НЕОБХОДИМОСТЬ СОБЛЮДЕНИЯ ТРЕБОВАНИЙ БЕЗОПАСНОСТИ ДАННЫХ ДЛЯ БАНКОВ И ФИНАНСОВЫХ УСЛУГ

Александру СКРИПЧЕНКО

Департамент Программной Инженерии и Автоматики, группа TI-231 M, Факультет Вычислительной Техники, Информатики и Микроэлектроники, Технический Университет Молдовы, Кишинев, Республика Молдова

Автор кореспондент: Александру Скрипченко, e-mail scripcenco.alexandru@mib.utm.md

Руководитель/научный консультант **Dorian SARANCIUC**, lect.univ.

Аннотация. *В статье анализируется необходимость соблюдения повышенных требований безопасности данных для сферы банковских и финансовых услуг, где защита персональных данных — не просто ключевое конкурентное преимущество, а обязательное условие существования на бизнес-рынке. Отмечается, что международные и отраслевые требования по защите личных и финансовых данных применимы ко всем государственным и частным предприятиям, которые обрабатывают финансовые данные, либо в качестве контролеров данных, либо в качестве обработчиков данных. Перечислены наиболее распространенные киберугрозы для финансовых услуг. Описаны основные мероприятия для предотвращения и решение основных проблем кибербезопасности.*

Ключевые слова: *защита, персональные данные, шифрование, стандарты безопасности, социальное программирование, управление, нарушение*

Введение

Проведение комплексной проверки в отношении собственных систем компании или систем, предоставленных поставщиком, является жизненно важным шагом для обеспечения соответствия требованиям безопасности и минимизации рисков утечки данных.

Наиболее распространенные киберугрозы финансовым услугам в последние годы все больше становились ориентированными на учетные записи: атаки на личные учетные записи, ведущие к краже личных данных и нарушению доверия между поставщиком услуг и клиентом. Вредоносные атаки на системы банкоматов являются растущей тенденцией, наряду с кибератаками, направленными на проникновение в сеть безопасности банков и нацеливание на клиентов с реальных адресов сотрудников [1]. Хотя базовые фишинговые атаки, направленные на клиентов, по-прежнему популярны, они приносят меньшую отдачу, чем захват всей системы и базы данных.

Основной подход к кибербезопасности в учреждении финансовых услуг должен включать прочную организационную структуру и процедуры отчетности по операциям по кибербезопасности; опытный директор по информационной безопасности; безопасная сетевая среда (например, облачные веб-сервисы); и офисная культура, которая включает осведомленность о кибербезопасности во все операции и потоки знаний в офисной среде. Регулярная оценка рисков должна лежать в основе снижения угроз данным в финансовых и банковских услугах, независимо от их размера и бизнес-модели. Отчеты об инцидентах и повторная оценка помогут построить модели угроз и разработать стратегии предотвращения. Реактивного подхода к кибербезопасности уже недостаточно, и для эффективного предотвращения угроз необходима проактивная позиция [2].

Шифрование и виртуальные частные сети

Шифрование данных и надежно зашифрованные облачные веб-сервисы для всех внутренних операций — важнейшее решение основных проблем кибербезопасности.

Существует множество провайдеров виртуальных частных сетей, которые шифруют все сообщения, обеспечивая канал обмена данными между всеми устройствами в корпоративной или личной сети. Хотя количество атак банковского вредоносного ПО сокращается, они становятся все более изощренными: как только хакеры получают контроль над частью сети банка, они могут легко атаковать клиентов массово, рассылая мошеннические электронные письма, чтобы украсть учетные данные пользователей. Использование служб виртуальных частных сетей для обеспечения безопасности системы — это лишь одна из мер, которые необходимо принять. Еще одним примером является двухфакторная аутентификация для доступа сотрудников и клиентов ко всем финансовым и платежным услугам.

Когда атака вредоносного ПО направлена против отдельного пользователя, она направлена на получение финансовых данных или кражу личных данных. Когда вредоносная атака нацелена на сотрудников поставщика финансовых услуг, она имеет гораздо более широкий спектр предполагаемого ущерба: от получения доступа к базе данных пользователей до компрометации всей системы и финансовых ресурсов компании.

