Załącznik nr 1

do zapytania ofertowego na usługi testów bezpieczeństwa

Ministerstwo Rozwoju i Technologii **Warszawa, dnia 26 lipca 2024 r.**

Plac Trzech Krzyży 3/5

00-507 Warszawa

Opis przedmiotu zamówienia

dotyczące usługi testów bezpieczeństwa weryfikujące skuteczność ochrony systemów teleinformatycznych MRiT

I. Przedmiot Zamówienia

1. Przedmiotem zamówienia są usługi testów bezpieczeństwa weryfikujące skuteczność ochrony systemów teleinformatycznych MRiT.
2. Testy bezpieczeństwa będą realizowane poprzez:
   1) testy penetracyjne, tj. weryfikację ochrony technicznej systemów;
   2) audyty bezpieczeństwa aplikacji oraz infrastruktury informatycznej;
   3) raporty z testów, uwzględniające rekomendacje w zakresie optymalizacji bezpieczeństwa aplikacji oraz infrastruktury informatycznej oraz raporty z przeprowadzonych czynności testowych.

II. Termin i sposób realizacji Zamówienia

1. Usługi testów bezpieczeństwa weryfikujące skuteczność ochrony systemów teleinformatycznych MRiT będą świadczone w okresie 12 miesięcy od daty zawarcia umowy.
2. Usługi w ramach zamówienia będą świadczone zgodnie z zapotrzebowaniem Zamawiającego, każdorazowo na podstawie zleceń uwzględniających uzgodniony z Wykonawcą zakres, liczbę osobodni oraz termin realizacji.
3. Maksymalna liczba osobodni została wskazana w Formularzu Ofertowym.
4. Zamawiający zastrzega sobie prawo do niewykorzystania maksymalnej liczby osobodni.
5. W terminie do 10 dni po wykonaniu każdego ze zleceń Wykonawca przekaże Zamawiającemu raport przygotowany według wymagań opisanych w pkt III w części Minimalne wymagania w zakresie raportowania wykonanych prac w ramach zamówionych usług.
6. Usługi testów bezpieczeństwa Wykonawca zobowiązuje się realizować w dwóch formach:
   1) w siedzibie Zamawiającego przez pracowników Wykonawcy. Termin wykonania tych usług zostanie uzgodniony z Wykonawcą i wskazany w zleceniu. Usługi te będą świadczone w osobodniach, tj.: przez 8 godzin w danym dniu;
   2) zdalnie przez pracowników Wykonawcy. Termin wykonania tych usług uzgodniony zostanie wcześniej z Wykonawcą i wskazany w zleceniu. Usługi te będą świadczone w osobodniach, tj.: przez 8 godzin w danym dniu poprzez szyfrowane połączenie.

III. Minimalne wymagania realizacji przedmiotu zamówienia

Usługi testów bezpieczeństwa weryfikujące skuteczność ochrony systemów teleinformatycznych MRiT muszą być realizowane zgodnie z poniżej opisanymi minimalnymi wymaganiami.

Minimalne wymagania w zakresie testów penetracyjnych

1. Usługa testów penetracyjnych musi poddawać ocenie oraz wskazywać podatności w co najmniej następujących obszarach dotyczących:
   1) mechanizmów uwierzytelniania – weryfikując skuteczność procesu uwierzytelniania oraz

wskazując podatności występujące w tym obszarze;

2) zarządzania sesją – weryfikując skuteczność mechanizmów zarządzania sesją użytkownika oraz wskazując możliwe podatności występujące w tym obszarze;

3) skuteczności walidacji danych – badając skuteczność użytych mechanizmów walidacyjnych oraz oceniając ich adekwatność, zarówno w zakresie walidacji rodzaju danych jak i ich rozmiaru czy dopuszczalnych ilości wprowadzanych danych wraz z identyfikacją podatności w tym obszarze;

4) stosowanych algorytmów kryptograficznych – weryfikując skuteczność oraz zgodność ze standardami (np. NIST) w zakresie zastosowanych mechanizmów ochrony kryptograficznej (np. TLS, funkcje skrótu – ang. *hash*, algorytmy szyfrujące i deszyfrujące, podpisywanie), ocena skuteczności wykorzystania certyfikatów i serwerów certyfikatów oraz identyfikacja podatności w tym zakresie;

5) obsługi błędów – podając ocenie poprawność obsługi błędów/wyjątków powstających na skutek użytkowania testowanego rozwiązania jak również wskazanie potencjalnych podatności w tym obszarze;

