Охрана предприятия

№5 (93), 2024

Оглавление

Главная тема

С чем столкнутся финансовые организации в сфере кибербезопасности в 2025 году

С приближением 2025 года в англоязычном интернет пространстве появляется все больше экспертных прогнозов о том, с какими вызовами столкнутся банки и финансовый сектор в целом в новом году.

Опираясь на экспертные оценки в авторитетных изданиях, в том числе securitylist.com («Crimeware predictions for 2025»), bawn.com («7 Cybersecurity Challenges Facing Fintechs and Small Financial Institutions in 2025), cloud.google.com («Emerging Threats: Cybersecurity Forecast 2025») и ряда других, редакция подготовила и предлагает вниманию читателей следующие прогнозы.

Рост изощренности и изобретательности хакерских атак

Фишинг и программы-вымогатели будут по-прежнему доминировать в арсенале киберкриминала. Хакеры-шантажисты вместо простого шифрования будут все чаще прибегать к модификации данных жертвы или накачке сетевой инфраструктуры неверными, ошибочными данным. Этот метод «отравления данных» затруднит или вообще сделает невозможным восстановление баз данных даже после дешифрования.

В больших масштабах, чем в настоящее время, будут использоваться технологии искусственного интеллекта и машинного обучения для персонализированных атак и эксплуатации уязвимостей. Продвинутые инновации позволяют хакерам проникать в сети незаметно и находиться там продолжительное время, прежде чем взлом обнаружат.

В 2025 году постоянные угрозы будут представлять создаваемые с помощью искусственного интеллекта вредоносы, дипфейки, автоматизированные кампании фишинга. Традиционный инструментарий кибербезопасности не сможет успешно противостоять динамичным атакам, потребует серьезной модернизации, в частности, ускоренного внедрения автоматизированных систем обнаружения аномалий.

Угрозы для API и риски партнерства

API (application programming interface - набор способов и правил, по которым различные программы общаются между собой и обмениваются данными), кровеносная система банковской активности, остается весьма уязвимой для кибератак при отсутствии адекватных мер и технологий защиты, включая строгие протоколы аутентификации, авторизации, непрерывного сетевого мониторинга и другие необходимые практики. Поскольку центральные банки несут большую долю ответственности за работу систем мгновенных платежей, за функционирование цифровой валюты, эксперты ожидают усиления атак на центральные банки и открытый банкинг.

Межпартнерские и клиентские взаимосвязи, облегчающие преступникам проникновение в корпоративную сеть намеченной жертвы, требуют от компаний более требовательного отношения к аудиту систем безопасности друг у друга.

Всплеск финансовых кибератак на смартфоны

В то время как, по наблюдениям экспертов, число атак на персональные компьютеры с использованием традиционных банковских или финансовых вредоносов уменьшается, атаки на смартфоны, напротив, вышли на траекторию роста. И это объяснимо. В 2024 году число атак на мобильные банковские и прочие финансовые приложения на смартфонах выросло вдвое по сравнению с 2023 годом.

Новые угрозы для блокчейн технологий

Все более широкое использование в новых технологиях блокчейна, а также криптовалюты как средства платежа усиливает риски и угрозы. Для защиты сетей, базирующихся на блокчейне и коммуникациях одноранговой сети, эксперты советуют обратить внимание на блокчейны нового поколения – NKN. New Kind of Network – одноранговый протокол нового поколения, обеспечивающий высоконадежный, безопасный и универсальный интернет. Полностью децентрализованная и анонимная одноранговая система обладает огромным потенциалом с точки зрения эффективности, устойчивости и безопасности.

Программы соответствия требованиям регуляторов

В 2025 году финансовые организации должны ожидать ужесточения законодательных и нормативных требований к защите персональных данных, к соблюдению правил и отчетности. Особенно это касается требований информирования об инцидентах безопасности, шифрования данных, регулярного тестирования систем защиты.

