УДК 004.056:355.451

ДОСЛІДЖЕННЯ ШЛЯХІВ ТА ВИРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНИХ РЕСУРСІВ В СИСТЕМАХ ЕЛЕКТРОННИХ ПЛАТЕЖІВ

Лось Д.І.
Науковий керівник – асистент Гвоздьов Р. Ю.
Харківський національний університет радіоелектроніки, каф. БІТ,
м. Харків, Україна
e-mail: dmytro.los1@nure.ua

The transition of client services online and the shift to remote work by banks demand a reassessment of information and cybersecurity. Even minor security incidents can cost financial institutions reputation and business loss. Essential protective measures include continuous security level evaluation, penetration testing, and cybersecurity risk assessment. Ongoing training for users and administrators focuses on reducing the impact of the "human factor." Monitoring events, incident response, and behavioral analysis are crucial amid the rising cyber threat landscape. Machine learning, secure endpoints, and server management enhance transaction security.

Перехід багатьох клієнтських сервісів в онлайн, а також вимушене переведення банками і фінкомпаніями своїх співробітників на віддалену роботу вимагає перегляду заходів інформаційної та кібербезпеки [1].

Навіть незначний інцидент у сфері безпеки платежів, як наприклад, витік конфіденційних даних, може коштувати фінансовій установі втрати репутації, що рівнозначно втраті бізнесу.

Для базового захисту своїх систем, операцій і даних потрібно зробити такі дії:

1. Постійна перевірка рівня захищеності і оцінка вразливостей – тестів на проникнення [2]. Постійний аудит та тест на проникнення для виявлення слабких місць у системі захисту фінансових установ. Тест на проникнення включає аналіз елементів IT-інфраструктури, прав доступу, привілейованих облікових записів та можливостей відновлення після можливої атаки.

2. Постійне навчання персоналу для зменшення впливу "людського фактора" на кібербезпеку. Тести на стійкість до соціальної інженерії для перевірки уваги користувачів. Тренінги для виявлення ознак атак, правильної реакції та роботи в інцидентах безпеки. Спеціальні тренінги для банківських працівників, які включають ідентифікацію загроз, дії при атаках та реагування на інциденти.

3. Моніторинг подій і реагування на інциденти [3]. З урахуванням зростання числа кібератак важливо ретельно враховувати всі аспекти безпеки для уникнення негативних наслідків. Основні заходи включають:

1) ведення журналу та записів системного аудиту на всіх пристроях;
2) збір даних, порівняння і аналіз подій з різних джерел;
3) виявлення загроз і реагування на них, аналіз поведінки.

4. Забезпечення безпеки кінцевих точок за допомогою аналізу даних та поведінкового аналізу. Каталогізація зовнішніх систем та блокування підозрілих IP, доменів і веб-сайтів.

5. Керування ідентифікацією і привілейованими обліковими записами. Централізоване керування ідентифікацією та доступом привілейованих облікових записів є ключовим аспектом для захисту конфіденційної інформації від кібератак:

1) використання greylisting для запобігання надання незнайомим додаткам доступу в Інтернет і отримання прав на запис, читання, зміну прав, необхідних для шифрування даних;
2) використання whitelisting на серверах для визначення дозволених команд і додатків, які можна запускати;
3) регулювання прав локальних адміністраторів, використання принципу найменших привілеїв, видача необхідних привілеїв лише на певний час, контроль над додатками;
4) повне приховування облікових даних (паролів, ключів), завдяки чому користувачі не зможуть передати ці дані зловмисникам;
5) керування паролями (складність, періодичність, термін дії);
6) використання багатофакторної автентифікації для всіх користувачів.

6. Моніторинг стану інфраструктури. За допомогою функції керування моніторингом стану інфраструктури здійснюється:

1) моніторинг за рівнем використання ресурсів (CPU, RAM, HDD);
2) аналіз шляхів доступу до даних і виконання виробничої діяльності;
3) оцінка ризиків і впливу.

У зв'язку з постійним тиском кіберзагроз, важливо вдосконалювати бізнес-процеси та використовувати сучасні технології для забезпечення ефективного кіберзахисту. Фінансові установи повинні виявляти та протистояти загрозам, реалізовувати кращі світові практики та вдосконалювати технологічні рішення для мінімізації ризиків та забезпечення безпеки операцій в онлайн-банкінгу та інших платіжних системах.

Список використаних джерел

1. Minfin. URL:https://minfin.com.ua/ua/2021/08/31/70762402/ (дата звернення: 12.03.2024).
2. Poddubnyi V., Sievierinov O., Pustomelnik O. Менеджмент вразливостей як складова частина політики безпеки ІТС. // Системи управління, навігації та зв’язку. Збірник наукових праць 4.62 (2020): 55-58.
3. Ушатов В., Сєвєрінов О.В. "Проблеми оперативного виявлення і реагування на інциденти інформаційної безпеки." (2019).