6) zapewnienia ochrony danych (dostępność, poufność, integralność) – weryfikując mechanizmy przetwarzania danych, ze szczególnym uwzględnieniem danych osobowych, w identyfikacji możliwości nieautoryzowanego dostępu lub modyfikacji jak również oceniać mechanizmy audytu prowadzonych na tych danych operacji (rozliczalność);

7) bezpieczeństwa komunikacji (na poziomie warstwy trzeciej – sieciowej i czwartej – aplikacyjnej modelu OSI, podział na strefy sieciowe np. DMZ) – weryfikując zastosowania oraz skuteczności dobrania zabezpieczeń sieciowych oraz usług sieciowych takich jak np. Firewall, Web Application Firewall, Proxy oraz wykrycie ewentualnych podatności w tym obszarze, a także weryfikacja separacji na poziomie sieciowej poprzez wydzielenie stref bezpieczeństwa takich jak np. DMZ, sieci administracyjnych, sieci połączeń między warstwami aplikacji, a także oceniając bezpieczeństwo w zakresie dostępu poprzez mechanizmy VPN;

8) przeciążenia systemu – oceniając skuteczność ochrony systemu przed przeciążeniem lub innym błędnym działaniem związanych przez nieuprawniony wzrost obciążenia systemu jak również wskazanie potencjalnych podatności;

9) bezpieczeństwa kodu źródłowego – polegając na analizie statycznej kodu z wykorzystaniem narzędzi automatyzujących wykonawcy wraz z manualnym wsparciem w zakresie weryfikacji wykrytych nieprawidłowości, wykonywane w środowisku zamawiającego;

10) wykrywanie usług sieciowych udostępnionych w Internecie – polegające na identyfikowaniu i badaniu usług i źródeł usług wystawionych do sieci Internet, jak również identyfikowaniu podatności w obrębie tych usług;

11) wykrywania infekcji szkodliwym oprogramowaniem (np. wykrywanie malware, programów wyłudzających, programów typu exploit, backdoor) – weryfikując bezpieczeństwo danych (np. plików komputerowych) oraz oprogramowania, a polegająca na wykrywaniu i eliminacji zagrożeń wynikających z infekcji szkodliwym oprogramowaniem, a także polegające na eliminacji błędnych identyfikacji zagrożenia (ang. *false-positive*);

12) zapewniania bezpieczeństwa oprogramowania bazowego (np. systemu operacyjny, firmware, kontenerów aplikacji np. JBOSS) – poddająca ocenie aktualność oraz odporność na znane zagrożenia wykorzystanego oprogramowania bazowego takiego jak na przykład system operacyjny (Linux, Windows), firmware (np. infrastruktura sieciowa), tomcat, JBOSS, a także oceniająca skuteczność konfiguracji w zakresie bezpieczeństwa (np. włączone usługi sieciowe, identyfikujące wymagane aktualizacje w obszarze bezpieczeństwa), poprawność działania mechanizmów zapewniających rozliczalność (np. logi audytowe, logi techniczne), poprawność działania systemów backupu;

13) zapewniania bezpieczeństwa urządzeń i sieci przewodowych;

14) zapewniania bezpieczeństwa urządzeń i sieci bezprzewodowych (zarówno GSM jak i Wi-

Fi) – polegająca na weryfikacji konfiguracji urządzeń komunikacji bezprzewodowej takich jak access-pointy oraz urządzenia klienckie – przenośne wraz z identyfikacją podatności w tym zakresie.

