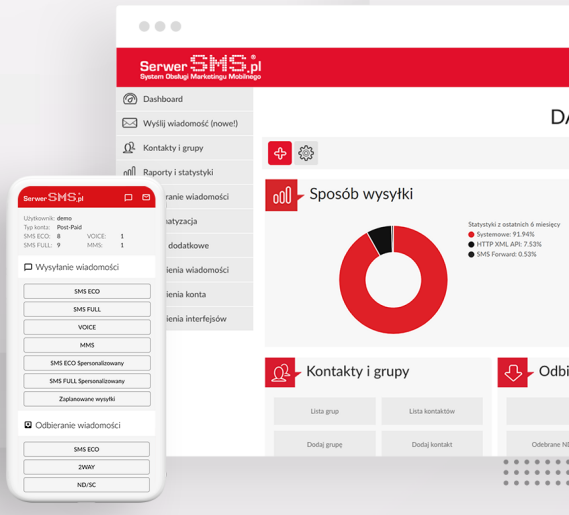
Serwer SMS.pl®
System Obsługi Marketingu Mobilnego

Opis zastosowanych środków technicznych i organizacyjnych



Opis zastosowanych środków technicznych i organizacyjnych

Wstęp

Zgodnie z art. 30 ust. 2 RODO każdy podmiot przetwarzający jest zobowiązany do rejestrowania wszystkich kategorii czynności przetwarzania i w tym cel prowadzi dedykowany rejestr. W rejestrze tym zamieszcza się m. in., jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa w zakresie a) pseudonimizacji i szyfrowania danych osobowych; b) zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania; c) zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego; d) regularnego testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Wykaz środków technicznych i organizacyjnych służący do zapewnienia bezpieczeństwa przetwarzania danych osobowych w biurach operacyjnych:

Środki ochrony fizycznej:

- monitoring wizyjny,
- systemy alarmowe,
- nadzór służby ochrony,
- recepcja,
- czujniki przeciwpożarowe,
- czujniki dymu,
- gaśnice lub automatyczne systemy gaszenia,
- zamykane pomieszczenia biurowe,
- zamykane szafy i szafki,
- system kontroli dostępu,
- niszczarki dokumentów,

Środki bezpieczeństwa teleinformatycznego:

- dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła
- zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych
- zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych
- zastosowano mechanizmy wymuszające użycia hasła o odpowiedniej złożoności,
- zastosowano wygaszacze ekranów
- zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika
- zastosowano środki ochrony przed szkodliwym oprogramowaniem
- użyto system firewall do ochrony dostępu do sieci komputerowej
- zastosowano systemy IDS/IPS
- zastosowano szyfrowanie nośników danych w tym w szczególności dysków w komputerach przenośnych
- zastosowano szyfrowanie teletransmisji
- użyto system zdalnego zarządzania urządzeniami mobilnymi w szczególności telefonami komórkowymi
- wykonywane są kopie zapasowe
- zastosowano szyfrowanie dysków urządzeń drukujących
- zastosowano wydruki personalne na sieciowych urządzeniach drukujących
- wykonywana jest aktualizacja aplikacji i systemów operacyjnych

Środki organizacyjne:

- Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych
- Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego

- Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy
- Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane
- Wdrożono politykę ochrony danych osobowych
- Przeprowadzane jest regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych (audyt)
- Stosowana jest zasada rozliczalności działań mająca na celu wykazanie, że dokonywane są czynności administracyjne związane z zapewnieniem bezpieczeństwa
- Prowadzona jest inwentaryzacja sprzętu przetwarzającego dane osobowe
- Ewidencjonowane są incydenty dot. bezpieczeństwa danych osobowych

CENTRUM DANYCH
Wykaz środków technicznych i organizacyjnych służący do zapewnienia bezpieczeństwa przetwarzania danych osobowych dotyczący serwerów dedykowanych, na których jest utrzymywana główna aplikacja (Outsourcingowe centrum danych).

Środki ochrony fizycznej danych:

- centrum danych znajduje się na terenie biurowca z całodobową ochroną zapewnianą przez właściciela
- po godzinach pracy biur budynek jest zamykany
- wejście na teren dostawcy (I strefa – całe piętro budynku z wyłączeniem klatki schodowej)
- chronione jest drzwiami otwieranymi kartą magnetyczną
- wejście do obszaru przetwarzania danych (II strefa - centrum danych) chronione jest drzwiami otwieranymi kartą magnetyczną
- karty magnetyczne umożliwiające dostęp do I strefy posiadają wszyscy pracownicy dostawcy posiadający umowę o pracę, dostęp do II strefy posiadają wyłącznie pracownicy działów technicznych posiadający odpowiednie upoważnienie
- każde wejście, zarówno do I jak i II strefy, jest logowane
- zarówno I, jak i II strefa objęte są systemem alarmowym
- teren dostawcy objęty jest systemem wideo monitoringu
- wszystkie pomieszczenia centrum są wyposażone w czujniki ruchu podłączone do głównego systemu alarmowego
- wszystkie pomieszczenia centrum są wyposażone w czujniki przeciwpożarowe podłączone do głównego systemu alarmowego

