Bezpieczeństwo

Prawdopodobnie najbezpieczniejszy system komunikacji SMS w kraju. Bezpieczeństwo na 5 gwiazdek!

W projekcie SerwerSMS.pl stale pracujemy nad udoskonaleniem działań platformy. Chcemy, by każdy, kto korzysta z serwisu, był maksymalnie zadowolony z narzędzi do komunikacji SMS. Chcemy, by użytkownik był przekonany, że przechowywane dane są chronione przez cały czas. Wysoka jakość usług, to dla nas priorytet, czego dowodem są międzynarodowe certyfikaty bezpieczeństwa oraz współpraca z najlepszymi dostawcami usług.

ISO 27001
LL-C (Certification)

Mamy certyfikat ISO 27001

Otrzymaliśmy Certyfikat od Międzynarodowej Organizacji Normalizacyjnej (ISO). ISO To organizacja pozarządowa i całkowicie niezależna, a jej członkowie nie są delegowani przez rządy.

Bardzo nam miło poinformować, że spółka Vercom S.A (SerwerSMS.pl) pozytywnie przeszła audyt certyfikacyjny Systemu Zarządzania Bezpieczeństwem Informacji według normy ISO/IEC 27001:2013, do prowadzenia działalności w zakresie: “Tworzenie, utrzymanie i rozwój rozwiązań komunikacji elektronicznej, w tym email i sms w modelu SaaS. Certyfikat ISO 27001, jest jednym z bardziej uznanych standardów zarządzania biznesem. Potwierdza to, że ochrona informacji w naszym serwisie spełnia najwyższe standardy bezpieczeństwa. Audyt w naszej firmie przeprowadziła jednostka LLC-(Certification) Czech Republic a.s z Pragi.

Pobierz ISO 27001

RODO READY

Jesteśmy zgodni z RODO!

To, co warto podkreślić na samym początku to informacja, że nasza spółka przeszła szczegółowy audyt systemu zarządzania bezpieczeństwem informacji. Można powiedzieć, że jesteśmy RODO ready.

Nasi pracownicy zostali przeszkoleni w kontekście nowych zasad bezpieczeństwa, Na każdym koncie klienta uruchomiliśmy tzw. Kartę powierzenia, która jest swego rodzaju centrum zarządzania powierzonymi danymi. Przez Kartę powierzenia można między innymi w prosty sposób określić zakres powierzonych danych i zawrzeć z nami odpowiednią umowę. Umieszczono tam dokumenty opisujące nasze zabezpieczenia oraz wprowadzono kilka funkcjonalności pozwalających naszym klientom, czyli Administratorom Danych, zarządzać swoimi danymi oraz prowadzić odpowiednie rejestry.

Jednocześnie należy podkreślić, że rozporządzenie RODO wymusza ciągłe doskonalenie i jest nieskończonym procesem, którego nie można zakończyć, dlatego nasza firma wprowadziła odpowiednie procedury, które mają na celu ciągłe doskonalenie.

Co konkretnie zmieniło się w dokumentacji:

Dokumentacja procesora dotycząca powierzonych danych

- Zgodnie z RODO, każdy Administrator Danych Osobowych, czyli firma będąca naszym klientem musi zawrzeć z procesorem danych, czyli z naszą firmą, UMOWĘ POWIERZENIA DANYCH. Jest to bardzo ważny dokument regulujący wiele kwestii związanych z bezpieczeństwem danych. Umowę powierzenia można zawrzeć podczas zakładania konta przez tzw. Kartę powierzenia. Draft dokumentu można pobrać również z naszej strony dokumenty, niemniej dla usprawnienia tego procesu zachęcamy do skorzystania z naszej „Karty powierzenia" i przejście procesu zawarcia umowy powierzenia w naszym systemie.

Dokumentacja Administratora

- Wprowadziliśmy kilka zmian w naszych dokumentach opisujących zasady korzystania z usługi: polityka prywatności, polityka cookies, regulamin. Pojawił się również nowy dokument Klauzula Informacyjna, która określa dokładnie, w jakich celach zbierane są dane, a także szczegóły ich przechowywania.

Bezpieczeństwo Klientów to klucz!

Zgodnie z przepisami RODO procesor, czyli nasza firma, ma obowiązek zapewnić pełne bezpieczeństwo danych. W związku z tym wprowadzamy nowe działania i procedury w tym m.in.:

- Dodatkowe zabezpieczenia związane z wyborem i zmianą hasła do Panelu Klienta.
- Kadra zobligowana została do podpisania oświadczeń o zachowaniu tajemnicy danych osobowych,
- Dzięki rozwiązaniom technicznym system zapewnia poufność, integralność, dostępność i odporność systemów i usług przetwarzania,
- W przypadku przyczyn losowych zapewnia możliwość szybkiego przywrócenia danych osobowych i dostępu do nich.
- Regularnie testujemy, mierzymy i oceniamy skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.
- Współpracujemy jedynie z zaufanymi partnerami!
- Odpowiednie środki techniczne zapewnią prawo do „bycia zapomnianym".

? Wysyłki realizowane przez bezpośrednie połączenie z Operatorami!

