Przelewy24

Jak zadbać

o bezpieczeństwo danych klienta

w sieci

Jakie zagrożenia dotyczą branży e-commerce?

Jednym z najczęstszych ataków hakerskich w branży e-commerce jest phishing. Polega on na przykład na podszywaniu się pod istniejącą firmę w celu wyłudzenia danych logowania, zwłaszcza do konta bankowego. Do najpopularniejszych sposobów phishingu można zaliczyć **wysyłanie smsów lub maili** informujących o konieczności weryfikacji zamówienia lub dopłaceniu niewielkiej kwoty za przesyłkę.

Innym sposobem ataku jest ransomware - złośliwe oprogramowanie, które szyfruje dane na dysku. Osoba zaatakowana dostaje następnie informacje z żądaniem okupu, który należy uiścić w celu odzyskania dostępu. **Wraz z tym działaniem pojawiają się także często wycieki, kradzieże i utrata informacji.**

Dbaj o bezpieczeństwo witryny i swoich klientów

Jedną z najważniejszych zasad ochrony danych w Internecie, jest wprowadzenie odpowiedniego zabezpieczenia strony internetowej. Jak dbać o bezpieczeństwo w sieci? Ważnymi elementami są:

Certyfikat SSL

Szyfrowana wersja protokołu http. Zabezpiecza stronę przed przechwyceniem danych. Taką stronę można rozpoznać po pojawieniu się kłódki przed adresem URL oraz po zmianie przedrostka http na https.

Backup

Kopia zapasowa danych umieszczona na bezpiecznym nośniku i najlepiej zaszyfrowana. W ten sposób chronisz się przed ewentualną utratą cennych danych wskutek awarii sprzętu, błędu ludzkiego lub działania złośliwego oprogramowania.

Podnoś świadomość swoich pracowników

Przelewy24

Niezwykle ważne jest podnoszenie świadomości konieczności dbania o bezpieczeństwo wśród pracowników. Przede wszystkim należy zadbać, by sprzęt służbowy wyposażony był w wysokiej jakości oprogramowanie zabezpieczające komputer, takie jak antywirus i firewall.

Warto regularnie przypominać personelowi zasady bezpiecznego korzystania z komputera, do których można zaliczyć:

regularne aktualizowanie oprogramowania

tworzenie kopii zapasowych danych, zwłaszcza na szyfrowanych dyskach

tworzenie mocnych haseł (powinny być one odpowiednio długie, np. Powyżej 16 znaków)

dokładne sprawdzanie wiadomości przed otwarciem załączników

- Zalecane jest korzystanie z managera haseł.
- Pracownicy powinni być także wyczuleni na podejrzane wiadomości e-mail.

Stosuj zaufane metody płatności

Przelewy24

Chcąc zadbać o bezpieczeństwo i komfort swoich klientów, powinno się zastosować **metody płatności online, do których mają zaufanie.** Nasza oferta zawiera rozwiązania, ułatwiające bezpieczną obsługę płatności w e-commerce.

Jedną z najczęściej wykorzystywanych płatności online jest BLIK

To metoda, która zyskała ogromne zaufanie wśród konsumentów. Polega na podaniu 6-cyfrowego kodu płatniczego wygenerowanego w aplikacji banku, a następnie potwierdzeniu transakcji. W ten sposób konsument nie musi podawać danych karty płatniczej, czy logować się do bankowości on-line.

Zabezpieczeniem płatności kartą jest natomiast procedura chargeback

Pozwala ona na uruchomienie procedury reklamacyjnej, która ma na celu zwrot pobranej kwoty na konto użytkownika. Stosuje się ją przede wszystkim podczas błędów operacji (błędna ilość pieniędzy wydanych przez bankomat, ponowne zaksięgowanie płatności), jednak można ją także wykorzystywać w momencie, gdy sklep nie wywiązał się z dostarczenia produktu, albo gdy towar był uszkodzony lub niezgodny z opisem.

Dziękujemy za uwagę

Przelewy24