Zakres przedmiotu zamówienia

1. Przedmiotem zamówienia publicznego jest wykonanie audytu bezpieczeństwa następujących systemów teleinformatycznych, które wykonane lub zmodernizowane zostały w ramach projektu pn. „Monitoring pracy i pobytu w celach zarobkowych cudzoziemców na terytorium Rzeczypospolitej Polskiej (MPPC)" nr POPC.02.01.00-00-0093/18, realizowanego w ramach Działania 2.1 „Wysoka dostępność i jakość e-usług publicznych" w ramach II osi priorytetowej PO PC 2014-2020 i współfinansowanego ze środków Europejskiego Funduszu Rozwoju Regionalnego:
   1.1. Broker SI PSZ;
   1.2. Centralna Baza Danych Cudzoziemców (CBDC);
   1.3. Centralna Baza Ofert Pracy (CBOP);
   1.4. Praca.gov.pl;
   1.5. Wortal PSZ;
   1.6. Zatrudnienie Cudzoziemców (ZC).
2. Celem głównym audytu jest określenie poziomu bezpieczeństwa systemów teleinformatycznych określonych w pkt 1, wykorzystywanej przez nie platformy sprzętowo-systemowej, wskazanie punktów obniżających ten poziom oraz zaproponowanie działań, które doprowadzą do uzyskania akceptowalnego przez Zamawiającego poziomu bezpieczeństwa.
3. Audyt zostanie wykonany w dwóch etapach. Pierwszy etap obejmować będzie pełen zakres prac audytowych opisanych w pkt 4 – 6 niniejszego dokumentu. Drugi etap to reaudyt mający na celu weryfikację poprawności implementacji zmian w systemach teleinformatycznych oraz wprowadzenia zmian konfiguracyjnych w wykorzystywanych przez nie platformach sprzętowo-systemowych w celu wyeliminowania bądź całkowitej redukcji ryzyk związanych z podatnościami stwierdzonymi w trakcie pierwszego etapu prac. Po każdym zrealizowanym etapie audytu bezpieczeństwa Wykonawca opracuje „Raport z audytu bezpieczeństwa systemów: Broker SI PSZ, CBDC, CBOP, Praca.gov.pl, Wortal PSZ i ZC", zawierający informacje określone w pkt 5.2.
4. Podstawowe informacje dotyczące systemów teleinformatycznych, o których mowa w pkt. 1:
   4.1. **Broker SI PSZ** – szyna komunikacyjna umożliwiająca wymianę danych w postaci elektronicznej między systemami teleinformatycznymi wykorzystywanymi przez jednostki Publicznych Służb Zatrudnienia i z systemami zewnętrznymi. Broker SI PSZ składa się m.in. z modułu Centralnej Bazy Użytkowników i Węzłów, służącego do identyfikacji jednostek i autoryzacji pracowników tych jednostek oraz modułu Słowniki Centralne, zawierającego słowniki i parametry centralne;
   4.2. **Centralna Baza Danych Cudzoziemców (CBDC)** – system teleinformatyczny, który zawiera informacje o cudzoziemcach, którym powierza się wykonywanie pracy, podmiotach powierzających cudzoziemcom wykonywanie pracy oraz sprawach z zakresu wykonywania pracy przez cudzoziemców na terytorium Rzeczypospolitej Polskiej, pozyskiwanych z MRPiPS, a także ze wszystkich PUP i UW;
   4.3. **Centralna Baza Ofert Pracy (CBOP)** – system teleinformatyczny dostępny pod adresem oferty.praca.gov.pl, umożliwiający gromadzenie, przetwarzanie i udostępnianie danych dotyczących ofert pracy, stażu, praktyk zawodowych i przygotowania zawodowego dorosłych, praktyk studenckich w administracji oraz wydarzeń (targów i giełd pracy, szkoleń, grupowych porad zawodowych, informacji zawodowych, spotkań

informacyjnych, itp.), pochodzących ze wszystkich PUP, WUP oraz ochotniczych hufców pracy;

4.4. **Praca.gov.pl** – system teleinformatyczny dostępny pod adresem praca.gov.pl, wykorzystywany przez PUP, UW i WUP do świadczenia usług elektronicznych na rzecz osób bezrobotnych, poszukujących pracy oraz pracodawców;

4.5. **Wortal PSZ** – internetowy serwis informacyjny Publicznych Służb Zatrudnienia, składający się m.in. z:

