OFERTA

Audyt i usługi doradcze związane z wdrożeniem systemu zarządzania bezpieczeństwem informacji

dla

jednostek administracji publicznej

Klient	**Gmina/Miasto/Starostwo/samorządowe jednostki organizacyjne**
Osoba odpowiedzialna	**.....**
Dostawcy usługi	**TBD MAZOWSZE Sp. z o.o.** ul. Asłanowicza 18 08-110 SIEDLCE NIP 8212264268 REGON 712363817 KRS 0000053292 Sąd Rejonowy dla m.st. Warszawy XIV Wydział Gospodarczy KRS Wysokość kapitału zakładowego 90 000 zł **Audytel S.A.** ks. I. Skorupki 5, 00-546 Warszawa NIP 779-21-69-697 REGON 634288697 KRS 0000309391 Sąd Rejonowy dla m.st. Warszawy XII Wydział Gospodarczy KRS Wysokość kapitału zakładowego 500 112 zł (w całości opłacony)
Osoba odpowiedzialna	Stefan Książek Telefon: (25) 631 14 00, 509 817 817 e-mail: stefan.ksiazek@tbdsiedlce.pl
Data	.....

1. Wstęp

Podmioty realizujące zadania publiczne na podstawie § 20 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektroniczne oraz minimalnych wymagań dla systemów teleinformatycznych zobowiązane są ustanawiać i wdrażać system zarządzania bezpieczeństwem informacji.[1]

Jednym z obowiązków nałożonych przez w/w Rozporządzenie, jak i naturalnym elementem prawidłowo funkcjonującego systemu zarządzania bezpieczeństwem informacji, jest okresowy (roczny) audyt w zakresie bezpieczeństwa informacji.

Zgodnie z wymaganiami prawnymi oraz dobrymi praktykami ochrona informacji, a w szczególności ochrona danych osobowych, wymaga budowy systemu zarządzania bezpieczeństwem informacji.

Celem proponowanych usług jest zapewnienie Klientowi zgodności z wymaganiami prawnymi:

1) Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych oraz wymaganiami norm: PN-ISO/IEC 27001, PN-ISO/IEC 17799, PN-ISO/IEC 27005, PN-ISO/IEC 24762.

2. Audyt systemów informatycznych na zgodność z wymaganiami Rozporządzenia Rady Ministrów z dnia

[1] Treść rozporządzenia mogą Państwo znaleźć pod adresem: (http://isap.sejm.gov.pl/DetailsServlet?id=WDU20120000526)

12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności

1) Analiza systemów informatycznych pod kątem wyposażenia w składniki sprzętowe lub oprogramowanie umożliwiające wymianę danych z innymi systemami teleinformatycznymi za pomocą protokołów komunikacyjnych i szyfrujących określonych w obowiązujących przepisach, normach, standardach lub rekomendacjach ustanowionych przez krajową jednostkę normalizacyjną lub jednostkę normalizacyjną Unii Europejskiej,
2) Analiza zgodności formatów danych w systemach informatycznych z załącznikach nr 2 i 3 do rozporządzenia,
3) Proces zarządzania ryzykiem aktywów informacyjnych – ocena dokonanej przez Klienta inwentaryzacji aktywów informacyjnych, zagrożeń oraz analizy ryzyka,
4) Proces zarządzania identyfikacją i autoryzacją – weryfikacji procesu zarządzania uprawnieniami w systemach informatycznych, ocena sposobu autoryzacji użytkownika, polityka hasłowa,
5) Świadomość pracowników w zakresie bezpieczeństwa informacji – analiza programu szkoleń oraz ocena świadomości użytkowników w zakresie zagrożeń, stosowanych zabezpieczeń oraz odpowiedzialności,
6) Proces zapewnienia odpowiedniego poziomu bezpieczeństwa informacji w systemach informatycznych - ocena stosowanych przez Klienta środków chroniących przed błędami, utratą, nieuprawnioną modyfikacją, analiza zastosowanych mechanizmów kryptograficznych oraz środków bezpieczeństwa dla pracy zdalnej i urządzeń mobilnych oraz weryfikacja zapewnienia odpowiedniego poziomu bezpieczeństwa zgodnie z par 20 pkt 2 ppkt 12 w/w Rozporządzenia,
7) Bezpieczeństwo w relacjach ze stronami zewnętrznymi – analiza umów serwisowych pod kątem zastosowania zapisów gwarantujących bezpieczeństwo informacji,
8) Proces zarządzania incydentami – ocena procedury zgłaszania incydentów, przegląd zgłaszanych w wybranym okresie czasu incydentów oraz ocena podjętych przez Klienta działań naprawczych i korygujących,
9) Proces przygotowania do odtworzenia systemu informatycznego na wypadek katastrofy – weryfikacja istnienia planu odtworzenia techniki informatycznej na wypadek katastrofy, ocena przyjętych w planie założeń oraz wyników testowego odtworzenia,
10) Proces audytu bezpieczeństwa informacji – ocena istniejącego programu audytu oraz sposobu jego realizacji,
11) Proces rozliczalności w systemach informatycznych – weryfikacja zapisach w dziennikach systemów oraz ocena zawartości tych zapisów, ocena sposobu składowania zapisów.