2. Realizacja usługi testów penetracyjnych będzie polegała na wykrywaniu podatności technicznych w oparciu o testy typu „Black box" – tester nie posiada wiedzy dotyczącej testowanego obiektu.
3. Realizacja usługi testów penetracyjnych będzie polegać na wykrywaniu podatności technicznych co najmniej uwzględniając przy tym sposoby takie jak:
    1) modyfikacja adresu URL – modyfikacja odwołań do usług sieciowych (serwisów), polegających na zmianie składni lub zawartości łańcucha URL;
    2) wprowadzanie niedozwolonych plików – wprowadzenie za pośrednictwem formularzy lub innych metod niedozwolonych plików lub danych, w tym:
        a) wprowadzaniu niedozwolonej treści (np. Cross-Site scripting),
        b) wywołania niedozwolonej akcji (np. Cross-Site request forgery),
    3) przechwytywanie komunikacji (Man in the Middle);
    4) utrata poufności danych (SQL injection, nieuprawniony dostęp do kodu źródłowego, code injection);
    5) nieuprawnione, zagrażające działania na XML (XML External Entity, XML Bomb);
    6) nieuprawniony dostęp do katalogów – wywoływanie funkcji trawersujących po niedozwolonych ścieżkach katalogowych z danymi (np. systemowymi);
    7) przepełnienie buforów/stosu – przerwanie działania oprogramowania często na skutek przeprowadzenia niedozwolonej operacji;
    8) identyfikacja szkodliwego oprogramowania – identyfikacja oprogramowania stanowiącego zagrożenia dla poufności i integralności danych, z uwzględnieniem mechanizmu eliminacji błędnych wykryć takiego oprogramowania (ang. *false positive*), wraz z korektami u dostawców skanerów oprogramowania.
4. Usługi testów penetracyjnych muszą obejmować:
    1) wykorzystanie informacji z baz danych o podatnościach, z uwzględnieniem co najmniej jednej z udostępnianych przez: SANS INSTITUTE (sans.org) , NIST (nist.gov – NVD), a także CVE – Common Vulnarabilities and Exposures (mitre.org), Web Application Security Consortium (webappsec.org) lub innych uznanych przez Zamawiającego jako równoważne,
    2) stosowanie co najmniej jednego ze standardów w zakresie testów bezpieczeństwa takich jak wytyczne: organizacji OWASP (owasp.org) – Open Web Application Security Project (ASVS), OSSTMM (isecom.org) – Open Source Security Testing Methodology Manual, PTES (pentest – standard.org) – Penetration Testing Execution Standards, NIST (nist.org) – w zakresie testów penetracyjnych lub innych uznanych przez Zamawiającego jako równoważne,
    3) umiejętności stosowania list kontrolnych w oparciu o uznane w zakresie bezpieczeństwa organizacje takie jak NIST (nist.gov), NSA (nsa.gov), CIS (cisecurity.org), US-CCU (us-ccu.us),
    4) formalne dokumentowanie wykonywanych testów na każdym etapie ich trwania.

<u>Minimalne wymagania w zakresie audytów bezpieczeństwa aplikacji oraz infrastruktury informatycznej</u>

1. Audyt bezpieczeństwa aplikacji oraz infrastruktury informatycznej musi obejmować:
    1) audyt przyjętych wariantów i zasad dotyczących warstwowości systemu i aplikacji zgodnie z modelem 1, 2 lub 3–warstwowym (prezentacja, logika i dane);
    2) audyt warstw systemów i aplikacji oraz wsparcie projektowe w zakresie bezpieczeństwa

w tym w szczególności weryfikacja:

a) mechanizmów uwierzytelniania, m.in. w zakresie rozliczalności,

b) mechanizmów autoryzacji,

c) bezpieczeństwa komunikacji (np. szyfrowanie w warstwie trzeciej i czwartej modelu OSI), podpisywanie komunikatów (np. XML),

d) mechanizmów walidacyjnych (weryfikacja danych wejściowych pod kątem zawartości składni, rozmiaru oraz z uwzględnieniem czynnika czasu – np. ilość zapytań w jednostce czasu),

3) audyt sposobów oraz wsparcie na etapie projektowania systemów i aplikacji w celu zapewnienia dostępności, poufności i integralności danych wraz z zachowaniem ich rozliczalności;

4) audyt architektury oraz wsparcie na etapie jej opracowywania w zakresie skalowalności systemu i aplikacji, zarówno w zakresie wolumenu danych jak i jednoczesności wykonywanych operacji;

5) audyt architektury;

6) audyty bezpieczeństwa mechanizmów przeciwdziałania wyciekom informacji (ang. *Data Leak Protection – DLP*).

2. Audyt bezpieczeństwa sieci oraz usług sieciowych oraz wsparcie na etapie ich projektowania ze szczególnym uwzględnieniem:

1) mechanizmów separacji sieci, także w zakresie segmentacji oraz reguł sieciowych firewall w warstwie 2, 3 i 4 modelu OSI;

2) mechanizmów zapewnienia bezpieczeństwa sieci bezprzewodowych GSM oraz Wi-Fi;

3) audyty bezpieczeństwa mechanizmów przeciwdziałania wyciekom informacji (ang. *Data Leak Protection* – DLP);

4) mechanizmów ochrony proaktywnej takich jak systemy IPS, IDS (ang. *Intrusion Prevention/Detection System*) oraz systemy korelacyjnej analizy zdarzeń.

3. Audyt bezpieczeństwa baz danych oraz wsparcie na etapie projektowania systemów bazodanowych ze szczególnym uwzględnieniem mechanizmów uwierzytelniania (poufności), obejmujący mechanizmy uprawnień na poziomie bazy danych, w tym schematów, kolumn oraz procedur, a także w zakresie rozliczalności i integralności danych oraz wydajności i skalowalności.

