Polityka bezpieczeństwa - notifications.pl

1. Ogólne wprowadzenie

Ten dokument przedstawia politykę bezpieczeństwa serwisu notifications.pl, fizyczną ochronę dostępu, zasadę autoryzacji i uwierzytelniania, metody autoryzacji, prawo dostępu oraz bezpieczną autoryzację; eksploatację serwerów, oprogramowania, rozwój aplikacji, ochrona przed programami szkodliwymi, w tym ochrona przed wirusami, i przed aktywnymi treściami; zabezpieczanie danych przed awariami, zdalna kontrola i utrzymanie komputerów osób zewnętrznych, urządzeń mobilnych, nośników danych.

2. Fizyczna ochrona dostępu

Serwerownie są utrzymywane w zewnętrznych firmach które zarządzają dostępem do swoich urządzeń, dlatego administrator serwisu jest zwolniony z zarządzania fizyczną ochroną dostępu.

3. Zasada autoryzacji i uwierzytelniania.

Użytkownicy podczas rejestracji ustalają własne, bezpieczne hasła, na zasadach
ustalonych przez administratora - minimum 64 znaki w tym 10 alfanumerycznych i 10 specjalnych.

Producenci używają tokenów które są generowane na podstawie czasu, co 1 minutę nowy, po podaniu hasła zdefiniowanego przy rejestracji.

4. Metody autoryzacji

Klienci i producenci mają do wyboru logowanie za pomocą haseł zdefiniowanych wcześniej przez nich, bądź generowanych co minutę tokenów.

5. Prawo dostępu

Prawo dostępu do zasobów ustala uprawniona osoba, w tym przypadku administrator serwisu notifications.pl. Subskrypcje poszczególnych tematów, użytkownicy mogą samodzielnie wybierać.

6. Eksploatacja serwerów

Monitoring oraz nadzór nad wykorzystaniem zasobów serwera przeprowadza administrator serwera w współpracy z personelem znajdującym się w danej serwerowni.

W przypadku wykrycia naruszeń ze strony poszczególnych użytkowników administrator serwisu ma prawo do wyłączenia poszczególnych kont, a w przypadkach drastycznych do całkowitego zaprzestania świadczenia usługi.

7. Rozwój aplikacji

Administrator serwisu oraz osoby powiązane są zobowiązane do monitorowania sytuacji rynkowej w celu wczesnego wykrywania zmian w poszczególnych serwisach i wprowadzania ich w aplikacjach tych serwisów Dzięki temu serwis zawsze będzie posiadał aktualne wersje oprogramowania co zapobiegnie ewentualnym atakom ze strony osób nieupoważnionych.

8. Ochrona przed programami szkodliwymi

Ochrona przed programami szkodliwymi zapewnia po części firewall wbudowany w poszczególne serwery. Specjalnie spreparowanie wiadomości są wykrywane na poziomie poczególnych aplikacji, dzięki temu nie możliwym jest przejęcie kontroli nad serwerem. Dodatkowo nieautoryzowany dostęp nie jest możliwy, gdyż użytkownicy i administrator posiadają własny metody logowania ustalone w poprzednich punktach.

10. Zabezpieczanie danych przed awariami

Bazy danych posiadają specjalne systemy archiwizujące, które w przypadku awarii uruchamiają się. Polegają one na wcześniejszych kopiach zapasowych, które w przypadku awarii są przywracane na serwer. Administrator serwisu jest zobowiązany do zautomatyzowania procesu tworzenia kopii zapasowych.

11. Zdalna kontrola i utrzymanie komputerów osób zewnętrznych, urządzeń mobilnych, nośników danych

Administrator serwisu ma prawo do zdalnej kontroli komputerów, urządzeń mobilnych oraz nośników danych należących do notifications.pl