

УДК 651

Федчик Христина

Тернопільський національний технічний університет імені Івана Пулюя (Україна)

БЕЗПЕКА ОСОБИСТИХ ДАНИХ В ЕЛЕКТРОННІЙ КОМЕРЦІЇ

Fedchyk Khrystyna

Ternopil Ivan Puluj National Technical University, Ternopil (Ukraine)

PERSONAL DATA SECURITY IN E-COMMERCE

Сучасна індустрія eCommerce – це величезний комплекс інструментів, які використовуються для збільшення продажів, розвитку бізнесу та підвищення комфорту клієнтів під час здійснення покупок. Сучасні веб-сайти електронної комерції залучають мільйони користувачів та оперують їх особистими й фінансовими даними. Такі ресурси не можуть не бути магнітом для кіберзлочинців. Відтак величезного значення в eCommerce набуває правильно побудована стратегія безпеки для таких ресурсів [3].

Основною проблемою безпеки електронної комерції в Internet з часу її виникнення була проблема передавання закритої інформації (номерів кредитних карток, сум платежів тощо) через відкриту мережу. Найпоширенішою є-крадіжка ідентифікаційної інформації злодії збирають персональну інформацію - імена, адреси, номери соціального страхування й інші важливі дані, а після цього замовляють картки під цими іменами. Хоча крадіжки такого типу - річ не нова, Internet значно полегшив їх здійснення. В деяких випадках злочинці вдають із себе легітимних он-лайнних торговців і збирають інформацію в покупців, які нічого не підозрюють. Дійсні номери карток також можуть бути автоматично згенеровані. Internet перенасичений хакерськими сайтами, які пропонують програмне забезпечення для генерації номерів кредитних карток, що здаються дійсними. Ці програми використовують складний алгоритм створення номерів, у яких, наприклад, перші чотири цифри відповідають дійсним цифрам банків-емітентів. Генератори створюють 12 додаткових цифр, які під час перевірки відповідають параметрам дійсних карток. Навіть якщо жоден банк ніколи не емітував картку з цим згенерованим номером, може так статися, що вони будуть авторизовані при електронних платежах. Існує ще й старий перевірений спосіб: кредитні картки викрадають і використовують для он-лайн закупівель [1].

Безпека будь-якої системи електронного бізнесу полягає в захисті від різного роду втручання у її дані. Усі ці втручання можна умовно розділити на кілька категорій:

- розкрадання даних (наприклад, розкрадання номерів кредитних карт із бази даних);
- втручання (наприклад, перевантаження даними сайту, не призначеного для такого великого обсягу інформації);
- перекручування даних (наприклад, зміна сум у файлах платежів і рахунків-фактур чи створення неіснуючих сертифікатів);
- руйнування даних (наприклад, при передачі користувачу і назад);
- відмова від виконаних дій (наприклад, від факту оформлення замовлення чи одержання товару);
- ненавмисне неправильне використання засобів сайту користувачем;
- несанкціонований доступ до інформації (несанкціоноване копіювання, відновлення або інше використання даних, проведення несанкціонованих трансакцій, несанкціонований перегляд чи передача даних). При цьому необхідно враховувати, що при забезпеченні безпеки електронного бізнесу є ряд об'єктивних проблем - прискорений розвиток технологій стосовно удосконалювання законодавчої бази, складність піймання зловмисників на місці злочину, можливість безслідного знищення

доказів і слідів злочинів і т.п. Усе це обумовлює необхідність ретельної розробки компаніями політики захисту свого електронного бізнесу.

Для захисту від зовнішнього вторгнення сьогодні існує безліч систем, які є різного роду фільтрами, що допомагають виявити спроби несанкціонованого втручання на ранніх етапах і по можливості не допустити зловмисників у систему через зовнішні мережі. До таких засобів належать:

- маршрутизатори - пристрої керування трафіком мережі, розташовані між мережами другого порядку і керують вхідним та вихідним трафіком приєднаних до нього сегментів мережі;

- брандмауери - засоби ізоляції приватних мереж від мереж загального користування, що використовують програмне забезпечення, яке відслідковує і припиняє зовнішні атаки на сайт за допомогою певного контролю типів запитів;

- шлюзи додатків - засоби, за допомогою яких адміністратор мережі реалізує політику захисту, якою керуються маршрутизатори, що здійснюють пакетну фільтрацію;

- системи відстеження вторгнень - системи, які виявляють навмисні атаки і ненавмисне неправильне використання системних ресурсів користувачами;

- засоби оцінки захищеності (спеціальні сканери та ін.) - програми, які регулярно сканують мережу на предмет наявності проблем і тестують ефективність реалізованої політики безпеки [2].

Сучасна індустрія eCommerce стрімко розвивається, пропонуючи широкий спектр інструментів для зручності покупців і зростання бізнесу. Водночас вона стикається з серйозними викликами в сфері безпеки, зокрема через загрози, пов'язані з передачею конфіденційної інформації та активністю кіберзлочинців. Захист електронної комерції вимагає комплексного підходу, що включає технічні, організаційні та правові заходи. Використання сучасних систем фільтрації, моніторингу та управління доступом, разом із чітко розробленою політикою безпеки, дозволяє мінімізувати ризики і забезпечити довіру користувачів. Лише системна та своєчасна робота над безпекою може гарантувати сталий розвиток eCommerce у цифрову епоху.

Список використаних джерел:

1. Безпека і захист інформації в електронній комерції. URL: <https://studfile.net/preview/10968806/page:16/>
2. Безпека електронної комерції. URL: <https://studfile.net/preview/9727527/page:15/>
3. Кібербезпека в eCommerce проектах: важливість та шляхи забезпечення. URL: <https://wezom.com.ua/ua/blog/kiberbezpeka-v-proektah-ecommerce-kompleksniy-gayd>
4. Краузе О., Бойко О. Роль хмарних технологій в удосконаленні обліково-аналітичних процесів / Трансформація бізнесу для сталого майбутнього: дослідження, цифровізація та інновації: монографія /за ред. д.е.н., проф. О. А. Сороківської. Тернопіль: ФОП Паляниця В.А., 2024. С. 36-45. URL: <https://elartu.tntu.edu.ua/handle/lib/46506>
5. Шведа Н., Краузе О. Трансформація бізнес-моделей в умовах цифрової економіки. *Соціально-економічні проблеми і держава* (електронний журнал). 2023. Вип. 1 (28). С. 86- 94. URL: <http://sepd.tntu.edu.ua/images/stories/pdf/2023/23snmute.pdf>
6. Шведа Н.М., Краузе О.І. Електронна комерція: сучасний стан та стратегії розвитку. *Міжнародний науковий журнал «Інтернаука». Серія: «Економічна науки»*. 2024. Вип. 2 (82). URL: <https://www.inter-nauka.com/archive/archive-of-issues-ekonomika>