Секція 1

МЕТОДИ ЗАХИСТУ САЙТУ «ІНТЕРНЕТ-МАГАЗИНУ» ВІД КІБЕРАТАК

Фещук Д.Ю.
Національний аерокосмічний університет ім. М.Є Жуковського
«Харківський авіаційний інститут»
Науковий керівник Землянко Г.А.

Актуальність. Комп'ютерні та інформаційні технології сьогодні охопили багато галузей економіки, а саме торгівлю, і в них є дуже багато факторів небезпеки. Однією із небезпек являється безпека їх торгівельних майданчиків в мережі інтернет. Мова йдеться не лише про безпеку самої компанії а й про її клієнтів. Для будь-якої сучасної компанії інформація стає одним із головних ресурсів, тому актуальною проблемою для підприємства стає забезпечення інформаційної безпеки.
Тому дуже важливо захистити свій сайт від можливих кібератак та іншого.

Мета. Метою доповіді буде проаналізувати методи які зможуть захистити сайт «інтернет-магазин» від кібератак

Основні положення. Інформаційна безпека – властивість системи протягом заданого часу протистояти несанкціонованому зняттю та модифікації інформації.

Розглянемо основні способи того, як можна вберегти свій сайт «інтернет магазин» від кібератак:
1. Захист корпоративної пошти. Половина всіх кібератак відбувається з боку корпоративної пошти, адже це критично важливий інструмент для компанії. Якщо безліч рекламних листів одразу не фільтрувати та не видаляти, то вони швидко заповнять всі ресурси сервера. Щоб убезпечитися від таких базових кібератак, поштовий сервіс варто розмістити у хмарі. Наприклад, хмарна платформа Microsoft Azure вже передбачає базовий захист від спаму, антифішинг тощо [1].
2. Аналіз поведінки внутрішніх користувачів. Система для аналізу поведінки користувачів допомагає виявити нетипові дії співробітників.
User behavior analytics (UBA) та User and Entity Behavior Analytics (UEBA) дозволяють за допомогою штучного інтелекту створити матрицю поведінки користувача або пристрою. Наприклад, співробітник щодня для робочих задач використовує Outlook, Microsoft Teams та завантажує 10 Мб файлів з пошти. Система запам’ятовує такий перелік дій, а тому помічає, коли раптом користувач починає завантажувати великий об’єм даних з

внутрішнього сервера компанії на зовнішній ресурс. Це суттєве відхилення від матриці, а тому UBA одразу реагує. Вона може просто повідомити службу безпеки про нетипову поведінку або ж тимчасово заблокувати дії користувача [1].

3. Турбота про безпеку клієнтів [2]:

– підвищуйте обізнаність клієнтів у питаннях ІБ;

– регулярно нагадуйте клієнтам про правила безпечної роботи в інтернеті, роз'яснюйте методи атак та способи захисту;

– застерігайте клієнтів від введення облікових даних на підозрілих веб-ресурсах і тим більше від повідомлення такої інформації будь-кому

– електронною поштою або під час телефонної розмови;

– роз'яснюйте клієнтам порядок дій у разі підозри про шахрайство;

– повідомляйте клієнтів про події, пов'язані з інформаційною безпекою.

Висновки. Проаналізувавши статистику з сайту компанії techexpert.ua [3], можна побачити , що кількість втрачених записів даних з кожним роком дуже стрімко збільшується – в 2005 році приблизно 15 мільйонів, в 2017 році – приблизно 63 мільйони, а в 2020 вже 101 мільйон втрачених записів даних. Зі звіту також видно, що інвестиції на захист даних за 2020 рік збільшилися на 10% з попереднього року і становлять близько 53 мільярдів доларів. Отже, можемо зробити висновок. З розвитком інформаційних технологій виростає ймовірність бути жертвою кібератаки.Тому варто серйозно віднестися до складової кібербезпеки в вашій компанії, а в нашому випадку сайту «інтернет-магазину».

Список літератури

1. 7 способів вас зламати або як захиститися від кібератак. *Kyivstar*. URL: https://hub.kyivstar.ua/news/7-sposobiv-vas-zlamaty-abo-yak-zahystyty-kompaniyu-vid-kiberatak/ (дата звернення: 23.06.2022).

2. Як захиститися від кібератак. *Positive Technologies*. URL: https://www.ptsecurity.com/ru-ru/research/knowledge-base/kak-zashchititsya-ot-kiberatak/ (дата звернення: 23.06.2022);

3. Кількість кібератак збільшується: що з цим робити. *Techexpert*. URL: https://techexpert.ua/ru/cyberattacks-number-research/ (дата звернення: 24.06.2022).

Відомості про авторів

Фещук Дмитро Юрійович, студент кафедри комп'ютерних систем, мереж і кібербезпеки,м.т. 0665868122, d.y.feshchuk@student.csn.khai.edu

Землянко Георгій Андрійович, асистент кафедри комп'ютерних систем, мереж і кібербезпеки, g.zemlynko@csn.khai.edu