УДК 330.3

ОСОБЕННОСТИ КИБЕРПРЕСТУПНОСТИ В БАНКОВСКОМ СЕКТОРЕ

Панычева А.С., студент гр. У-бс-о-2193, II курс

Киберпреступность – это любая преступная деятельность, в которой используется компьютер, сетевое устройство или сеть. Некоторые киберпреступления совершаются с целью получения денег. С другой стороны, некоторые из них делаются для уничтожения или выведения из строя компьютерной системы. Среди нескольких мотивов совершения киберпреступлений финансовая выгода остается неизменным победителем на протяжении последних многих лет, вытесняя другие мотивы, включая месть, вымогательство и политические мотивы.

Киберпреступность в сфере финансов – это акт получения финансовой выгоды путем преступной деятельности, направленной на получение прибыли, включая мошенничество с использованием личных данных, атаки с помощью программ-вымогателей, мошенничество с электронной почтой и мошенничество в интернете, а также попытки украсть информацию о финансовых счетах, кредитных картах или других платежных картах.

Развитие новых технологий создает дополнительные риски, поскольку обеспечивает почти полную анонимность преступникам, стремящимся использовать технологии для совершения преступлений. Электронные платежные системы облегчают кражу денег, поскольку они более удобны для перемещения больших сумм денег и из-за скорости транзакций трудно контролировать имущество или замораживать его. Киберпреступление трудно обнаружить из-за того, что оно может быть совершено из любой точки мира.

Во многих отношениях банковские и страховые учреждения, наиболее подвержены киберпреступности по сравнению с любым другим типом компаний. Они не только оперируют большими суммами денег, что неизбежно привлекает киберпреступников, но и несут ответственность за финансы своих клиентов. Это означает, что, взломав банковское или страховое учреждение, хакеры могут получить доступ к данным неограниченного количества компаний – клиентов взломанной организации.

Например, в 2022 году российские банки столкнулись с огромным количеством атак на свою инфраструктуру. В ноябре 2022 г. Альфа-банк и еще несколько финансовых организаций потеряли более 60 млн руб., но потери были не из-за хакерских атак. Злоумышленники загрузили в банкоматы поддельные купюры, а реальные деньги, зачисленные на счет, обналичили в других банкоматах. Такая атака оказалась возможной из-за устаревшего ПО в банкоматах, поясняет аналитик исследовательской группы компании Positive Technologies [1].

Обнаруженные и необнаруженные киберпреступления стали более частыми и изощренными, став сегодня одним из основных бизнес-рисков, с

которыми сталкиваются компании по всему миру. У компании больше шансов пострадать от разрушительной утечки данных или мошенничества, чем столкнуться с любыми другими трудностями в бизнесе.

Вот несколько ключевых статистических данных, согласно исследованию Global Banking Fraud Survey 2019 [2], которые показывают более полное представление о состоянии угроз банковской и страховой кибербезопасности,:

– Более 50% компаний, пострадавших от мошенничества, возмещают менее 25% убытков от мошенничества;

– Более 60% банков сообщают об увеличении объемов мошенничества, а более 50% испытывают увеличение стоимости мошенничества;

– 77% банков планируют инвестировать в кибербезопасность на базе искусственного интеллекта и ML.

Проблемы кибербезопасности продолжают расти, и финансовые учреждения, особенно те, которые находятся в процессе цифровой трансформации, становятся мишенью киберпреступников. Коммерческие банки, кредитные союзы, биржевые брокерские фирмы, фирмы по управлению активами и страховые компании, которые поддерживают цифровые транзакции с помощью мобильных приложений, все чаще становятся мишенью и используются злоумышленниками.

Меры кибербезопасности банковских секторов, которые используют мобильные и веб-сервисы для предоставления услуг, как правило, имеют слабую систему безопасности, поэтому многие киберпреступники предпочитают использовать онлайн- и мобильные банковские системы. Кроме того, злоумышленнику удается перехватить информацию о клиентах и сотрудниках и использовать их для проникновения в систему безопасности банка, чтобы украсть банковские данные и деньги.

Наиболее частые виды преступлений в секторе интернет-банкинга:

– Кража личных данных: использование чужих личных данных, таких как имя, дата рождения и адрес, для мошеннических действий является одной из распространенных тактик, применяемых киберпреступниками при работе с электронным бизнесом, особенно с услугами интернет-банкинга. Информация, полученная в результате кражи личных данных киберпреступниками, впоследствии может быть использована для выполнения многих обязательств, таких как открытие новых банковских счетов, получение кредитной карты или займов и получение государственных пособий.

