

Opis Przedmiotu Zamówienia

Usługi mające na celu przygotowanie PAŻP do spełnienia wymogów z zakresu bezpieczeństwa informacji wskazanych w normach ISO, a w szczególności w normie PN-ISO/IEC 27002.

Przeprowadzenie audytu wykazującego potrzeby PAŻP w zakresie bezpieczeństwa informacji obejmuje następujące obszary:

I. Analiza i inwentaryzacja istniejącej infrastruktury informatycznej we wszystkich komórkach/jednostkach organizacyjnych Zamawiającego, w tym:

1. Serwerownie i obiekty typu Data Center.
2. Architektura w zakresie sieci LAN, SAN, WAN oraz styku z sieciami zewnętrznymi.
3. Produkcyjne serwery fizyczne.
4. Produkcyjne macierze dyskowe.
5. Stacje robocze.

II. Weryfikacja stosowanych zasad bezpieczeństwa informacji pod kątem wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji ISO27001, w tym:

1. Opracowanie zaleceń/wytycznych do Polityki Bezpieczeństwa Informacji.
2. Przegląd prowadzonych analiz ryzyka i sposobu oceny ryzyk informatycznych lub w przypadku ich braku opracowanie wytycznych w przedmiotowym zakresie.
3. Ocena sposobu zapewnienia bezpieczeństwa informacji.
4. Ocena sposobu zarządzania ciągłością działania i bieżącymi operacjami.
5. Ocena zarządzania zasobami.
6. Ocena zaimplementowanych mechanizmów bezpieczeństwa sieci teleinformatycznej i systemów produkcyjnych.

III. Audyt systemu backupu, w tym:

1. Określenie powiązań pomiędzy systemami IT a systemem centralnego backupu.
2. Ocena stopnia spełnienia wymagań biznesowych (krytyczność systemu, RPO, RTO).
3. Audyt architektury systemu składowania danych.
4. Ocena właściwości lokalizacji składowania danych i kopii zapasowych.
5. Ocena procedur i instrukcji.

IV. Ocena zasad eksploatacji systemów IT, w tym:

1. Zarządzanie infrastrukturą IT w poszczególnych obszarach PAŻP posiadających systemy IT.
2. Podejście do cyberbezpieczeństwa.
3. Zarządzanie problemami i incydentami z analizą pokrycia wszystkich obszarów IT.
4. Zarządzanie zmianami w systemach IT i nowymi wydaniem w perspektywie całej organizacji
5. Wsparcie dla użytkowników końcowych (help-desk).

V. Ocena usług zewnętrznych, w tym:

1. Zarządzanie umowami na usługi IT (serwisowe/wsparcia/dostaw usług IT i telekomunikacyjnych) z dostawcami zewnętrznymi (zabezpieczenie obszarów pokryte umowami).
2. Zasady współpracy z firmami zewnętrznymi świadczącymi usługi IT (umowy SLA) oraz kontrola i rozliczenie poziomu tych usług.
3. Obowiązująca polityka i proces pozyskiwania dostawców usług zewnętrznych.
4. Sposób ochrony wiedzy biznesowej/ własności procesów biznesowych.
5. Mechanizmy gwarantowania bezpieczeństwa.

VI. Audyt konfiguracji urządzeń, w tym:

1. Audyt konfiguracji systemów operacyjnych, w tym:
 - a. Systemów typu Windows, Linux, .BSD, AIX, Solaris, HP-UX.

POLSKA AGENCJA ŻEGLUGI POWIETRZNEJ, ul. Wieżowa 8, 02-147 Warszawa, POLSKA;

Telefon: (0 22) 574 50 00, Fax: (0 22) 574 50 09

NIP: 522-283-83-21, Regon: 140886771

www.pansa.pl

- b. Sprawdzenie udostępnionych usług.
- c. Sprawdzenie kluczowych dostępów i uprawnień.
- d. Sprawdzenie mechanizmów aktualizacji oraz logowania zdarzeń.
- e. Hardening systemu.
- 2. Audyt konfiguracji produkcyjnych systemów baz danych, w tym:
 - a. Analiza konfiguracji serwera.
 - b. Sprawdzenie kluczowych dostępów i uprawnień.
 - c. Sprawdzenie polityki haseł.
- 3. Audyt konfiguracji urządzeń sieciowych, w tym:
 - a. Analiza systemów typu Cisco, Brocade, Juniper, HP i innych.
 - b. Analiza konfiguracji reguł bezpieczeństwa.
 - c. Analiza występowania znanych podatności.
 - d. Analiza mechanizmów logowania zdarzeń.
 - e. Przegląd kont użytkowników.
- 4. Audyt konfiguracji urządzeń firewall i innych systemów bezpieczeństwa, w tym:
 - a. Analiza systemów typu CheckPoint, Cisco, Juniper, PaloAlto, Fortigate i innych.
 - b. Analiza reguł i stref bezpieczeństwa.
 - c. Analiza konfiguracji dostępu do urządzeń.
 - d. Analiza konfiguracji reguł bezpieczeństwa np. w zakresie reguł ACL.
 - e. Analiza użytych mechanizmów kryptograficznych.
 - f. Przegląd kont użytkowników.

VII. Testy penetracyjne wybranych systemów, w tym:

- 1. Testy typu black-box.
- 2. Testy typu grey-box.
- 3. Testy typu white-box.
- 4. Testy wewnętrznej sieci WiFi, w tym:
 - a. Wykrycie dostępnych sieci.
 - b. Określenie zastosowanych mechanizmów i próby przełamania zabezpieczeń.
 - c. Ocena zasad dostępu do urządzeń.
- 5. Testy kontrolera domeny AD, w tym:
 - a. Próby eskalacji uprawnień.
 - b. Próba pozyskania danych uwierzytelniających.
 - c. Ataki na SMB.
 - d. Próby wyszukania użytkowników z wysokimi uprawnieniami.
 - e. Próby wydobycia skrótów haseł.

VIII. Opracowanie zaleceń w zakresie stosowanych mechanizmów zapewnienia ciągłości działania (BCP) i odtwarzania po katastrofie (DRP), w tym:

- 1. Wytyczne/opracowanie dokumentacji niezbędnej w przedmiotowym zakresie.
- 2. Wytyczne/opracowanie polityki dotyczącej ciągłości działania.
- 3. Wytyczne/opracowanie planów odtwarzania utraconych zasobów.
- 4. Wytyczne/opracowanie procedur kontroli środowiska informatycznego.