Audyt bezpieczeństwa systemów informatycznych przeprowadzony zgodnie z wymaganiami § 20 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012r w sprawie Krajowych Ramach Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2012r. poz. 526). W ramach audytu należy wykonać między innymi:

Przegląd systemu ochrony technicznej i fizycznej wraz z oceną jego stanu. Przegląd zabezpieczeń danych osobowych na poziomie sprzętowym i oprogramowania. Analizę systemu zarządzania kopiami zapasowymi.Badanie podatności sieci LAN. Zakres zadać obejmuje:

Określenie usług działających w sieci LAN; Weryfikacja mechanizmów ochronnych w warstwie 2 i 3 modelu OSI; Badanie luk w wybranych komputerach, serwerach, urządzeniach sieciowych, podatności na ataki różnych typów (dos, aql, sniffing).

Audyt bezpieczeństwa aplikacji (Sprawdzenie podatności aplikacji na komputerach (w tym serwerów aplikacyjnych i baz danych), próby uzyskania dostępu do panelu administracyjnego za pomocą kont zwykłych użytkowników min. przez: wykorzystanie bieżącej sesji, podniesienie uprawnień, próby uzyskania większych uprawnień, próby uzyskania nieautoryzowanego dostępu do danych znajdujących się w systemie, próby uzyskania nieautoryzowanego dostępu do plików znajdujących się na serwerze/komputerze). Ten punkt ma pokazać czy możliwe jest włamanie się do aplikacji poprzez jej podatności.

Badanie podatności styku LAN/WAN przeprowadzone z zewnątrz sprawdzające odporność urządzeń Zamawiającego na włamania i inne podatności obniżające sprawność działania. Testy bezpieczeństwa VPN (IPsec/SSL). Zakres zadań obejmuje:

Zbadanie poziomu bezpieczeństwa systemów klasy VPN;

Weryfikacja możliwości użycia systemów klasy VPN jako punkt pośredniego do ataku na infrastrukturę IT;Określenie realnego zabezpieczenia komunikacji sieciowej oferowanej przez wdrożoną u Zamawiającego implementację VPN; Próba wykrycia aktywności serwera VPN; Próba wykrycia rodzaju wykorzystywanego rozwiązania VPN (dostawcy sprzętu); Próby inicjowania tunelu z różnymi algorytmami kryptograficznymi (szyfry symetryczne, funkcje skrótu, metoda uwierzytelniania, grupa DH);

Testy socjotechniczne mające na celu pozyskanie loginów i haseł do zasobów lub udostępnienie danych osobowych/poufnych. Testy w postaci mail, telefonów, osobistych rozmów (na wybranej grupie osób). Przeprowadzenie szkolenia dla pracowników (ok 250 osób) z ochrony danych osobowych. Szkolenie przypominające mające na celu utrwalenie podstawowej wiedzy i zasad wynikających z zapisów Polityki ochrony danych osobowych w Wojewódzkim Urzędzie Pracy w Szczecinie- w tym zachowania się w

przypadku podejrzenia wystąpienia incydentu bezpieczeństwa Szkolenie musi również obejmować zagadnienia z bezpieczeństwa wykonywania pracy zdalnej. Omówieniu powinny zostać kwestie bezpieczeństwa danych osobowych przetwarzanych w wersji tradycyjnej, jak i systemach elektronicznych (ochrona hasła, zagrożenia w przypadku wysyłania maili, nie posiadania aktualnego oprogramowania antywirusowego, szyfrowanie). Dokładne tematy i treści szkolenia należy uzgodnić z IOD.

Rezultatem audytu bezpieczeństwa ma być dokument zawierający przyjętą metodologię testów/badań, przedstawienia użytego oprogramowania i sprzętu, wyniki ww. testów i badań oraz określenie poziomu zgodności z KRI. Dokument musi zawierać również wskazanie obszarów w których Zamawiający musi dokonać głębszej analizy, obszary gdzie wymagana jest zmiana procedur, obszary w których Zamawiający spełnia lub nie spełnia założeń KRI.

Rezultatem przeprowadzonych szkoleń ma być aktualizacja wiedzy i praktycznych umiejętności z zakresu ochrony danych osobowych.

Informacje ogólne:

Zamawiający posiada 3 lokalizacje ale wszystkie testy i założenia audytu będą wykonywane jedynie w centrali na ulicy Mickiewicza 41.

Urząd posiada ok 300 hostów w tym 200 komputerów i laptopów, 10 serwerów i 90 pozostałych urządzeń. W centrali jest jedna serwerownia. Mamy wdrożoną Active Directory.

Zamawiający posiada 3 podsieci. Podsieci są spięte ze sobą. Mamy również 2 VLAN’y i 4 sieci bezprzewodowe. Sieci bezprzewodowe nie są objęte audytem. Posiadamy 10 adresów zewnętrznych.