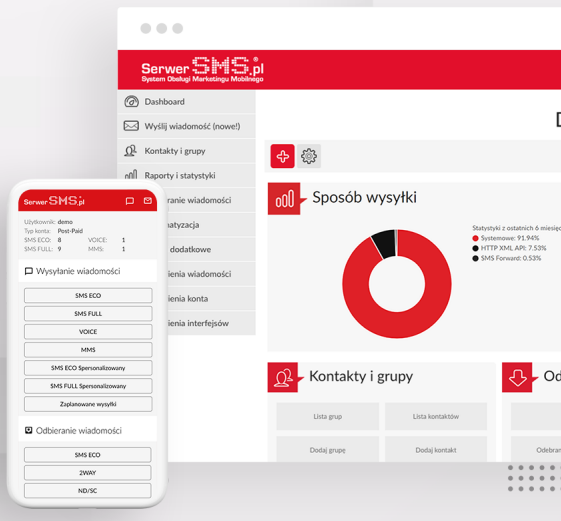
Serwer SMS.pl
System Obsługi Marketingu Mobilnego

Środki zaradcze i zapobiegawcze po incydencie



Środki zaradcze i zapobiegawcze po incydencie

Działania tuż po incydencie

- Podatność w systemie wykorzystana do przeprowadzenia ataku została natychmiast zidentyfikowana i usunięta.
- Wymusiliśmy zmianę haseł na kontach klientów.
- Ograniczyliśmy możliwość logowania z nieautoryzowanych adresów IP poza tymi, które zidentyfikowaliśmy jako bezpieczne.
- Rozszerzyliśmy zakres monitoringu platformy, w szczególności monitoring live ruchu HTTP.
- Potwierdziliśmy brak naruszenia integralności danych klientów.
- Serwery zostały przeskanowane pod względem obecności złośliwego oprogramowania.

Działania w trakcie i na przyszłość

- Wdrożenie w systemie funkcjonalności umożliwiające anonimizację danych według indywidualnych parametrów (zakres, czas) per konto użytkownika.
- Wdrożenie systemu SIEM (security information and event management) dla wszystkich podsystemów usługi.
- Rozszerzenie i uszczegółowienie reguł systemu WAF (Web Application Firewall)
- Wdrożenie NIPS/NIDS (Network Intrusion Prevention / Detection System) do monitorowania ruchu sieciowego.
- Przeprowadzenie dodatkowych testów penetracyjnych systemu przez zewnętrzny i niezależny podmiot, który zakończy się uzyskaniem certyfikatu bezpieczeństwa.
- Przeprowadzenie sesji lessons learned oraz wprowadzenie modyfikacji do procedur bezpieczeństwa wynikających z zaistniałego incydentu.
- Przeprowadzenie szkolenia z zakresu nowych procedur bezpieczeństwa dla pracowników.