożenia
- *tabelą I- 3. Skala szacowania – poziom ryzyka dla określenia poziomu ryzyka.*

Ustalenie prawdopodobieństwa zdarzenia, określenie wielkości oddziaływania oraz ustalenie ryzyka muszą być oparte o wiedzę ekspercką wykonawcy.

5. Określenie rekomendacji w celu mitygowania ryzyka i raportowanie

5.1. Kryteria oceny i raportowanie – uwagi metodyczne

Zamawiający wymaga wykorzystania znanych baz danych o podatnościach i słabościach bezpieczeństwa systemów informatycznych, w trakcie prac prowadzonych przez Wykonawcę w ramach przedmiotu zamówienia, np.:

a. Common Weakness Enumeration - CWE

b. Common Vulnerabilities and Exposures – CVE

lub równoważnych (za równoważne Zamawiający uzna takie bazy danych, które stanowią aktualne źródło informacji o lukach bezpieczeństwa, są publikowane lub utrzymywane przez uznane powszechnie organizacje, działające na rzecz zapewnienia bezpieczeństwa systemów informatycznych).

Stwierdzone przez wykonawcę podatności rozwiązań informatycznych o ile znajdują na liście znanych podatności, muszą być oznaczone w standardzie CVE, CWE lub równoważnym.

Tam gdzie nie wyznaczono normy, lub kryteriów przyjmuje się jako punkt odniesienia tzw. dobre praktyki i listy kontrolne wynikające ze standardów takich jak NIST SP 800-123, 800-210, ISO:27001 lub równoważnych (w szczególności takich, które stanowią aktualne źródło informacji o bezpiecznej konfiguracji, są publikowane lub utrzymywane przez uznane powszechnie organizacje, działające na rzecz zapewnienia bezpieczeństwa systemów informatycznych).

5.2. Zasady raportowania obserwacji oraz niezgodności z dobrymi praktykami

Niezgodność z dobrymi praktykami, a także obserwacja (zwane łącznie uchybieniami) powinna być opisana w raporcie w sposób jednoznaczny i precyzyjny. W celu zapewnienia pełnej klarowności, wykonawca musi uwzględnić następujące elementy:

a) **Identyfikacja obszaru i zakresu**: Wykonawca musi jasno wskazać, do jakiego obszaru, procesu, systemu lub aplikacji odnosi się niezgodność. Należy dokładnie określić, na której części infrastruktury, systemu informatycznego lub elementu systemu ochrony danych występuje niezgodność. Zamawiający nie dopuszcza stwierdzeń na poziomie ogólnym np. „brak monitorowania infrastruktury" bez szczegółowego określenia zakresu takiego monitoringu.
b) **Dowód z audytu**: Wykonawca stwierdzając niezgodność lub obserwację musi przedstawić dowód lub uzasadnienie obiektywnie potwierdzające stwierdzony przez niego stan faktyczny.
c) **Ryzyko – potencjalny wpływ zagrożeń na aktywa**: Wskazując na niezgodność dobrymi praktykami Wykonawca musi opisać wpływ niezgodności na bezpieczeństwo danych, systemu czy infrastruktury.
d) **Uzasadnienie zastosowania praktyki:** Jeśli Wykonawca wskaże obserwację, niezgodność lub stwierdzi konieczność zastosowania danej praktyki, musi przedstawić uzasadnienie oparte w rzeczywistym kontekście Zamawiającego. Niedopuszczalne są stwierdzenia nieprawidłowości uzasadnione jedynie powszechnością danego zabezpieczenia czy powszechnością praktyki u innych administratorów. Wykonawca mus wykazać bezpośredni związek stwierdzonego uchybienia z konkretnymi aktywami czy procesami Zamawiającego, a także istotnymi zagrożeniami.
e) **Działania naprawcze i środki ograniczające ryzyko:** Do wskazanej przez siebie niezgodności lub obserwacji Wykonawca musi przedstawić rekomendację działań naprawczych. Rekomendowane działania naprawcze, muszą być bezpośrednio związane odpowiednio z obserwacją, niezgodnością lub podatnością.

5.3. Raport z audytu

W wyniku przeprowadzonego audytu bezpieczeństwa Prototypu Wykonawca dostarczy raport zawierający:

a) Opis przeprowadzonych działań, o których mowa w szczegółowym opisie przedmiotu zamówienia,
b) Wyniki testów/badań i ich opartą o wiedzę ekspercką interpretację, w tym wykaz podatności, niezgodności z dobrymi praktykami, błędów i obserwacji wraz oraz opisem ich znaczenia dla bezpieczeństwa Prototypu,

W szczególności, w ramach opisu testów w modelu black-box wykonawca musi ująć w raporcie poniższe dane:
- skuteczne ataki na 1000 prób (liczba skutecznych ataków, liczba udanych nieuprawnionych modyfikacji algorytmów, liczba udanych ataków sfinalizowanych zainstalowaniem złośliwego oprogramowania, liczba udanych prób wykradzenia danych),
*- liczba wykrytych **krytycznych luk** w zabezpieczeniach technicznych na 1000 prób.*

c) Wyniki szacowania ryzyka - określenie ilościowego i jakościowego poziomu niebezpieczeństwa,
d) Rekomendacje i zalecenia pozwalające na redukcję ryzyka w tym propozycję rozwiązań, które pozwolą wyeliminować lub ograniczyć prawdopodobieństwo wykorzystania wykazanych w audycie podatności wraz z szacowaniem w jakim stopniu rekomendowane działanie naprawcze wpłynie na poziom ryzyka.
Rekomendacje i zalecenia muszą odnosić się do każdego badanego obszaru (jeżeli dotyczy).

Informacje, o których mowa w punkcie 5 lit. b,c,d, z chwilą powstania otrzymują klasyfikację *informacji poufnych*.