4.5.1. Witryny Centralnej PSZ, dostępnej pod adresem psz.praca.gov.pl, zawierającej informacje dotyczące krajowego i europejskiego rynku pracy, zadań państwa w zakresie promocji zatrudnienia, łagodzenia skutków bezrobocia i aktywizacji zawodowej osób oraz przepisów prawnych regulujących kwestie z tym związane. Witryna Centralna PSZ wykonana jest w pięciu wersjach językowych: angielskiej, białoruskiej, polskiej, rosyjskiej i ukraińskiej,

4.5.2. Witryn WUP i PUP, do których odwołania znajdują się pod adresem psz.praca.gov.pl/wybor-urzedu, które w sposób kompleksowy i ujednolicony prezentują informacje dotyczące oferowanego wsparcia, świadczonych usług oraz aktualnej sytuacji na lokalnych rynkach pracy,

4.5.3. Witryn Intranetu Centralnego PSZ i Witryn Intranetów PUP i WUP, dedykowanych dla Użytkowników posiadających nadane stosowane uprawnienia, zawierających m.in. następujące informacje: pisma i komunikaty, akty prawne wraz z wyjaśnieniami, kalendarz wydarzeń, publikacje, odwołania do systemów i innych stron internetowych PSZ, ankiety. Intranet Centralny PSZ dostępny jest pod adresem intranet.praca.gov.pl,

4.5.4. Poczty PSZ – systemu poczty elektronicznej PSZ;

4.6. **Zatrudnianie Cudzoziemców (ZC)** – system teleinformatyczny umożliwiający UW i MRPiPS obsługę procesu wydawania decyzji administracyjnych dotyczących zezwoleń na pracę cudzoziemców na terytorium Rzeczpospolitej Polskiej.

5. W ramach każdego z etapów audytu bezpieczeństwa, o których mowa w pkt 3, Wykonawca zobowiązany jest do:

5.1. Wykonania prac związanych ze zbadaniem wewnętrznych i zewnętrznych podatności i wynikających z nich zagrożeń wraz z oceną poziomu bezpieczeństwa systemów teleinformatycznych określonych w pkt 1 oraz wykorzystywanej przez nie platformy sprzętowo-systemowej, w szczególności w odniesieniu do:

5.1.1. zastosowanych technologii i standardów zabezpieczeń,

5.1.2. słabości oprogramowania oraz poprawności konfiguracji urządzeń i systemów sieciowych,

5.1.3. faktu istnienia styków sieci o różnym charakterze, np. styku z siecią Internet, styku systemów z innymi sieciami, w tym potencjalne zagrożenia ze strony sieci zewnętrznej,

5.1.4. polityk bezpieczeństwa skonfigurowanych na ww. urządzeniach.

5.2. Opracowania „Raportu z audytu bezpieczeństwa systemów: Broker SI PSZ, CBDC, CBOP, Praca.gov.pl, Wortal PSZ i ZC" zawierającego w odniesieniu do poszczególnych systemów teleinformatycznych określonych w pkt 1:

5.2.1. Opis działań i testów, które zostały wykonane,

5.2.2. Opis podatności stwierdzonych w trakcie audytu w odniesieniu do systemów teleinformatycznych oraz wykorzystywanych przez nie platform sprzętowo-systemowych,

5.2.3. Wskazanie niezbędnych i adekwatnych działań koniecznych do zrealizowania w celu wyeliminowania bądź całkowitej redukcji ryzyk związanych ze stwierdzonymi podatnościami w odniesieniu do systemów teleinformatycznych i wykorzystywanych przez nie platform sprzętowo-systemowych,

5.2.4. Wskazanie propozycji wprowadzenia dodatkowych mechanizmów zabezpieczających, które doprowadzą do podniesienia poziomu bezpieczeństwa systemów teleinformatycznych i zapewnią ich lepszą ochronę przed możliwymi atakami sieciowymi i aplikacyjnymi.

6. Audyt bezpieczeństwa systemów teleinformatycznych określonych w pkt 1 obejmie (o ile dotyczy danego systemu):

6.1. Testy styku systemów teleinformatycznych z Internetem.

6.1.1. Realizacja testów styku systemów teleinformatycznych z Internetem ma na celu:

6.1.1.1. Wskazanie miejsc, które mogą być bezpośrednio zaatakowane z poziomu sieci Internet (włamania do zewnętrznych systemów w DMZ);

6.1.1.2. Wskazanie miejsc ewentualnego wycieku informacji o infrastrukturze IT;

6.1.1.3. Oszacowanie skuteczności obecnie stosowanych zabezpieczeń w warstwie sieciowej (w tym odporność na ataki techniczne i szczelność systemów klasy firewall);