– Фишинг – это стратегии, используемые киберпреступниками для того, чтобы заставить жертв раскрыть свою личную и другую секретную финансовую информацию. Для фишинга существует множество тактик, которые используют кибер-мошенники, но наиболее важной тактикой является отправка фишингового электронного письма клиентам интернет-банка, представляя, что подлинная организация предлагает электронные услуги.

– Вишинг – это способ использования поддельного колл-центра для получения данных клиентов интернет-банка и их финансовых данных. Для

достижения этой цели мошенники используют систему электронной почты, запрашивая у клиентов интернет-банка подтверждение их банковских реквизитов и другой информации в процессе обычной проверки безопасности по номеру телефона, указанному в фишинговом электронном письме.

– Вредоносное ПО. Одной из наиболее опасных кибер-угроз для электронных банковских услуг являются атаки на основе вредоносных программ. При таких атаках создается вредоносный код. Почти каждый вирус имеет две характеристики: во-первых, он обеспечивает незаметное проникновение в систему, а во-вторых, он крадет учетные данные пользователя.

– Взлом ПО. Посредством взлома компьютеров киберпреступники могут проникать в компьютеры и компьютерные сети для кражи финансовой информации, которая впоследствии может быть использована в несанкционированных целях. Различные вредоносные программы могут быть использованы с целью взлома компьютерными мошенниками, такими как троянский вирус.

Поскольку банковское дело является основной системой, в которой люди хранят свои персональные данные месяцами и годами, сохраняют и удваивают свои средства, банковские учреждения должны постоянно улучшать свои системы защиты данных. Создание кибербезопасности банка – это не разовое мероприятие, а непрерывный процесс. Системы необходимо постоянно контролировать с помощью технологий наблюдения, чтобы выявлять лазейки, которые могут быть использованы преступниками. Однако простого решения не существует. Успешная кибер-программа будет основываться на размере учреждения, бизнес-модели и чувствительности собираемых и хранимых данных. Важно, чтобы представление учреждения о своих кибер-рисках оставалось динамичным, поскольку эти факторы меняются и развиваются с течением времени.

Для того, чтобы кибер-безопасность банковских учреждений оставалась актуальной, необходимо соблюдение банками следующих рекомендаций:

- партнерство с другими организациями по безопасности, которые предлагают управляемые услуги для обеспечения защиты;
- внедрение программ непрерывного обучения по вопросам безопасности или оценка текущих программ, чтобы убедиться, что они актуальны и соответствуют текущему ландшафту угроз;
- приобретение инструментов обнаружения и реагирования, которые могут предотвратить атаку;
- использование фаерволла на каждой рабочей станции и подключенном к интернету устройстве в организации, поскольку фаерволл блокирует все сообщения из неавторизованных источников;
- проведение программ информирования потребителей, чтобы клиенты не раскрывали конфиденциальные данные киберпреступникам;
- создание комитета по рискам, который регулярно пересматривает меры кибербезопасности;

– разработка плана антикризисного управления для восстановления после кибератаки и смягчения ее пагубных последствий.

Безопасность данных является первоочередной задачей для финансового сектора, который играет жизненно важную роль в общем функционировании экономики. Банковский сектор имеет особенности, которые делают кибератаки очень серьезной проблемой, как с точки зрения возникновения, так и потенциальной серьезности последствий – атака на банковское учреждение может иметь пагубные последствия для повседневной жизни всей страны или даже региона мира.

Выражаем благодарность за научное руководство Аблямитовой А.Л., ассистенту ФГАОУ ВО «Крымский федеральный университет имени В. И. Вернадского», Институт Экономики и Управления, г. Симферополь

Список литературы:

1 Официальный сайт новостного канала «Ведомости»: «ЦБ о потерях банков из-за хакерских атак в 2022 году». – 2022 – [Электронный ресурс]. – Режим доступа: https://www.vedomosti.ru/finance/articles/2023/02/22/964073-tsb-rasskazal-o-poteryah-bankov-iz-za-hakerskih-atak

2 Global Banking Fraud Survey. – 2019 – [Электронный ресурс]. – Режим доступа: https://assets.kpmg.com/content/dam/kpmg/hr/pdf/2019/global-banking-fraud-survey.pdf