VULCAN
ZARZĄDZANIE OŚWIATĄ

Informacja o zabezpieczeniach danych, przechowywanych i przetwarzanych w systemach hostowanych oferowanych przez VULCAN sp. z o. o.

Systemy hostowane oferowane przez VULCAN Sp. z o.o. zapewniają bardzo wysoki poziom bezpieczeństwa danych, dzięki zastosowaniu szeregu zabezpieczeń. W szczególności wypełniają one wymagania nakładane przepisami prawa na systemy przetwarzające dane osobowe. Poniżej zostały ogólnie opisane najważniejsze z tych zabezpieczeń.

Zabezpieczenia fizyczne urządzeń

Wszystkie urządzenia służące do przetwarzania danych zabezpieczone są fizycznie przed kradzieżą, uszkodzeniem i dostępem osób nieupoważnionych. Zabezpieczenia fizyczne obejmują między innymi:

- konstrukcję budynku, w którym zlokalizowana jest serwerownia, zapewniającą ochronę przed powodzią i zalaniem z góry,
- zabezpieczenia mechaniczne dostępu do pomieszczeń (ściany, drzwi antywłamaniowe, zamki),
- ograniczenie dostępu do pomieszczeń wyłącznie do osób upoważnionych,
- ewidencjonowanie osób wchodzących do pomieszczeń,
- całodobowy monitoring,
- całodobową ochronę,
- system przeciwpożarowy.

Zabezpieczenia integralności danych

Zabezpieczenie integralności danych jest realizowane za pomocą technik i narzędzi programistycznych oraz rozwiązań serwerowych, które gwarantują integralność danych. Ponadto zabezpieczenie integralności danych jest realizowane również przez wewnętrzną politykę bezpieczeństwa i zasady realizacji operacji na danych klientów (w szczególności na przykład pełna dokumentacja operacji usuwania danych, odtwarzania kopii itp.).

Zabezpieczenie dostępu do danych

Dostęp do danych zabezpieczony jest wielopoziomowo, między innymi z wykorzystaniem:

- szyfrowania komunikacji między stacją użytkownika a serwerem (m.in. przy użyciu SSL),
- realizacji dostępu administracyjnego do zarządzania infrastrukturą serwerową z wykorzystaniem VPN między centralą firmy a serwerownią,
- stosowaniem zapór ogniowych (tzw. firewall) separujących obszary infrastruktury i chroniących jej istotne elementy przed potencjalnymi atakami z zewnątrz,

- ograniczenie dostępu do danych na serwerach wyłącznie do uprawnionych osób, koniecznych do właściwej realizacji usług,
- stosowanie mechanizmów kontroli dostępu do danych, w szczególności stosowanie regularnie zmienianych haseł o dużym stopniu skomplikowania.

Zabezpieczenie ciągłości dostępu do danych

Zabezpieczenie ciągłości dostępu do danych realizowane jest w szczególności poprzez:

- zabezpieczenie zasilania serwerowni z co najmniej dwóch niezależnych źródeł,
- stosowanie urządzeń podtrzymujących napięcie na wypadek chwilowego zaniku zasilania,
- zapewnienie podłączenia infrastruktury do Internetu za pośrednictwem co najmniej dwóch niezależnych dostawców,
- zapewnienie dublowania nośników przechowujących dane (np. tzw. mirrory dysków),
- zapewnienie dublowania wybranych elementów infrastruktury logicznej, w szczególności na przykład poprzez zdublowane kluczowe elementy infrastruktury LAN,
- zapewnienie dublowania wybranych elementów infrastruktury fizycznej, w szczególności na przykład poprzez równolegle funkcjonujące serwery aplikacyjne.

Zabezpieczenie na wypadek awarii

Zabezpieczenie na wypadek awarii realizowane jest w szczególności poprzez:

- regularne wykonywanie kopii zapasowych danych,
- przechowywanie wykonanych kopii zapasowych danych w bezpiecznych lokalizacjach,
- wykonywane regularnie testy infrastruktury zapasowej, przywracanej po symulowanej awarii infrastruktury podstawowej.