6.1.1.4. Wskazanie ewentualnych dodatkowych metod ochrony.

6.1.2. W ramach tego etapu audytu Wykonawca zobowiązany jest do realizacji m.in. następujących prac:

6.1.2.1. Analiza topologii (architektury) brzegu sieci;

6.1.2.2. Testy szczelności systemów klasy firewall;

6.1.2.3. Analiza komunikacji sieciowej z poziomu Internetu;

6.1.2.4. Skanowanie portów (kilka technik) – próby wykrycia usług sieciowych/ urządzeń sieciowych dostępnych z poziomu Internetu;

6.1.2.5. Próby detekcji wersji oraz typu oprogramowania systemowego zainstalowanego na urządzeniach dostępnych z Internetu;

6.1.2.6. Próby wykorzystania znanych podatności w wykrytych komponentach;

6.1.2.7. Próby wybranych ataków typu DoS;

6.1.2.8. Skanowanie podatności na aktywnych hostach z badanej (pod) sieci publicznej.

6.1.3. W trakcie testów Wykonawca powinien m.in.: przeprowadzić kilka rodzajów skanowania portów TCP/UDP, skany typu LIST, fingerprint urządzeń, zaawansowane wersje traceroute, generację pakietów niezgodnych z RFC w celu mapowania topologii sieci, zastosować kilka metod omijania systemów klasy firewall.

6.2. Testy penetracyjne aplikacji webowych (Blackbox).

6.2.1. Realizacja testów penetracyjnych aplikacji webowych (Blackbox) ma na celu:

6.2.1.1. Zbadanie odporności aplikacji webowych na ataki z Internetu;

6.2.1.2. Wskazanie potencjalnych skutków ataku dla znalezionych luk i określenie ich krytyczności;

6.2.1.3. Wskazanie metody naprawy każdej ze znalezionych luk w bezpieczeństwie;

6.2.1.4. Wskazanie sposobu unikania podobnych błędów w przyszłości.

6.2.2. W ramach tego etapu audytu Wykonawca zobowiązany jest do realizacji co najmniej następujących prac:

6.2.2.1. Google Hacking, tj.:

6.2.2.1.1. Detekcja sposobu wyświetlania błędów oraz błędów klasy information leakage;

6.2.2.1.2. Detekcja lustrzanych serwisów w domenie dostawcy oprogramowania;

6.2.2.1.3. Detekcja aktywnych poddomen;

6.2.2.1.4. Detekcja lokalizacji panelu administracyjnego.

6.2.2.2. Detekcja wykorzystanego oprogramowania, w tym:

6.2.2.2.1. Detekcja ogólnie znanego oprogramowania (aplikacje, biblioteki, systemy wspomagające);

6.2.2.2.2. Próby lokalizacji znanych błędów w wykrytym oprogramowaniu.

6.2.2.3. Detekcja błędów aplikacyjnych – kilka testów w odniesieniu do m.in. następujących klas błędów:

6.2.2.3.1. SQL Injection;

6.2.2.3.2. XSS (Cross Site Scripting) – błędy typu reflected oraz stored;

6.2.2.3.3. CSRF (Cross Site Request Forgery);

6.2.2.3.4. Broken Authentication and Session Management (badanie losowości ID sesji, próba detekcji składni nazywania cookie sesyjnego, sprawdzenie bezpieczeństwa budowy formularza logowania);

6.2.2.3.5. Authorization Bypass (próby dostępu do zasobów bez uwierzytelnienia użytkownika);

6.2.2.3.6. Code Execution (próby wykonania wrogiego kodu na serwerze);

6.2.2.3.7. Information Leakage (próby detekcji wycieku istotnych informacji – technicznych i biznesowych – z serwera);

6.2.2.3.8. Insecure Communications (np. dostęp do istotnych danych – np. konta administracyjnego bez szyfrowania);

6.2.2.3.9. Source Disclosure (próby prowadzące do ujawnienia kodów źródłowych wykorzystanego oprogramowania);

6.2.2.3.10. Path Traversal;

6.2.2.3.11. Open Redirectio;

6.2.2.3.12. Denial of Service (DoS);

6.2.2.3.13. File Inclusion;

6.2.2.3.14. Response Splitting;

6.2.2.3.15. kilka prób lokalizacji błędów logicznych.