Хакеры будут проверять, насколько ответственно организация, намеченная для атаки, относится к своим обязательствам перед регуляторами, будут намеренно шифровать или «отравлять» данные, чтобы создать впечатление нарушений нормативных требований, угрожая донести информацию о нарушениях до регулятора, если жертва не выполнит их требования.

Более жесткие условия и требования со стороны страховых компаний

Особенно в том, что касается шифрования данных, мониторинга, регулярного тестирования систем кибербезопасности, планирования мер реагирования на инциденты. В 2025 году организации, которые не смогут продемонстрировать соответствие ужесточающимся правилам и требованиям, будут испытывать трудности страхования, которое им станет дороже.

Усиление давления по вопросу защиты персональных данных

Организации, обладающие огромными объемами персональных данных и финансовой информации, будут испытывать возрастающее давление на них как со стороны регуляторов, так и со стороны клиентов, требующих внедрять наилучшие практики и процедуры защиты конфиденциальности. Последние предусматривают, в частности, шифрование данных, хранящихся и в трафике, усиление контроля доступа, систематический аудит и тестирование инструментов кибербезопасности.

Квантовые вычисления потеснят традиционные алгоритмы шифрования

Хотя сегодня еще рано говорить об устарелости нынешних стандартов шифрования, финансовые организации должны начать готовиться к постквантовой криптографии, к переходу на новые стандарты, устойчивые к атакам на квантовых компьютерах.

Технологии, методологии

Как видеоаналитика трансформирует охрану периметра

Традиционно эффективность видеонаблюдения в решающей степени зависела от способности оператора вести непрерывный мониторинг в поиске потенциальных угроз несанкционированного вторжения в охраняемую зону. При этом большую проблему создавали технические помехи и ложные сигналы. Без огромной затраты человеческой энергии отдача видеонаблюдения стремилась к нулю. Поэтому развитие охранного видеонаблюдения на первых этапах концентрировалась на технических характеристиках. Увеличивались скорость записи, разрешение, угол обзора, светочувствительность.

Качественный скачок произошел с внедрением роботов, искусственного интеллекта, видеоаналитики. Именно эти инновации проложили путь к преодолению главной сложности – расчистке информационного шума.

К фоновым помехам могут относиться дождь, снег, град, падающая листва, качающиеся ветви деревьев, тени от облаков, вибрация самой видеокамеры. «Все это может вызвать срабатывание обычного видеодетектора движения; в результате оператор может прекратить обращать внимание на его сигналы и, как следствие, пропустить тревожное событие – пересечение периметра», отмечает Е. Ерошин (компания «БайтЭрг», разработчик и производитель мобильного видеонаблюдения). Ложный сигнал тревоги при грубой настройке могут вызывать птицы, небольшие животные.

Видеоаналитика способна решать сложные технические задачи. В частности, преодолевать фоновые помехи, возникающие вследствие ухудшения погодных условий, выявлять ложные тревоги из-за движения животных, определять движение нарушителя, отличающееся от стандартного, контролировать периметр большой протяженности.

Главное преимущество видеоаналитики видится в кардинальном снижении роли человеческого фактора в процессе обнаружения и реагирования на потенциальный инцидент. Поскольку значительная часть видеоданных автоматически отсеивается за ненужностью, нагрузка на оператора, каналы связи, систему архивации существенно уменьшается.

Возможности искусственного интеллекта позволяют современным умным видеокамерам идентифицировать человека, его пол, цвет волос, возраст, что значительно расширяет функциональный спектр систем обнаружения вторжений, снижает количество ложных срабатываний.

Таким образом, видеоаналитика на базе ИИ предоставляет недоступные ранее возможности точно, безошибочно фиксировать, отслеживать, классифицировать, а главное – предотвращать инциденты безопасности по всему периметру охраны.