Raport z audytu musi zostać przygotowany w dwóch częściach:
a) **Raport szczegółowy** – opisujący wszystkie elementy wymagane w niemniejszym zamówieniu w tym informacje wskazane w punkcie 5 lit. b,c,d,
b) **Raport ogólny** (na potrzeby klientów, instytucji i innych podmiotów zewnętrznych) – potwierdzający fakt i zakres wykonanego audytu (5 lit. a), zawierający informacje nieobjęte klauzulą poufności. Raport ogólny ze względów bezpieczeństwa nie może zawierać informacji o podatnościach, obserwacjach, rekomendacjach oraz stwierdzonych niezgodnościach z dobrymi praktykami.

Raport z audytu musi być dostarczony Zamawiającemu, w formie elektronicznej – w formacie .DOC lub .PDF.

Plik zawierający informacje poufne w formacie (.docx) lub PDF, powinien być szyfrowany za pomocą funkcji szyfrowania dostępnych aplikacjach obsługujących te formaty plików lub opcjonalnie w formacie ZIP z użyciem hasła.

Zamawiający, o ile raport będzie spełniał wymogi przedstawione w zamówieniu, dopuszcza dowolną formę prezentacji informacji składających się na raport.

6. Zasady bezpieczeństwa

Wykonawca oraz osoby wydelegowane przez Wykonawcę do realizacji przedmiotu zamówienia, muszą stosować się do poniższych zasad bezpieczeństwa.

1. Każda osoba, która otrzyma dostęp do informacji na temat systemów i zabezpieczeń Zamawiającego musi zachować poufność informacji uzyskanej w związku z realizacją Zamówienia oraz podpisać deklarację zachowania poufności.

2. W zakresie testowania bezpieczeństwa Wykonawca może używać jedynie bezpiecznego i sprawdzonego oprogramowania, którego sposób działania jest mu znany.

2. Instalacja oprogramowania w zasobach Zamawiającego (np. użycie agenta) wymaga zgody Wykonawcy.

3. W celu uzyskania zgody na instalację danego oprogramowania(narzędzia) Wykonawca musi przedłożyć następujące informacje:

a) nazwa i wersja oprogramowania

b) kategoria oprogramowania (open source, rozwiązanie komercyjne, rozwiązanie własne)

c) nazwa producenta rozwiązania.

4. Realizacja audytu nie może zakłócać pracy operacyjnej firmy w dniach roboczych w godzinach od 8:00 do 16:00.

5. Wykonawca będzie ponosił odpowiedzialność w przypadku ewentualnych szkód lub strat wynikających z audytu, a także za wszelkie naruszenia lub uszkodzenia wyrządzone w trakcie audytu.

6. Wykonawca nie może naruszać zasad bezpieczeństwa stron trzecich w tym naruszać regulaminów dostawców usług chmurowych (np. Microsoft Azure).

6. Po zakończeniu audytu Wykonawca jest zobowiązany do usunięcia z infrastruktury Zamawiającego wszelkich narzędzi i oprogramowania, które zostały wykorzystane podczas audytu.

7. Definicje zastosowanych pojęć

W przypadku wątpliwości w zakresie terminologii występującej w języku angielskim przyjmuje się znaczenie przyjęte w ”Słowniku kluczowych pojęć z zakresu cyberbespieczeństwa” wydanym przez pełnomocnika rządu ds. cyberbezpieczeństwa w ramach Narodowego Standardu Cyberbezpieczeństwa (NSC 7298) z dnia 01/09/2021.

Przez ryzyko rozumie się potencjalną szansę materializacji zagrożenia oraz jego wpływu na aktywa organizacji. Wyraża się prawdopodobieństwem i skutkami negatywnego zdarzenia.

Obserwacja to fakt lub zauważenie dokonane przez audytora podczas przeprowadzania audytu bezpieczeństwa danych. W odróżnieniu od niezgodności, obserwacja nie jest bezpośrednią stwierdzoną nieprawidłowością czy odstępstwem od wymagań bezpieczeństwa, ale wskazuje na potencjalne obszary, które mogą wymagać dalszej analizy lub poprawy. Może to obejmować sugestie w celu wzmocnienia zabezpieczeń lub zidentyfikowanie potencjalnych ryzyk.

Dowód z audytu jest dokumentacją lub materiałem zgromadzonym podczas procesu audytu, który potwierdza fakty, obserwacje, wnioski i oceny dokonane przez audytora. Jest to zbiór dokumentów, informacji, notatek, wyników testów i innych danych, które stanowią podstawę dla wniosków i rekomendacji wynikających z audytu.

Luka krytyczna to rodzaj podatności lub błędu w oprogramowaniu, systemie lub aplikacji, który ma potencjał spowodowania poważnych skutków lub naruszenia bezpieczeństwa, a także istnieje wysokie prawdopodobieństwo, ze może być wykorzystany przez atakujących.

---

* Przekazanie danych stanowiących tajemnicę przedsiębiorstwa wymaga zawarcia stosowanej umowy o zachowaniu poufności. Wzór umowy znajduje się w Załączniku nr 6. Na wyraźną prośbę Oferenta, dane poufne zostaną mu przekazane w ciągu 2 dni roboczych od przesłania drogą mailową umowy o zachowaniu poufności podpisanej kwalifikowanym podpisem elektronicznym lub jej podpisanego skanu. Podpisaną umowę o zachowaniu poufności należy przesłać nie później niż na 2 dni robocze przed terminem składania ofert, w celu umożliwienia udostępnienia dokumentów objętych poufnością w wyznaczonym terminie składania ofert. Umowa winna zostać uzupełniona i podpisana przez osobę upoważnioną do reprezentowania Oferenta.
*