6.3. Zewnętrzny test serwerów HTTP.

6.3.1. Realizacja zewnętrznego testu serwerów HTTP ma na celu:

6.3.1.1. Zbadanie odporności serwera WWW na ataki z Internetu;

6.3.1.2. Wskazanie potencjalnych skutków ataku dla znalezionych luk i określenie ich krytyczności;

6.3.1.3. Wskazanie metody naprawy każdej ze znalezionych luk w bezpieczeństwie;

6.3.1.4. Wskazanie ewentualnych dodatkowych metod ochrony.

6.3.2. W ramach tego etapu audytu Wykonawca zobowiązany jest do realizacji m.in. następujących prac:

6.3.2.1. Próby detekcji typu i wersji serwera WWW; po udanej detekcji, próba zlokalizowania znanych podatności w danej wersji serwera;

6.3.2.2. Sprawdzenie obsługi błędów na serwerze WWW (kilka testów bazujących na błędnie wysłanych requestach http lub requestach do nieistniejących zasobów;

6.3.2.3. Sprawdzenie dostępności domyślnych katalogów/ plików;

6.3.2.4. Sprawdzenie dostępności oraz konfiguracji protokołu szyfrującego HTTPS (możliwość negocjacji TLSv1.3, dostępność słabych szyfrów sesji, sprawdzenie poprawności oraz ważności certyfikatu TLS);

6.3.2.5. Sprawdzenie metod http udostępnianych na serwerze (GET, POST, HEAD, TRACE, OPTIONS, itd.);

6.3.2.6. Sprawdzenie informacji wysyłanych w nagłówkach HTTP response (wybranie kilku różnych nagłówków);

6.3.2.7. Sprawdzenie możliwości wykorzystania serwera jako open proxy;

6.3.2.8. Sprawdzenie możliwości dostępu do danych zabezpieczonych protokołem HTTPS poprzez nieszyfrowany protokół HTTP.

7. Realizując audyt bezpieczeństwa Wykonawca będzie kierował się następującymi zasadami przeprowadzania testów penetracyjnych:

7.1. Testy będą prowadzone w trybie 24/7;

7.2. Nie będą realizowane testy celowo destrukcyjne, np.: usuwanie lub modyfikacja danych, znane rodzaje DoS (np. XML Bomb), DDoS, wyczerpanie pamięci na serwerze, wyczerpanie zasobów procesora na serwerze;

7.3. Nie będą realizowane testy celowo modyfikujące dane w testowanych systemach;

7.4. Nie będą stosowane gotowe exploity;

7.5. Poszukiwanie błędów typu SQL Injection będzie odbywać się z użyciem „lekkich" zapytań, niegenerujących w odpowiedzi znacznych ilości danych lub wymagających długiego czasu przetwarzania (tzn. będą unikane zapytania typu „OR 1=1", itp.);

7.6. W przypadku błędów typu Path Traversal/ File Inclusion, pierwszym testem będzie potwierdzenie czy podatność nie usuwa pliku na serwerze;

7.7. W przypadku błędów typu Path Traversal/ File Inclusion, próby będą wykonywane na plikach, które z dużym prawdopodobieństwem mają mały rozmiar, aby zniwelować ryzyko przepełniania pamięci serwera;

7.8. Błędy typu Stored XSS będą testowane w taki sposób, aby były wykonywane tylko na testowych kontach, a nie dotyczyły pozostałych użytkowników systemu.

8. „Raporty z audytu bezpieczeństwa systemów: Broker SI PSZ, CBDC, CBOP, Praca.gov.pl, Wortal PSZ i ZC" Wykonawca przekaże Zamawiającemu w dwóch egzemplarzach w postaci papierowej oraz w dwóch egzemplarzach w postaci elektronicznej np. na płycie CD/DVD. Zamawiający wymaga, aby dokumenty dostarczone np. na płycie CD/DVD były w edytowalnym formacie elektronicznym, np. .doc/ .docx, umożliwiającym swobodne przeszukiwanie treści.

9. Wykonawca zobowiązany jest do zapewnienia wsparcia Zamawiającemu oraz Wykonawcom świadczącym na rzecz Zamawiającego usługi utrzymania i rozwoju systemów: Broker SI PSZ, CBDC, CBOP, Praca.gov.pl, Wortal PSZ i ZC, w celu usprawniania implementacji zmian w systemach teleinformatycznych oraz wprowadzenia zmian konfiguracyjnych w wykorzystywanych przez nie platformach sprzętowo-systemowych, aby doprowadzić do wyeliminowania bądź całkowitej redukcji ryzyk związanych z podatnościami stwierdzonymi w trakcie pierwszego etapu prac, poprzez udzielanie odpowiedzi na pytania zadawane np. za pośrednictwem telefonu lub poczty elektronicznej. Szacuje się, że czasochłonność wsparcia nie powinna przekroczyć 24 roboczogodzin.