Elektron tijorat (e-commerce) tizimidan foydalanuvchi mijozlarga xavfsizlik yuzasidan qo’yiladigan talablar

Elektron tijorat (e-commerce) xizmatlarini bank orqali ulovchi tashkilotlar uchun axborot va kiberxavfsizlik sohasida bir qator talablar mavjud. Bu talablar ma'lumotlarni, tranzaksiyalarni himoya qilish va xavfsizlik standartlariga rioya qilishni ta'minlashga qaratilgan.

1. PCI DSS standartiga muvofiqligi

•To'g'ridan-to'g'ri PCI DSS standartlariga rioya qilish mas'uliyati sotuvchilarga yuklansa-da, ular mijozlarning ma'lumotlarini (masalan, karta raqamlari) himoya qilish choralarini ko'rishlari kerak. Bunga quyidagilar kiradi:

-Karta ma'lumotlarini saqlamaslik. (PAN, CVV, CARDHOLDER NAME, EXP DAY)

-Uzatilayotgan ma'lumotlarni shifrlash orqali himoya qilish (kamida TLSv 1.2).

2. Xavfsiz aloqa protokollaridan foydalanish

•Sotuvchilar, bank sayti yoki to'lov tizimi bilan ma'lumot almashish jarayonida tranzaksiyalar va foydalanuvchi ma'lumotlarini himoya qilish uchun HTTPS orqali xavfsiz ma'lumot uzatish kanallarini o'rnatishlari shart (kamida TLSv 1.2).

3. Ko'p faktorli autentifikatsiya (MFA)

•Mijozning shaxsiy kabinetiga kirish yoki bankning protsessing xizmatlariga kirish uchun ko'p faktorli autentifikatsiyani joriy qilish, bu esa e-commerce xizmatlarini ishlatadigan akkauntlarga kirishni xavfsizroq qilishga yordam beradi.

4. Hujumlardan himoya

•SQL-inyektsiyalar, XSS (Cross-Site Scripting), DDoS va boshqa zaifliklardan himoyalanish uchun himoya mexanizmlarini o'rnatish zarur. Bu tranzaksiyalar amalga oshiriladigan veb-saytlar va platformalarning xavfsizligini ta'minlash uchun muhimdir.

•Fishing va boshqa firibgarlik sxemalaridan himoyalanish, shuningdek, foydalanuvchilarga tarmoqda xavfsiz xulq-atvorni o'rgatish.

5. Yangilanishlar va xavfsizlik patch'lari

•Sotuvchilar o'z tizimlarini va dasturiy ta'minotlarini muntazam ravishda yangilab turishlari kerak, chunki bu zaifliklar hujumchilar tomonidan foydalanilishi mumkin.

6. Ma'lumotlarni shifrlash

•Shaxsiy ma'lumotlar va to'lov kartalari ma'lumotlarini uzatish va saqlashda shifrlash. Bu talab tranzaksiyalar ma'lumotlarini va mijozlar haqida ma'lumotlarni saqlashga tegishli.

7. Xodimlarni o'qitish

•Xodimlarga xavfsizlik bo'yicha muntazam treninglar o'tkazish, shu jumladan phishing, ijtimoiy injiniring va boshqa xavfsizlik tahdidlaridan himoya qilish choralarini o'rgatish.

8. Kirish nazorati

•To'lov tizimlari yoki mijozlar ma'lumotlariga kirish huquqiga ega xodimlar uchun qat'iy kirish nazorati siyosatini o'rnatish. Masalan, to'lov ma'lumotlariga kirish faqat ushbu ma'lumotlarni o'z vazifalarini bajarish uchun zarur bo'lgan xodimlar bilan cheklanishi kerak.

9. Muntazam auditlar va testlar

•Tizimdagi zaifliklarni aniqlash va xavfsizlik standartlariga muvofiqlikni ta'minlash uchun muntazam xavfsizlik auditlarini va penetratsion testlarni o'tkazish.

10. Xavfsizlik uchun javobgarlik

•Bank orqali elektron tijorat xizmatlarini ulovchi sotuvchilar tranzaksiyalar xavfsizligi, mijoz ma'lumotlarini himoya qilish va barcha tegishli standartlarga rioya qilish mas'uliyatini tushunishlari kerak.