Środki sprzętowe, informatyczne i telekomunikacyjne (nazwy zwyczajowo przyjęte albo symbole norm lub standardów technicznych):

- serwery typy RACK z procesorami Intel Xeon 3060 lub wyższe
- karty sieciowe typu GBEthernet,
- router z oprogramowaniem firewall,
- switche typu Nortel 5520-48T
- UPS typu on-line 30kVA
- Agregat prądotwórczy z SZR 130kVA
- klimatyzacja pomieszczeń zapewniająca odpowiednią temperaturę pracy urządzeń

Środki ochrony w ramach oprogramowania urządzeń teletransmisji (nazwy zwyczajowo przyjęte albo symbole norm lub standardów technicznych):

- Technologia: SSLv3, TLSv1.2 - Aplikacje: openssl, vsftpd, apache+mod_ssl, stunell
- Technologia: SSHv2 - Aplikacje: openssh
- transmisja danych odbywa się szyfrowanym protokołem
- ograniczony dostęp do urządzeń teletransmisji: identyfikatorem i hasłem, które składa się minimum z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne
- firewall

Środki ochrony w ramach oprogramowania systemów (nazwy zwyczajowo przyjęte albo symbole norm lub standardów technicznych):

<u>Środki zabezpieczenia systemu serwera:</u>

- system użytkowników systemu linux
- system praw dostępu systemu linux
- ograniczenie dostępu do poziomu poleceń systemowych w zależności od stanowiska pracy,
- oprogramowanie monitorujące pracę serwera (własna implementacja)
- codziennie, automatycznie tworzone są kopie zapasowe

Środki zabezpieczenia systemu serwera www:

- system użytkowników systemu linux (aplikacja działa na wydzielonym użytkowniku
- systemowym)
- system praw dostępu systemu linux
- oprogramowanie monitorujące pracę serwera (własna implementacja)
- codziennie, automatycznie tworzone są kopie zapasowe
- logi dostępu do usługi
- pełna separacja środowiska serwera (serwer www jest odizolowany od innych serwerów)

Środki zabezpieczenia systemu poczty elektronicznej:

- zainstalowane oprogramowanie antywirusowe dla poczty przychodzącej/wychodzącej
- codziennie, automatycznie tworzone są kopie zapasowe
- oprogramowanie monitorujące pracę serwera (własna implementacja)
- logi dostępu do usługi
- system użytkowników/haseł (3 poziomowy dla konta email, domeny i konta użytkownika)

Środki zabezpieczenia systemów baz danych:

- system praw dostępu oraz użytkowników silnika serwera baz danych (mysql/postgresql)
- całkowity brak dostępu do poleceń systemowych w środowisku pracy serwera
- codziennie, automatycznie tworzone kopie zapasowe
- logi zmian danych
- pełna separacja środowiska serwera (serwer baz danych jest odizolowany od innych serwerów)
- oprogramowanie monitorujące pracę serwera (własna implementacja)

Środki zabezpieczenia systemów DNS:

- całkowity brak dostępu do poleceń systemowych w środowisku pracy serwera
- codziennie, automatycznie tworzone kopie zapasowe
- logi zmian danych
- pełna separacja środowiska serwera (serwer DNS jest odizolowany od innych serwerów)
- oprogramowanie monitorujące pracę serwera (własna implementacja)

Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych (nazwy zwyczajowo przyjęte albo symbole norm lub standardów technicznych), uzaleznione od Klienta.

Lista używanego oprogramowania zawiera między innymi:

- apache
- linux
- apache-mod_ssl
- mysql
- postgresql
- openssl
- vsftpd
- openssh
- qmail
- courier-imap
- php, perl, python, bash

Środki organizacyjne:

- dostęp do danych posiadają wyłącznie upoważnieni i odpowiednio przeszkoleni pracownicy
- wyznaczony została osoba nadzorująca przestrzeganie zasad ochrony przetwarzanych danych osobowych,
- pracownicy mający dostęp do zbiorów danych zostali zaznajomieni z powszechnie obowiązującymi przepisami dotyczącymi ochrony danych osobowych,
- prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych,
- kopie zapasowe przechowywane są w sejfie.

APLIKACJA GŁÓWNA
Wykaz środków technicznych i organizacyjnych służący do zapewnienia bezpieczeństwa przetwarzania danych osobowych dotyczący aplikacji (Autorskie oprogramowanie w modelu SaaS)

Środki techniczne:

