ProfiBaza
Narodowy Instytut Zdrowia Publicznego – Państwowy Zakład Higieny
ul. Chocimska 24, 00-791 Warszawa
tel.: 22 54 21 365
email: profibaza-kontakt@pzh.gov.pl
www.profibaza.pzh.gov.pl

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Przeprowadzenie audytu bezpieczeństwa systemu ProfiBaza

1. Kontekst, przedmiot i realizacja zamówienia

Zamawiający realizuje szereg projektów IT. Zgodnie z wymaganiami oraz dobrymi praktykami branżowymi, przewidziany jest audyt bezpieczeństwa systemu IT, obejmujący:

- Testy penetracyjne web aplikacji (frontend i backend),
- Audyt infrastruktury (backend) w obszarze hardeningu urządzeń sieciowych i bezpieczeństwa, które współtworzą audytowany system, w tym audyt architektury sieciowo-systemowej oraz analiza konfiguracji OS i DB;
- Przegląd proceduralny dotyczący instrukcji, polityki, procedur i instrukcji będących składową audytowanego systemu m.in. procedury eskalacji, backupu, instalacji i serwisowania systemu, zgłaszania incydentów przez użytkowników, reakcji na incydenty po stronie obsługi SOC dla audytowanego systemu. Wykonawca wykona audyt istniejących lub opracuje nowe dokumenty;
- Użyteczność (w tym badania UX, dostępności interfejsów użytkownika pod kątem WCAG);
- Jakość i kompletność kodu źródłowego.

Przedmiot zlecenia będzie realizowany w 2 etapach:

- etap I – właściwy audyt bezpieczeństwa,
- etap II – powtórny audyt bezpieczeństwa (retesty) w celu potwierdzenia usunięcia przez Zamawiającego wszystkich podatności oraz słabości audytowanego systemu, wykrytych przez Wykonawcę w trakcie realizacji etapu I.

2. Ogólny opis audytowanego systemu

Założenia w kontekście audytowanego systemu IT:

- możliwość wykonania przez Wykonawcę audytu 24/7,
- praca na środowisku testowym z testowymi danymi,
- audytowany system dostępny z sieci Internet,
- frontend to web aplikacja z ok 10 dynamicznymi elementami (pola wejściowe),
- brak konieczności badania kodu źródłowego audytowanego systemu IT.

3. Charakter i miejsce wykonywanych prac

Przegląd bezpieczeństwa zostanie wykonany poprzez analizę i ocenę dokumentacji, architektury i konfiguracji poszczególnych komponentów oraz bezpośrednio w środowisku informatycznym Zamawiającego w postaci testów penetracyjnych. Testy penetracyjne prowadzone będą metodą „white-box". Audyt będzie wykonywany

Projekt ProfiBaza współfinansowany przez Unię Europejską ze środków EFRR 2014-2020 w ramach POPC nr POPC.02.03.01-00-0015/17-00

ProfiBaza
Narodowy Instytut Zdrowia Publicznego – Państwowy Zakład Higieny
ul. Chocimska 24, 00-791 Warszawa
tel.: 22 54 21 365
email: profibaza-kontakt@pzh.gov.pl
www.profibaza.pzh.gov.pl

zdalnie poprzez sieć Internet oraz na podstawie dostarczonej dokumentacji i wyników działania narzędzi Wykonawcy.

Prace audytowe dotyczące web aplikacji będą wykonywane zgodnie z OWASP Testing Guide. Potencjalne podatności zostaną zaklasyfikowane zgodnie z OWASP TOP 10:

- Injection,
- Broken Authentication and Session Management,
- Cross-Site Scripting (XSS),
- Insecure Direct Object References,
- Security Misconfiguration,
- Sensitive Data Exposure,
- Missing Function Level Access Control,
- Cross-Site Request Forgery (CSRF),
- Using Components with Known Vulnerabilities,
- Unvalidated Redirects and Forwards.

Wszystkie parametry dostępnych formularzy są testowane pod kątem występowania powyższych luk bezpieczeństwa jak i wielu innych znanych typów luk. Dodatkowo analizowane są takie elementy aplikacji webowych jak:

- pliki cookie i inne zasoby składowane przez przeglądarkę,
- nagłówki wysyłane przez serwer,
- elementy RIA aplikacji webowych (pliki SWF, aplety java),
- skrypty javascript,
- czasy odpowiedzi serwera przy poszczególnych operacjach,
- reakcja na dane wejściowe w zapytaniach (nagłówki, agent przeglądarki, wadliwe zapytania protokołu HTTP).