Jako najstarsza firma z branży uruchomiliśmy taki rodzaj połączeń już wiele lat temu. Bezpośrednie połączenie do komunikacji z Operatorami (DCSMS), to najwyższym standardem w komunikacji SMS

Dzisiaj możemy zagwarantować realizację usług we współpracy z wszystkimi operatorami infrastrukturalnymi w naszym kraju. Oznacza to, że ??jesteśmy w stanie uniknąć wysyłania wiadomości poprzez wielu pośredników. Jest to najbezpieczniejszy i zdywersyfikowany rodzaj komunikacji dostępny na rynku SMS A2P. Z racji tego, że krótkie wiadomości tekstowe kierowane są przez bezpośrednie połączenia, kanał ten możemy nazwać "kanałem komunikacji bez przeszkód" oraz "bez luk" w zakresie bezpieczeństwa, które w ostatnim czasie nabierają coraz większego znaczenia. Zapraszamy również do zapoznania się z naszym komentarzem do najnowszego raportu na temat bezpieczeństwa komunikacji oraz istoty bezpośredniego połączenia z Operatorami. Poniżej przedstawiamy argumenty, dlaczego ten temat jest tak istotny.

Bezpieczeństwo

Operatorzy GSM oraz Provider SMS współpracujący na bezpośrednim połączeniu, na bieżąco monitorują wysyłki i mogą panować niemal w 100% nad jakością i źródłem danych. Jeżeli zależy Ci na tym, aby Twoje wiadomości SMS były dostarczone sprawnie, szybko i bezpieczenie wraz z informacją o ścieżce wysyłki, to taki sposób realizacji usługi jest najlepszym wyborem, a bezpieczeństwu Twojej kampanii nic nie może zagrozić.

Dostarczalność

Ponieważ wiadomości SMS są wysyłane natychmiast do Operatorów komórkowych, znacząco skraca się czas i skuteczność dostarczenia. Z tego względu szybkość dostarczania będzie znacznie wyższa niż w przypadku, gdyby były one przesyłane pośrednim kanałem. Mimo że bezpośrednie połączenia jest nieco droższe niż te pierwsze, to niezawodność i jakość kanału jest dużo wyższa.

Gwarantowana nazwa nadawcy

W przypadku bezpośredniego połączenia można mieć pewność, że zdefiniowana alfanumeryczna nazwa nadawcy będzie wyświetlona u odbiorcy, w taki sposób jak to zostało wcześniej ustawione.

Raporty doręczenia wiadomości

Połączenia bezpośrednie gwarantują pełny dostęp do raportów po każdej zrealizowanej kampanii. W przypadku słabej jakości kanału takiej możliwości może nie być, może być realizowane w ograniczonym stopniu, lub być zafałszowana. liczba doręczonych wiadomości będzie inna niż wskazana w statystykach. Jeżeli korzystasz z serwisu, który posiada DCSMS, dostarczanie SMS-ów są niezawodne i z pełnym raportowaniem.

Dywersyfikacja

Kluczowe dla wysyłek szczególnie z powiadomieniami jest ciągłość w działaniu usługi, dlatego bezpośrednie połączenie gwarantuje, że w przypadku awarii jednego z Operatorów GSM w 99% przypadków provider SMS może niezauważalnie przełączyć się na innego Operatora infrastrukturalnego, bez konieczności radzenia sobie z przestojem w wysyłce.

Pobierz wyd. 6 raportu CERT Orange

OWASP TOP 10 2018 veryfied by TestArmy

Przeszliśmy testy bezpieczeństwa OWASP

Aby być bezpiecznym, należy dać się zhakować...! Trzeba w tym miejscu zaznaczyć, że musi się to odbywać w warunkach kontrolowanych, aby odkryć wszystkie newralgiczne miejsca, które potencjalnie narażone są na napaść cyberprzestępców.

Czym w zasadzie jest OWASP? OWASP to międzynarodowy standard badania bezpieczeństwa serwisów i powierzonych tam danych. Są to testy bezpieczeństwa, a konkretnie testy penetracyjne, posługujące się metodą OWASP ASVS, czyli Application Security Verification Standard. Dzięki testom penetracyjnym można wykryć potencjalne podatności, które mogłyby zostać wykorzystane przez atakujących – tłumaczy Dawid Bałut. Te „potencjalne podatności" są niczym innym jak „dziurami w płocie", narażającymi firmę na niebezpieczeństwo, a testy penetracyjne mają za zadanie sprawdzić, czy złodziej przez taką dziurę może się przemknąć na teren firmy. Serwer, aplikacja, czy strona internetowa firmy poddawana jest sterowanemu atakowi hakerskiemu, który weryfikuje czy zabezpieczenia są wystarczająco mocne, by powstrzymać cyberprzestępców i wskazuje miejsca, które mogą potencjalnie stać się celem ataku.

Pobierz Certyfikat OWASP

TARCZA CPT

Tarcza CPT

Pierwszy w kraju system ochrony komunikacji SMS, działający jako Anty-spam i Anty-phishing!

Customer Protection Tool to najwyższej jakości narzędzie do ochrony Twojego kanału komunikacji SMS. System stworzyliśmy z myślą o reagowaniu na potencjalne zagrożenia. Wyłudzenie danych czy podszywanie się pod brand staje się niemożliwe! Za pomocą "Tarczy" oraz połączeń bezpośrednich z operatirami GSM realizujemy politykę "zero tolerancji dla nadużyć". DCSMS gwarantuje najwyższej jakości usługę i ochronę. Nasze algorytmy gwarantują niemal 100% pewność, że żadna wysyłka nie będzie realizowana bez autoryzacji zlecającego.
Czytaj więcej o tarczy CPT