- Konfigurowalna polityka zarządzania haseł np. brak możliwości użycia przez miesiąc czasu tego samego hasła dla opcji z hasłem zmiennym i trudnym,
- Regularne testy penetracyjne w standardzie OWASP
- W przypadku 10-ciu nieudanych prób logowania do aplikacji, blokada możliwości logowania na 30 minut,
- Trzy możliwe stopnie zabezpieczeń logowania do Panelu Klienta, do wyboru wg zapotrzebowań Abonenta (proste hasło, trudne hasło z wymuszoną zmianą lub dodatkowa autoryzacja kodem z SMS)
- Bezpieczne szyfrowane połączenie HTTPS szyfrowane certyfikatem SSL przy logowaniu oraz przy wykonywaniu operacji w aplikacji.
- Możliwość ograniczenia zakresu IP dla logowania do aplikacji oraz API,
- Powiadomienia o udanych i nieudanych próbach logowania do aplikacji oraz API,
- Dostęp ograniczany jest wg zalogowanej sesji użytkownika,
- Wszystkie operacje na danych osobowych są logowane w historii operacji,
- Możliwość samodzielnej edycji danych na koncie oraz oznaczania zgód na np. mailingi informacyjne,
- Możliwość ograniczania uprawnień do widoku oraz operacji w zakresie tworzonych subkont w systemie,
- Każdy dodatkowy użytkownik może mieć osobny, indywidualny login i hasło do systemu, aby identyfikować osobę zalogowaną oraz wykonywane przez nią zmiany i operacje,
- Automatyczne mailowe potwierzenia w momencie zmiany danych wysyłane drogą elektroniczną,
- Możliwość zestawienia tunelu ipsec/VPN z systemem np. na potrzeby połączeń do API.
- Automatycznie tworzony backup aplikacji i bazy danych z poziomu serwera.

Środki organizacyjne

- Uwzględniana jest ochrona danych osobowych w fazie projektowania i domyślnej ochrony danych osobowych,
- Został wyznaczony właściciel biznesowy aplikacji,
- Realizowany jest stały nadzór nad aplikacją,
- Wykonywane są regularne przeglądy aplikacji i jej aktualizacja,
- Prowadzony jest changelog wykonywanych poprawek i aktualizacji,
- Poprzez system realizowana jest procedura zgłaszania ewentualnych błędów.

BACKUPY I KOPIE ZAPASOWE
Zestaw ogólnych zasad dotyczących bezpieczeństwa kopii zapasowych głównej aplikacji

Kopie wykonywane są w codziennie (pełne) w ramach usługi profesjonalnej i obejmują wszystkie dane na serwerach dedykowanych obsługujących aplikację, konfigurację oraz bazy danych.

Szczegóły:

- Dane przechowywane są w tej samej serwerowni,
- dane przechowywane są na innym serwerze poza serwerem produkcyjnym,
- dostęp do serwera ma wydzielona liczba pracowników,
- dane dostępne są do 31 dni wstecz,
- system kopii wykonywany jest w trybie inceremental-forever,
- wykonywane są pełne kopie baz danych codziennie w formie SQL oraz backup całego serwera baz danych, dane są przechowywane w trybie 4x4, tj 4 dni wstecz plus po jednej kopii z ostatnich 4 tygodni,
- dane z backupu dostępne są przez system udostępniania danych z backupu w trybie 4x4 (4 dni wstecz oraz 4 x w tygodniu) w trybie tylko do odczytu po wcześniejszym zgłoszeniu przez panel administracyjny serwera.

Szczegóły:

- Kopia wykonywana jest codziennie 1:1 dla baz i plików,
- jest synchronizowana z serwerami,
- synchronizacja danych w wyznaczonych lokalizacjach na serwerze źródłowym i aktualizacja plików na docelowym,

- synchronizacja wykonywana jest wykonywana minimum raz na 24 godziny i odbywa się automatycznie.

INFORMACJE DODATKOWE
Informacje ogólne oraz dokumentacja dodatkowa

- Lokalizacje serwerowni zostały opisane w załączniku nr 4 do Umowy Powierzenia Danych.
- Posiadamy bezpośrednie połączenia ze wszystkimi Polskimi Operatorami GSM (Plus, Play, Orange oraz T-mobile) które zabezpieczone są przez tunele VPN/IPSEC.
- Nasze rozwiązanie pozwala na wysyłkę wiadomości SMS, MMS, VMS, VIBER, Push oraz odbiór wiadomości SMS, MMS, VIBER. Dostępna jest również możliwość sprawdzenia numeru (HLR, LOOKUP oraz NAT).
- System umożliwia wysyłkę w jednym czasie wiadomości SMS z szybkością kilkaset na sekundę, a pojedyncze konto ma ustawioną szybkość na poziomie 50-100 SMS/sek.

Dokumenty i informacje dodatkowe

- Ogólna specyfikacja techniczna: https://serwersms.pl/dokumenty/125-specyfikacja-techniczna
- Nasza usługa jest realizowana w oparciu o model samoobsługowy CPaaS https://panel.serwersms.pl/logowanie
- Istnieje możlliwość integracji metodą REST API, SMPP, SQL API, SMS przez FTP, email2sms itd. dokumentacja techniczna https://dev.serwersms.pl/
- Dokumentacja związana z bezpieczeństwem danych:
  Opis ogólny: https://serwersms.pl/bezpieczenstwo
  Certyfikat testów penetracyjnych OWASP https://serwersms.pl/dokumenty/118-certyfikat-owasp
- Informacje na temat Certyfikatu ISO 27001 https://serwersms.pl/dokumenty/139-ISO27001SerwerSMS
- Prezentacja usługi https://serwersms.pl/dokumenty/1-prezentacja