Poniżej przedstawiono uszczegółowiony zakres dla audytu infrastruktury serwerowo-sieciowej:

- Szczegółowej analizie zostanie poddane rozmieszczenie kluczowych systemów IT w poszczególnych strefach bezpieczeństwa,
- Wykonana zostanie identyfikacja występujących słabości otoczenia infrastrukturalnego i zastosowanych zabezpieczeń,
- Szczegółowej analizie zostanie poddana integralność badanej infrastruktury IT z perspektywy bezpieczeństwa,
- Określone zostaną potencjalne wektory ataków na infrastrukturę i wewnętrzne systemy.

Analiza mechanizmów bezpieczeństwa uruchomionych na urządzeniach będzie obejmować:

Projekt ProfiBaza współfinansowany przez Unię Europejską ze środków EFRR 2014-2020 w ramach POPC nr POPC.02.03.01-00-0015/17-00

ProfiBaza
Narodowy Instytut Zdrowia Publicznego – Państwowy Zakład Higieny
ul. Chocimska 24, 00-791 Warszawa
tel.: 22 54 21 365
email: profibaza-kontakt@pzh.gov.pl
www.profibaza.pzh.gov.pl

- Weryfikacji pod kątem poprawnej konfiguracji i skuteczności zostaną poddane wszystkie mechanizmu bezpieczeństwa zaimplementowane na badanym urządzeniu,
- Weryfikacji zostanie poddana obecność nieuruchomionych mechanizmów bezpieczeństwa oferowanych przez urządzenie, a mogących wpłynąć na zwiększenie bezpieczeństwa infrastruktury IT.

Analiza konfiguracji urządzeń sieciowych i bezpieczeństwa:

- Weryfikacji zostanie poddana wersja sytemu operacyjnego pod kątem obecności podatności,
- Weryfikacji zostanie poddana wersja systemu operacyjnego pod kątem dostępności wparcia producenta,
- Weryfikacji zostanie poddana konfiguracja mająca wpływ na zabezpieczenie i wymuszenie bezpiecznego dostępu do badanego urządzenia,
- Weryfikacji zostanie poddana konfiguracja logowania zdarzeń na urządzeniu,
- Weryfikacji zostaną poddane mechanizmy rozliczalności użytkowników,
- Weryfikacji zostanie poddana cała konfiguracja pod kątem występowania zbędnie uruchomionych usług, protokołów i funkcji,
- Weryfikacji zostanie poddana konfiguracja usług, protokołów i funkcji pod kątem ich poprawnej konfiguracji, uwzględniającej najlepsze praktyki bezpieczeństwa,
- Weryfikacji zostanie poddana obecność domyślnej konfiguracji mającej negatywny wpływ na bezpieczeństwo urządzenia, oraz infrastruktury IT.

4. Zespół audytowy Wykonawcy

Kompetencje zespołu Wykonawcy, którego specjaliści będą brać udział w audycie, musi posiadać następujące certyfikaty branżowe:

- Offensive Security Certified Expert (OSCE) lub OSCP,
- Certified Information Systems Security Officer (CISSO) lub CISSP,
- Audytor normy ISO 27001.

5. Metodyka prowadzenia testów bezpieczeństwa i produkt audytu

Zamawiający wymaga, aby Wykonawca przedstawił w ofercie metodykę realizacji testów bezpieczeństwa. Produktem prac będzie raport, tzw. Raport z audytu, składający się z części technicznej oraz części przeznaczonej dla managementu. Część techniczna opisuje szczegółowo znalezione luki wraz z rekomendacją ich załatania. Część zarządcza to wysokopoziomowe podsumowanie dla kierownictwa, w którym znajdują się najważniejsze aspekty prowadzonych prac wraz z rekomendacjami wysokopoziomowymi, jeśli takie występują.

Projekt ProfiBaza współfinansowany przez Unię Europejską ze środków EFRR 2014-2020 w ramach POPC nr POPC.02.03.01-00-0015/17-00