Чуйко М.М., Григор'єв А.В.

БЕЗПЕКА В ЕЛЕКТРОННІЙ КОМЕРЦІЇ

Електронна комерція, або e-commerce – це сфера економіки, коли торгові або фінансові операції проводяться в інтернеті. Якщо говорити простими словами, це будь-яка транзакція, виконана з електронного пристрою, підключеного до мережі. Аналог торгового центру, але з великим асортиментом і комфортом: його можна відвідати, не виходячи з дому.

Основний, але далеко не єдиний, плюс інтернет-торгівлі в відсутності географічних обмежень. Співпраця з логістичними компаніями допоможе охопити аудиторію в світовому масштабі. Так діють гіганти інтернет-торгівлі, такі як AliExpress, Alibaba, eBay, Amazon, Zappos, iTunes.

Коли бренд стає популярний, логотип пізнаваний, бізнес отримує нових користувачів по «сарафанне» радіо: люди діляться посиланнями в соціальних мережах на цікаві товари, приємні ціни або УТП (унікальна торгова пропозиція). Таким чином, інтернет допомагає привести умовно безкоштовних клієнтів.

Електронна комерція має свої недоліки, які необхідно враховувати всім її учасникам. Так підприємці мають пам'ятати про проблеми, які можуть виникнути з інтернет-ресурсами. Відсутність доступу до сайту – це втрата клієнтів і доходу. Крім того, не слід забувати про величезний рівень конкуренції. Для того, щоб випередити своїх суперників, доведеться докласти чимало зусиль.

У реальному світі багато приділяємо фізичній безпеці, а у світі електронної комерції доводиться піклуватися про засоби захисту даних, комунікацій і транзакцій. Зі зростанням індустрії електронної комерції, зросли також випадки кіберзлочинів. Зловмисники використовують різні засоби для наживи або просто, щоб дестабілізувати онлайн-бізнес конкурентів.

Керівники підприємств електронної комерції в належному ступені усвідомлюють серйозність інформаційних загроз і важливість організації захисту своїх ресурсів тільки після того, як останні піддалися інформаційним атакам. Як видно, всі перераховані перешкоди відносяться до сфери інформаційної безпеки.

Серед основних вимог до проведення комерційних операцій – конфіденційність, цілісність, аутентифікація, авторизація, гарантії і збереження

таємниці. Загрози безпеці електронної комерції викликають хаос в онлайн-торгівлі. Хакери стають все хитрішими та витонченішими, автоматизуючи свої процеси та масштабуючи ресурси. Злочинці націлені на адміністраторів, користувачів і співробітників інтернет-магазинів, використовуючи багато зловмисних методів.

В Інтернет-безпеці не існує “срібної кулі” – єдиного програмного рішення, що усунуло б усі ризики. Для ефективного зниження ризиків необхідне ретельне ручне опрацювання на всіх ділянках бізнес-процесів із використанням сучасних технологій безпеки. На жаль, багато видів кіберзагроз можуть зашкодити онлайн-магазинам та негативно вплинути на репутацію продавця. Найбільш поширеним типом загрози лишається спроба кіберзлочинців отримати доступ до платіжної інформації відвідувачів.

У рамках забезпечення комплексної інформаційної безпеки, перш за все, слід виділити ключові проблеми в галузі безпеки електронного бізнесу, які включають: захист інформації при її передачі по каналах зв'язку; захист комп'ютерних систем, баз даних та електронного документообігу; забезпечення довгострокового зберігання інформації в електронному вигляді; забезпечення безпеки транзакцій, секретність комерційної інформації, аутентифікацію, захист інтелектуальної власності тощо.

Для протидії цим загрозам використовується цілий ряд методів, заснованих на різних технологіях, а саме: шифрування – кодування даних, що перешкоджає їх прочитання чи спотворення; цифрові підписи, що перевіряють справжність особи відправника і одержувача; stealth-технології з використанням електронних ключів; брандмауери; віртуальні та приватні мережі.

Таким чином, якщо кожен підприємець буде дотримуватись всіх рекомендацій, що необхідні для створення своєї компанії для роботи в e-commerce, то не буде ніяких проблем з безпекою клієнтів, а також це не позначиться на репутації цієї компанії.