

Bezpieczeństwo w Fakturowo.pl

Czwartek, 1 październik 2026, 08:29, autor: Fakturowo.pl

W związku z coraz częściej pojawiającymi się informacjami o atakach na serwisy internetowe, wyciekach danych, próbach przejmowania kont oraz kampaniach phishingowych chcemy wyjaśnić, w jaki sposób dbamy o bezpieczeństwo Użytkowników Fakturowo.pl. Zagrożenia w Internecie cały czas się zmieniają. Atakujący wykorzystują nie tylko podatności w oprogramowaniu, ale również przejęte hasła, fałszywe wiadomości e-mail, podszywanie się pod znane serwisy czy automatyczne próby logowania na dużą liczbę kont. Dlatego bezpieczeństwo traktujemy jako proces ciągły. Stosujemy rozwiązania techniczne po stronie serwisu, monitorujemy jego działanie, aktualizujemy wykorzystywane oprogramowanie, zlecamy zewnętrzne audyty bezpieczeństwa, a jednocześnie udostępniamy Użytkownikom dodatkowe funkcje pozwalające lepiej chronić własne konto.



Szyfrowane połączenie z serwisem

Szyfrowane połączenie HTTPS jest obecnie podstawowym i niezbędnym standardem bezpieczeństwa dla każdego serwisu internetowego, w którym Użytkownik loguje się do swojego konta lub przesyła dane. Traktujemy je więc jako podstawę, na której opierają się kolejne stosowane przez nas mechanizmy zabezpieczeń. Połączenie z Fakturowo.pl odbywa się przy użyciu szyfrowanego połączenia HTTPS. Dzięki temu dane przesyłane pomiędzy urządzeniem Użytkownika a serwisem są chronione podczas transmisji. Dotyczy to zarówno danych logowania, jak również informacji przesyłanych podczas korzystania z serwisu.

Uwierzytelnianie dwuskładnikowe 2FA

Użytkownik może dodatkowo zabezpieczyć swoje konto poprzez włączenie uwierzytelniania dwuskładnikowego 2FA. Po jego aktywacji w zakładce - Konto - samo hasło nie wystarcza do zalogowania się na konto. Wymagany jest również dodatkowy kod generowany w aplikacji uwierzytelniającej, np. Google Authenticator. Jest to szczególnie ważne w sytuacji, gdy hasło Użytkownika zostało ujawnione w wyniku wycieku danych z innego serwisu, przejęte przez złośliwe oprogramowanie lub podane na fałszywej stronie logowania. Włączenie 2FA znacznie ogranicza możliwość zalogowania się na konto przez osobę niepowołaną, nawet jeżeli zna ona hasło.

Więcej informacji - <https://www.fakturowo.pl/pomoc/uwierzytelnianie-dwuskladnikowe-2fa>

Powiadomienia o logowaniu z nowego adresu IP

W zakładce - Konto - można włączyć dodatkową kontrolę adresów IP używanych podczas logowania. Jeżeli system wykryje logowanie z adresu IP, z którego nie logowano się na dane konto w ciągu ostatnich 6 miesięcy, na adres e-mail Użytkownika zostanie wysłane odpowiednie powiadomienie. Pozwala to szybciej zauważyć nietypowe logowanie i w razie potrzeby odpowiednio zareagować.

Więcej informacji - <https://www.fakturowo.pl/pomoc/powiadomienia-o-logowaniu>

Rejestrowanie nieudanych prób logowania

W zakładce - Konto - można również włączyć rejestrowanie wszystkich nieudanych prób logowania. Po aktywacji tej funkcji w dzienniku zdarzeń zapisywane są próby, podczas których podano poprawny adres e-mail, ale nieprawidłowe hasło. Użytkownik może dzięki temu sprawdzić, czy ktoś podejmował próby uzyskania dostępu do jego konta.

Okresowa zmiana hasła

Fakturowo.pl umożliwia również włączenie obowiązkowej okresowej zmiany hasła. Po aktywacji tej opcji system raz w roku wymusi ustawienie nowego hasła podczas logowania. Jest to dodatkowy mechanizm pozwalający ograniczyć ryzyko długotrwałego korzystania z tego samego hasła.

