УДК 004.056.53

ЗАЩИТА ФИНАНСОВЫХ ДАННЫХ В ЭПОХУ ЦИФРОВЫХ УГРОЗ

Долженко А.С., студент гр. ИБт-221, III курс, Горобец Н., студент гр. ИБт-221, III курс
Научный руководитель: Коротин В.О.
Кузбасский государственный технический университет
имени Т.Ф. Горбачева,
г. Кемерово

Аннотация

В современном мире кибербезопасность становится одной из ключевых тем для финансового сектора. С развитием цифровых технологий и увеличением объема электронных транзакций, защита финансовых данных и систем становится критически важной задачей. В этой статье рассмотрим основные аспекты кибербезопасности в финансах, актуальные угрозы и меры по их предотвращению [1].

Введение

Финансовый сектор всегда был привлекательной целью для киберпреступников. Банки, страховые компании и другие финансовые учреждения хранят и обрабатывают огромные объемы конфиденциальной информации, что делает их уязвимыми для кибератак. В последние годы наблюдается рост числа инцидентов, связанных с кражей данных, фишингом и другими видами киберпреступлений. В настоящее время набирают популярность Угрозы цифровой трансформации. Помимо традиционных киберугроз, финансовый сектор сталкивается с новыми вызовами, связанными с цифровизацией бизнеса. Развитие онлайн-банкинга, мобильных приложений и блокчейн-технологий открывает новые возможности для атак. Киберпреступники становятся всё более изобретательными, используя автоматизированные инструменты и методы социальной инженерии для обхода защитных механизмов.

Анализ основных угроз

1. Фишинг: Один из наиболее распространенных методов кибератак, при котором злоумышленники пытаются получить доступ к конфиденциальной информации, такой как пароли и номера кредитных карт, посредством обманных электронных писем или веб-сайтов (Рис.1).

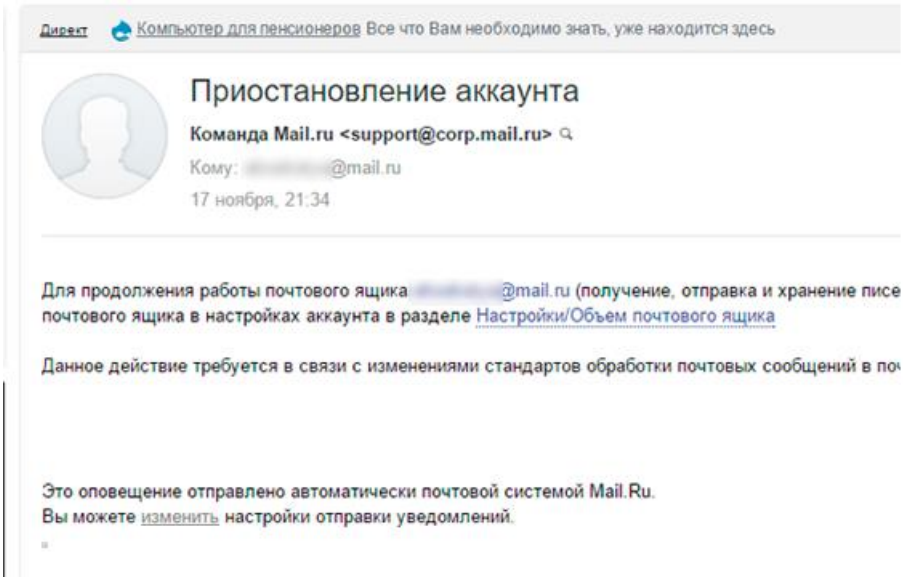

Рисунок 1 –Пример фишингового

2. Вредоносное ПО: Вирусы, трояны и другие виды вредоносного программного обеспечения могут проникать в системы финансовых учреждений, вызывая сбои в работе и кражу данных.

3. DDoS-атаки: Атаки типа "распределенный отказ в обслуживании" направлены на перегрузку серверов финансовых организаций, что приводит к их недоступности для клиентов (Рис.2).

