Z Polityki Bezpieczeństwa

ROZDZIAŁ III Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przy przetwarzaniu danych

1 Zabezpieczenia serwerowni:

1.1 Systemy zarządzania budynkiem:

- Monitoring budynku: Centralny system monitoringu CCTV, kontrola 24/7/365
- Systemy alarmowe: Wszystkie systemy alarmowe monitorowane 24/7/365
- Ochrona fizyczna: Obiekt zamknięty, ogrodzony, strzeżone wejścia dostępowe oraz strefa dostaw wraz z magazynem.

1.2 Łączność:

- Okablowanie zewnętrzne:
  Bezpośredni styk z sieciami szkieletowymi wiodących operatorów telekomunikacyjnych (międzynarodowych Tier 1 i krajowych); niezależne, redundantne linie światłowodowe doprowadzone z różnych stron serwerowni.
- Dostępni operatorzy: operatorzy klasy Tier 1: Cogent, Level3, Interoute, Kaia Global Networks, NTT Communications, RETN, TeliaSonera i wszyscy kluczowi operatorzy krajowi
- Punkt wymiany ruchu: Poznański Punkt Wymiany Ruchu Internetowego PIX

1.3 Zasilanie:

- Standard: Tier III (rating III wg ANSI/TIA-942)
- Zasilanie: 800kVA
- Dystrybucja energii: Do każdej szafy niezależne obwody zasilania gwarantowanego UPS 230 V / 400 V z niezależnych torów zasilających
- Gęstość zasilania: do 25 kW na szafę. Inne obwody dostępne na życzenie klienta; Dwie pionowe listwy zarządzalne zasilające PDU 0U 32A po jednej na każdym torze zasilania
- Systemy zasilania awaryjnego: systemy UPS
- Generator prądotwórczy:
  agregat prądotwórczy, zbiorniki paliwa z zapasem na 24h, z możliwością uzupełnienia w trakcie pracy agregatu

1.4 Kontrola środowiskowa:

- Standard: Tier III (rating III wg ANSI/TIE-942)
- Chłodzenie: Klimatyzatory z redundancją N+1, układ ciepłych i zimnych korytarzy,
- Temperatura: 23st.C (+-3st.)
- Wilgotność względna: wilgotność 55% (+-10%)

1.5 Ochrona przeciwpożarowa:

- Systemy przeciwpożarowy:
  System detekcji pożaru w oparciu o czujniki multisensorowe optyczno-temperaturowe oraz system wczesnej detekcji dymu VESDA
- System Gaśniczy:
  Automatyczny system tłumienia ognia: dwustrefowo – pod i nad podłogą techniczną; instalacja gasząca certyfikowana do użytku w UE.

1.6 Ochrona:

- Systemy ochrony:
  Monitoring CCTV, kontrola 24/7/365; System strefowej kontroli dostępu oparty na kartach zbliżeniowych oraz zamkach biometrycznych; wizyty gości w eskorcie służb obiektu; lista osób uprawnionych do dostępu wejścia na teren obiektu, śluzy dostępowe.
- Usługi w systemie 24/7/365:
  Pracownicy ochrony monitorujący cały obiekt, monitoring CCTV, Centrum Zarządzania Siecią (NOC), Całodobowa obsługa techniczna dwóch zespołów: infrastruktura i technologia.

2 Środki sprzętowe, infrastruktury informatycznej i telekomunikacyjnej oraz narzędzia programowe i baz danych zastosowane w celu ochrony danych osobowych

2.1 Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.

2.2 Użyto systemu firewall do ochrony dostępu do sieci komputerowej.

2.3 Zastosowano system rejestracji dostępu do systemu informatycznego.

2.4 Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji

2.5 Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych.

2.6 Dostęp do systemu informatycznego wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.

2.7 Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego w przypadku dłuższej nieaktywności pracy użytkownika.

2.8 Zbiór danych osobowych przetwarzany jest przy użyciu komputerów przenośnych.

2.9 Zastosowano urządzenia UPS chroniące system informatyczny przed skutkami awarii zasilania.

3 Środki organizacyjne zastosowane w celu ochrony danych osobowych

3.1 Osoby przetwarzające dane osobowe zostały:

3.1.1 zaznajomione z przepisami dotyczącymi ochrony danych osobowych,

3.1.2 przeszkolone w zakresie zabezpieczeń systemu informatycznego,

3.1.3 upoważnione do przetwarzania danych osobowych

3.1.4 zobowiązane do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczania.

3.2 Zenbox Sp. z o.o. prowadzi rejestr osób upoważnionych.

3.3 Wdrożona została dokumentacja dotycząca ochrony danych osobowych: polityka bezpieczeństwa danych osobowych oraz instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

3.4 Zenbox Sp. z o.o. przeprowadza regularne przeglądy polityki bezpieczeństwa danych osobowych oraz instrukcji zarządzania systemem informatycznym.

3.5 Przekazywanie danych osobowych do podmiotów trzecich (udostępnianie i powierzanie) jest nadzorowane oraz odbywa się na zasadach zgodnych z przepisami prawnymi.