Основные стандарты безопасности

Базовые стандарты безопасности для поставщиков финансовых услуг соблюдаются всеми мировыми операторами. Требования PCI DSS, например, применяются ко всем компаниям, которые принимают платежи по кредитным картам онлайн и гарантируют, что компания, обрабатывающая финансовые данные, соблюдает стандарты обработки, хранения и передачи данных. Стандарты PCI DSS диктуют минимальные требования к шифрованию передаваемых данных, защите хранения данных, мониторингу доступа к данным, ограничению доступа к банковским данным клиентов, а также регламентируют аутентификацию доступа к компонентам системы. Сочетание физических и виртуальных методов безопасности защищает хранящиеся пользовательские данные от кражи личных данных, а шифрование передаваемых данных защищает их от перехвата третьими лицами.

Социальное программирование

Обучение персонала — еще один важный шаг в стратегии безопасности данных. Когда речь идет о финансовых услугах, утечка данных чаще всего вызвана вредоносными целевыми атаками опытных хакеров. Однако человеческая ошибка или халатность являются распространенной причиной утечки данных во всем мире. Обучение персонала — это непрерывный процесс, который необходимо проводить в рамках механизма комплексной проверки, чтобы обеспечить осведомленность о случайной загрузке вредоносного ПО и других рисках, связанных с социальным программированием. Каждый сотрудник имеет уникальные учетные данные для доступа, которые необходимо обновлять в ходе обычной работы, что сводит к минимуму риски компрометации и использования в злонамеренных целях.

Управление и отчетность

На уровне управления крайне важно установить прямую подотчетность. Наличие отчета директора по информационной безопасности непосредственно перед генеральным директором может быть одним из факторов, способствующих эффективному снижению киберугроз в крупных банковских и финансовых компаниях [3].

Утечка данных обходится дорого, особенно для компаний, которые предоставляют финансовые услуги, обрабатывают банковские транзакции или привлекают третье лицо для обработки транзакций онлайн-платежей. Средняя стоимость утечки данных в

финансовой отрасли составляет 245 долларов за украденную запись, что делает ее второй по величине после сектора здравоохранения [3]. Это означает, что в зависимости от количества отдельных записей клиентов, обрабатываемых компанией, затраты на борьбу с утечкой данных будут расти все выше и выше. Нарушение финансовых данных клиента приведет к огромным затратам на сдерживание и устранение угрозы: коммуникация и связи с общественностью, следственные действия, услуги службы поддержки, юридические расходы, компенсации клиентам и многое другое. Очевидно, что принятие профилактических мер и мер по снижению рисков во избежание утечки данных приносит пользу не только субъектам данных (клиентам), но также репутации и финансовому благополучию компании. Следует напомнить, что согласно GDPR ЕС, об утечке данных следует сообщать не позднее, чем через 72 часа после обнаружения. Во всех штатах США теперь действуют законы, обязывающие компании уведомлять пользователей об утечках данных [3].

Верно, также и то, что чем быстрее будет выявлено нарушение, тем ниже будут затраты на его сдерживание. Корпоративные исследования показывают, что почти половина утечек данных вызвана злонамеренными преступными атаками, которые гораздо сложнее выявить и сдержать, и, следовательно, они обходятся дороже, чем, например, утечки, вызванные человеческой халатностью или системными сбоями.

Выводы

Одним из основных последствий утечки данных для поставщика финансовых услуг является потеря доверия клиентов и, как следствие, потеря клиентов. Для поставщиков финансовых услуг однажды потерянный клиент обычно теряется навсегда. Для многих организаций информирование клиентов и других заинтересованных сторон о своей стратегии обеспечения безопасности данных является определенным способом смягчить потерю доверия в случае взлома.

Библиография

[1] Introduction to Financial Services: Financial Cybersecurity. - [Электронный ресурс]. Режим доступа: https://crsreports.congress.gov/product/pdf/IF/IF11717 /
[2] Cybersecurity for Financial Services: Best Practices. [Электронный ресурс]. Режим доступа: https://www.netguru.com/blog/cybersecurity-best-practices-finance-services
[3] Banking and financial cyber-security compliance. [Электронный ресурс]. Режим доступа: https://www.ekransystem.com/en/blog/banking-and-financial-cyber-security-compliance