3. Testy podatnościowe (opcjonalne)

1) audyt bezpieczeństwa sieci lokalnej (LAN)
2) audyt bezpieczeństwa zabezpieczeń na styku z Internetem

3) audyt bezpieczeństwa urządzeń sieciowych
4) audyt bezpieczeństwa sieci WiFi
5) audyt bezpieczeństwa systemów operacyjnych, baz danych i aplikacji

Przedmiotem prac jest weryfikacja poziomu bezpieczeństwa elementów infrastruktury informatycznej poprzez przeprowadzenie testów podatnościowych i sprawdzenia prawidłowości konfiguracji oraz przygotowanie raportu z tych prac.

Cele etapu:

1) Przygotowanie i przeprowadzenie w maksymalnie bezinwazyjny sposób testów wszystkich urządzeń aktywnych w podanych zakresach sieci wewnętrznej oraz publicznej (adresy IP należące do Klienta) – dla wszystkich urządzeń aktywnych (router, switch, drukarka sieciowa, koncentrator itp.);
2) Przygotowanie raportu z wykonanych prac, zawierającego listę niezgodności tylko dla tych elementów i komponentów, które wykazują znane podatności związane z bezpieczeństwem informacji.

PROPONOWANE PODEJŚCIE DO REALIZACJI PROJEKTU

W ramach realizacji testów, zostanie przeprowadzony skan każdego adresu IP aktywnego w podanych zakresach podsieci, którego celem będzie:

1) określenie typu/rodzaju urządzenia,
2) wykrycie usług sieciowych udostępnianych na danym urządzeniu,
3) określenie wersji oprogramowania udostępniającego wykryte usługi sieciowe,
4) określenie ewentualnych podatności w działającym na każdym z urządzeń oprogramowaniu, poprzez porównanie zidentyfikowanej wersji oprogramowania z bazami danych o znanych w chwili realizacji testów podatnościach, dotyczących danej wersji oprogramowania czy też danej, udostępnionej w sieci usługi.

GŁÓWNE FAZY PROJEKTU

Niniejsza ekspertyza bezpieczeństwa zostanie podzielona na trzy etapy:

Etap 1

Wykonawca przeprowadzi skany sieciowe, niezbędne do zebrania danych, które w następnych etapach zostaną poddane analizie. Testy powodujące obciążenie systemów zostaną wykonane w dni wolne od pracy - takie podejście zapobiega obciążania testowanych systemów w czasie ich normalnej pracy oraz umożliwia szybszą realizację zadania dzięki relatywnie małemu obciążeniu sieci. Na tym etapie ciężko jest przewidzieć czas trwania testów, gdyż zależy on od wielu czynników (np. szybkość odpowiedzi serwerów, reguły na urządzeniach *firewall*, szybkość sieci).