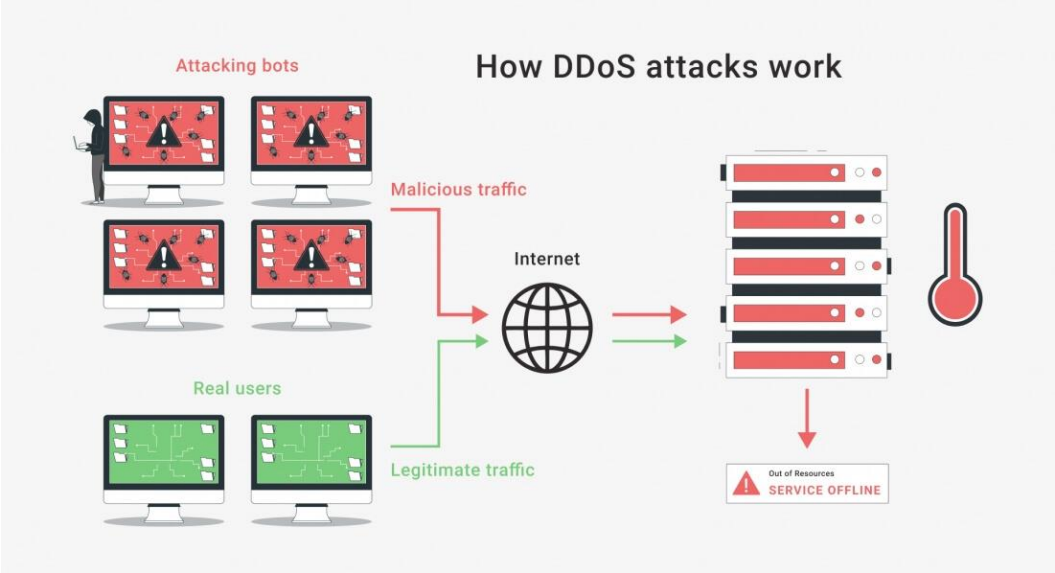

Рисунок 2 – Пример DDoS-атаки

4. Внутренние угрозы: Сотрудники финансовых учреждений могут намеренно или непреднамеренно стать источником утечки данных.

5. Социальная инженерия. Этот метод выходит далеко за рамки классического фишинга. Современные атаки часто включают в себя психологическое манипулирование жертвами через звонки, мессенджеры и социальные сети. Использование сложных сценариев и техник маскировки делает такие атаки особенно опасными.

6. Атаки на цепочки поставок. Финансовые организации часто полагаются на сторонних поставщиков услуг и программного обеспечения. Атака на одного из таких поставщиков может привести к масштабному инциденту безопасности. Примером может служить атака на компанию SolarWinds, которая затронула десятки организаций по всему миру.

7. Криптоджекинг. Это относительно новый вид атаки, когда злоумышленники используют вычислительные мощности чужих устройств для добычи криптовалют. Особенно актуально для компаний, использующих облачные сервисы и высокопроизводительное оборудование [5].

Расширение мер по обеспечению кибербезопасности

1. Обучение сотрудников: Регулярное обучение сотрудников основам кибербезопасности помогает снизить риск внутренних угроз и повысить общую осведомленность о возможных уязвимостях.

2. Использование современных технологий: Внедрение передовых технологий, таких как искусственный интеллект и машинное обучение, позволяет более эффективно выявлять и предотвращать кибератаки.

3. Регулярные аудиты безопасности: Проведение регулярных аудитов и тестирование на проникновение помогают выявить слабые места в системе безопасности и своевременно их устранить.

4. Импортозамещение: Переход на отечественные технологические продукты позволяет снизить зависимость от иностранных поставщиков и повысить уровень безопасности.

5. Управление идентификацией и доступом (IAM). Важный аспект защиты данных заключается в строгом контроле над правами доступа пользователей. Современные решения IAM позволяют внедрять многофакторную аутентификацию, биометрическую верификацию и динамическое управление привилегиями.

6. Безопасность данных на всех этапах жизненного цикла. Финансовая информация должна быть защищена не только в процессе хранения и передачи, но и при её обработке и уничтожении. Шифрование данных на уровне приложения и использование технологии токенизации значительно снижает риски компрометации.

7. Разработка культуры кибербезопасности. Обучение сотрудников должно включать не только технические аспекты, но и поведенческие модели. Формирование корпоративной культуры, где безопасность воспринимается как неотъемлемая часть работы каждого сотрудника, существенно повышает общий уровень защищенности [3] [4].

Актуальные тенденции и будущее кибербезопасности

Искусственный интеллект против искусственного интеллекта. Будущее кибербезопасности связано с использованием AI/ML не только для защиты, но и для нападения. Киберпреступники будут применять алгоритмы для

автоматизации и улучшения своих атак, что потребует разработки новых оборонительных стратегий.

Защита данных в условиях децентрализации. Развитие блокчейна и распределенных систем хранения данных требует пересмотра классических подходов к защите информации. Необходимо разрабатывать механизмы контроля и мониторинга в условиях отсутствия централизованного управления.

Примеры успешных инициатив

Одним из ярких примеров успешных инициатив в области кибербезопасности является Уральский форум «Кибербезопасность в финансах», организованный Банком России. Форум проходит ежегодно и собирает представителей финансовых организаций, экспертов в области информационной безопасности и государственных органов для обсуждения актуальных вопросов и обмена опытом. В рамках форума также проводится молодежная программа, направленная на подготовку кадров для финансового сектора.

Заключение

Кибербезопасность в финансах — это комплексная задача, требующая совместных усилий всех участников рынка. Только при условии постоянного совершенствования мер безопасности и активного взаимодействия между финансовыми учреждениями, государственными органами и образовательными учреждениями можно обеспечить надежную защиту финансовых данных и систем [2].

Подводя итог, можно сказать, что кибербезопасность в финансовом секторе — это непрерывный процесс адаптации к новым условиям и вызовам. Важно не только внедрять современные технологии, но и постоянно повышать квалификацию специалистов, укреплять сотрудничество между участниками рынка и создавать устойчивые экосистемы защиты данных.

Список литературы

1. Уральский форум «Кибербезопасность в финансах» .
2. Форум «Кибербезопасность в финансах» | Банк России .
3. Уральский форум "Кибербезопасность в финансах" - Мероприятия - Интерфакс .
4. Уральский форум «Кибербезопасность в финансах» в г. Екатеринбург 12.02.2024 | All-events - Все бизнес-события .
5. Итоги Уральского форума «Кибербезопасность в финансах» | «ДиалогНаука» .