4. Audyt bezpieczeństwa urządzeń końcowych wraz ze wsparciem dotyczącym opracowywania polityk bezpieczeństwa dla tych urządzeń, uwzględniających rodzaj przetwarzanych danych, uprawnienia użytkowników oraz z uwzględnieniem aspektów dotyczących bezpieczeństwa poczty elektronicznej, dostępu do sieci Internet, ochrony antywirusowej oraz ochrony przed innego rodzaju atakami (np. socjotechnicznymi, żądaniami okupu – ransomware).

5. Audyt bezpieczeństwa systemów operacyjnych oraz oprogramowania bazowego firmware jak również konsultacje na etapie projektowym (w tym wyboru rozwiązania) w zakresie zabezpieczania (ang. *hardening*), podziału przestrzeni pamięci RAM oraz pamięci dyskowej, weryfikacji aktualności oprogramowania bazowego oraz systemu operacyjnego wraz ze wszystkimi zainstalowanymi komponentami, ocena przyjętych mechanizmów rozliczalności działań użytkowników, operatorów oraz administratorów tych systemów wraz z oceną adekwatności przyznanych uprawnień.

6. Audyt bezpieczeństwa w zakresie zasad backupu i archiwizacji danych z uwzględnieniem wymagań w zakresie parametrów przywrócenia do działania po awarii (ang. RTO, RPO, MTD).

<u>Minimalne wymagania w zakresie raportowania wykonanych prac w ramach zamówionych usług</u>

1. Raporty z wykonanych usług muszą być wykonywane każdorazowo po przeprowadzonych testach oraz muszą co najmniej obejmować poniżej opisany zakres:

1) Informacje dla kierownictwa – streszczenie najważniejszych kwestii związanych i wynikających z przeprowadzonych testów takich jak przedmiot i cel testów wraz z wynikiem, a także zwięzłe rekomendacje;

2) Informacje szczegółowe opisujące co najmniej:

   a) opis testowanego przedmiotu,

   b) zakres prowadzonych testów,

   c) cel prowadzonych testów,

   d) przyjęte założenia oraz metodyka/sposób testowania (wraz z uzasadnieniem),

   e) przebieg testów (wraz ze wszystkimi zapiskami powstałymi w procesie testowania),

   f) obserwacje i ustalenia – opis sytuacji (zawierające także przyczyny występujących błędów i podatności oraz potencjalny wektor ataku),

   g) wyniki przeprowadzonych testów – wskazanie podatności wraz ich ważnością,

   h) wnioski – ocena badanego obszaru wraz z kryterium ważności (poziomu zagrożenia),

   i) rekomendacje – zalecane zmiany wraz ze wskazaniem miejsc oraz propozycją ich implementacji,

2. W przypadku oceny kodów źródłowych testy powinny wskazać na źródło błędu, interpretację (ocenę potencjalnych skutków, potencjalny wektor ataku) oraz uwzględniać sposoby ich wyeliminowania.

3. Raporty będą wykonywane każdorazowo na szablonach, które zostaną przedstawione przez Wykonawcę oraz po akceptacji tych szablonów przez Zamawiającego.

<u>Minimalne wymagania w zakresie kompetencji osób wykonujących testy bezpieczeństwa.</u>

Zespół realizujący testy bezpieczeństwa musi składać się z nie mniej niż 2 osób o kompetencjach opisanych poniżej:

1) muszą posiadać co najmniej średnie wykształcenie, a także posiadać aktualne kompetencje merytoryczne potwierdzone poniżej wskazanymi certyfikatami:

   a) co najmniej jedna osoba w zespole musi posiadać kompetencje potwierdzone co najmniej jednym z certyfikatów: CISA (aktualnym i wydany przez isaca.org) lub CISSP (aktualnym i wydanym przez ISC2.org) lub Audytor Wiodący normy ISO 27001:2022 (aktualnym i wydanym przez akredytowane organizacje certyfikujące) oraz jednym z certyfikatów eWPTv1 lub WAPTXv2 (wydanym przez eLearn Security – elearnsecurity.com) lub CMWAPT (wydanym przez IACRB – iacertification.org) lub CEH (wydanym przez EC-Council)

   oraz

   b) wszystkie osoby w zespole muszą posiadać kompetencje potwierdzone jednym z certyfikatów: OSCP (aktualnym i wydanym przez Offensive Security) lub CPTE (aktualnym i wydanym przez Mile2.com) lub GIAC (aktualny i wydany przez giac.org).

2) Zamawiający wymaga aby osoby oddelegowane przez Wykonawcę do realizacji zamówienia i wskazane w ofercie Wykonawcy osobiście świadczyły usługi.