Więcej informacji - <https://www.fakturowo.pl/pomoc/okresowa-zmiana-hasla>

Warto pamiętać, że przejęcie konta Użytkownika nie zawsze jest wynikiem ataku bezpośrednio na serwis, w którym konto jest prowadzone. Jednym z częstszych zagrożeń jest używanie tego samego adresu e-mail i hasła w wielu

serwisach. Jeżeli dane logowania zostaną ujawnione w wyniku wycieku z jednego serwisu, mogą być później automatycznie sprawdzane również w innych serwisach. Takie próby wykonywane są często automatycznie na bardzo dużą skalę. Dlatego bardzo ważne jest korzystanie z unikalnego hasła do Fakturowo.pl.

Dziennik zdarzeń

W serwisie dostępny jest dziennik zdarzeń, który pozwala kontrolować wybrane operacje związane z kontem. W zależności od włączonych ustawień mogą być w nim rejestrowane między innymi próby logowania. Dzięki temu Użytkownik może łatwiej zauważyć aktywność, której sam nie wykonywał.

Aktualizacje i monitoring serwisu

Na bieżąco aktualizujemy wykorzystywane oprogramowanie oraz reagujemy na informacje dotyczące nowych zagrożeń i podatności. Monitorujemy również działanie infrastruktury serwisu i podejmujemy działania mające ograniczać ryzyko nieautoryzowanego dostępu do danych. Bezpieczeństwo nie polega na jednorazowym wdrożeniu określonych zabezpieczeń. Wymaga ono stałego monitorowania, aktualizacji i dostosowywania stosowanych rozwiązań do zmieniających się zagrożeń.

Zewnętrzne audyty bezpieczeństwa

Bezpieczeństwo Fakturowo.pl weryfikujemy nie tylko wewnętrznie. Zlecamy również audyty bezpieczeństwa wyspecjalizowanym firmom zewnętrznym, które niezależnie sprawdzają stosowane przez nas rozwiązania, konfigurację systemów oraz potencjalne podatności. Niezależna weryfikacja pozwala spojrzeć na zabezpieczenia z innej perspektywy i wykrywać potencjalne problemy, które następnie mogą zostać usunięte lub dodatkowo zabezpieczone. Zewnętrzne audyty są jednym z elementów stałego procesu dbania o bezpieczeństwo Fakturowo.pl i danych naszych Użytkowników.

Kopie bezpieczeństwa

Dane przechowywane w serwisie są objęte systemem kopii bezpieczeństwa. Kopie zapasowe ograniczają ryzyko utraty danych w przypadku awarii lub innych nieprzewidzianych zdarzeń.

Co może zrobić Użytkownik?

Bezpieczeństwo konta zależy zarówno od zabezpieczeń stosowanych przez serwis, jak i od sposobu korzystania z konta przez Użytkownika. Zalecamy:

- używanie silnego i unikalnego hasła do Fakturowo.pl,
- nieużywanie tego samego hasła w innych serwisach,
- włączenie uwierzytelniania dwuskładnikowego 2FA,
- włączenie powiadomień o logowaniu z nowych adresów IP,
- włączenie rejestrowania nieudanych prób logowania,
- regularne sprawdzanie dziennika zdarzeń,
- nieudostępnianie danych logowania innym osobom,
- zachowanie ostrożności wobec wiadomości zawierających odnośniki do stron logowania,
- korzystanie z aktualnego systemu operacyjnego i przeglądarki internetowej.

Czy można całkowicie wyeliminować ryzyko ataku?

Nie istnieje system internetowy, w przypadku którego można zagwarantować całkowity brak ryzyka ataku. Każdy publicznie dostępny serwis internetowy jest na bieżąco narażony między innymi na automatyczne skanowanie portów, próby wyszukiwania podatności, nieudane próby logowania czy inne działania wykonywane przez automatyczne narzędzia działające w Internecie.

Tego typu aktywność obserwujemy praktycznie każdego dnia, dlatego bezpieczeństwo Fakturowo.pl traktujemy jako proces ciągły. Monitorujemy zagrożenia, aktualizujemy stosowane rozwiązania, analizujemy podejrzaną aktywność, korzystamy z niezależnych audytów bezpieczeństwa i rozwijamy mechanizmy pozwalające dodatkowo chronić konta Użytkowników.

Zachęcamy również do korzystania z dostępnych w zakładce Konto funkcji bezpieczeństwa, szczególnie z uwierzytelniania 2FA, powiadomień o nowych adresach IP oraz dziennika zdarzeń.

Tagi: bezpieczeństwo fakturowo, bezpieczeństwo danych, 2fa, uwierzytelnianie dwuskładnikowe, ochrona konta, szyfrowanie https, audyt bezpieczeństwa, kopie bezpieczeństwa, phishing, bezpieczeństwo faktur