Etap 2

Dane zebrane w trakcie skanów zostaną uporządkowane i skonfrontowane z bazami danych zawierającymi aktualne dane w chwili przeprowadzania analizy, dotyczące znanych podatności, wpływających na stabilność i bezpieczeństwo badanych systemów.

Etap 3:

Zebrane w trakcie trwania ekspertyzy dane zostaną wykorzystane do opracowania raportu końcowego zawierającego listę komponentów i systemów, w których wykryto podatności.

STOSOWANE STANDARDY

[1] NIST-SP800-115 Technical Guide to Information Security Testing and Assessment,

[2] OWASP (Open Web Application Security Project),

[3] ISAAF (OISSG Penetration Testing Framework),

[4] OSSTMM (Open Source Security Testing Methodology Manual),

[5] PN-ISO/IEC 27001:2007 Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji – Wymagania,

[6] PN-ISO/IEC 17799:2007 Technika informatyczna - Techniki bezpieczeństwa - Praktyczne zasady zarządzania bezpieczeństwem informacji,

[8] PN-I-13335-1:1999 Technika informatyczna - Wytyczne do zarządzania bezpieczeństwem systemów informatycznych - Pojęcia i modele bezpieczeństwa systemów informatycznych,

[9] PN-ISO/IEC 20000-1: 2007 - Technika informatyczna - Zarządzanie usługami - Część 1: Specyfikacja,

[10] PN-ISO/IEC 20000-2: 2007 - Technika informatyczna - Zarządzanie usługami - Część 2: Reguły postępowania.

4. Usługi doradcze związane z wdrożeniem systemu zarządzania bezpieczeństwem informacji

W ramach usług doradczych podczas wdrażania systemu zarządzania bezpieczeństwem informacji (SZBI) proponujemy następujący schemat pracy:

1) Analiza przedwdrożeniowa SZBI:
   a) określenie zakresu i granic SZBI,
   b) określenie ról, odpowiedzialności i uprawnień związanych z bezpieczeństwem informacji,
   c) ocena świadomości użytkowników w zakresie zagrożeń, stosowanych zabezpieczeń oraz odpowiedzialności,
   d) analiza istniejącej dokumentacji i procedur.
2) Zdefiniowanie podejścia do szacowania ryzyka w organizacji:
   a) opracowanie metodyki szacowania ryzyka,

b) kryteria akceptacji i poziom akceptacji ryzyka.

3) Identyfikacja podatności i zagrożeń, szacowanie ryzyka oraz określenie planu postępowania z ryzykiem:
   a) inwentaryzacja aktywów informacyjnych i ich właścicieli,
   b) określenie podatności aktywów informacyjnych,
   c) identyfikacja zagrożeń dla aktywów,
   d) określenie skutków naruszenia bezpieczeństwa
   e) wyliczenie i ocena ryzyk w odniesieniu do poufności, integralności i dostępności informacji,
   f) wybór zabezpieczeń jako środków postępowania z ryzykiem,
   g) przedstawienie wyników analizy i propozycji planu postępowania z ryzykiem do oceny i akceptacji kierownictwa.
4) Wdrożenie i eksploatacja SZBI:
   a) wdrożenie planu postępowania z ryzykiem,
   b) opracowanie polityki bezpieczeństwa opisującej SZBI,
   c) opracowanie szczegółowej dokumentacji bezpieczeństwa – procedury, instrukcje,
   d) wdrożenie zabezpieczeń.
5) Szkolenia z zakresu bezpieczeństwa informacji:
   a) szkolenie kierownictwa,
   b) szkolenia dla pracowników.

5. Warunki handlowe

Warunki handlowe uzależnione są od specyfiki Klienta oraz indywidualnych ustaleń.