Одно из перспективных направлений – умные тепловизоры. Работающие на принципе излучаемого тепла, они устраняют помехи, связанные с недостаточным освещением, ненастной погодой, природными или искусственными заграждениями. Действуют круглосуточно. На их работу не воздействуют прямо падающие солнечные лучи, световые отблески, огни автомобильных фар и уличных фонарей, другие световые явления. Их сенсоры точно улавливают появление, присутствие человека на значительном расстоянии (International Security Journal, internationalsecurityjournal.com).

Интеграция тепловизоров и PTZ камер видеонаблюдения (камер с приводом для поворота, наклона и зуммирования), считают эксперты, на порядок повышает безопасность. Тепловизор, обнаружив объект, сигнализирует об этом PTZ устройству, которое разворачивает камеру к объекту и отслеживает его перемещение, одновременно посылая сигнал оператору. Продвинутые системы видеоаналитики определяют геолокацию нарушителя.

Интеграция с другими цифровыми продуктами и технологиями, например, с тревожной сигнализацией, устройством «умного дома», системами массового оповещения многократно увеличивают функциональность и эффективность охраны периметра.

Роботы революционно преображают охранную индустрию

Уже сегодня искусственный интеллект существенно воздействует на процессы управления рисками. Роботы появляются в разных сферах охранной индустрии. Но для ученых и практиков многое остается не ясным. Каков реальный потенциал роботов в обозримом будущем? Каковы социально-культурные последствия их внедрения в повседневную работу охранных предприятий, корпоративных служб безопасности? Нужно ли приближать их внешний дизайн к человеческому облику и что это даст?

Эти и другие вопросы задают эксперты, в их числе Уильям Планте, директор по управлению рисками компании Everon Solutions (интегрированные решения по безопасности). Он указывает на уникальность задач, которые стоят перед роботами-охранниками: автономный режим работы в закрытых помещениях и на открытом пространстве, непрерывное взаимодействие с операторами, высочайший уровень чувствительности и восприятия окружающей среды, способность принимать в определенных обстоятельствах самостоятельные решения (Security Management, August, 2024).

Более конкретно предъявляемые роботам-охранникам требования выглядят следующим образом:

Автономный режим работы. Предполагает экипировку роботов видеокамерой, лидарами (оптическими локаторами, дальномерами), системой космической навигации или SLAM (навигация и картографирование). Названные технологии позволяют роботу автономно передвигаться на определенной территории, преодолевая возможные препятствия и помехи.

Аудио и видео сенсоры. Обеспечивают возможность идентифицировать и реагировать на звуковые и визуальные сигналы, а также – с использованием ИИ – распознавать людей по лицам, языку жестов и движения.

Взаимодействие с операторами. Здесь также требуется способность различать людей по особенностям речи, лицу и жестам.

Разработка и внедрение некоторых программ еще в начале пути. Сегодня функции большинства роботов в сфере безопасности сводятся к базовым задачам: патрулированию по заранее выбранному маршруту, фиксации и передаче сигнала об аномалиях.

На повестке дня – создание роботов с LLM и CNN. (Для справки: LLM - «большая языковая модель», предназначенная для обработки естественной речи, в частности для генерации текста; CNN – «сверточные нейронные сети», способные в отличие от традиционных нейронных сетей автоматически выявлять важные характеристики изображений, т.е. обеспечивать «компьютерное зрение»). Вооруженные продвинутыми технологиями на базе ИИ роботы могут автономно ориентироваться в сложной окружающей среде, анализируя колоссальные объемы данных в реальном времени, самостоятельно принимая решения.

Мечты иногда сбываются. В Китае создали робота-полицейского RTG, оснащённого искусственным интеллектом. Устройство, придуманное и сконструированное командой Чжэцзянского университета, плавает и работает совместно с другими роботами. Робот способен выдерживать падения с высоты и стабилизироваться при кувырках и ударах, никогда не опрокидываясь. В системе функционирования робота используется автономный алгоритм с процессом самообучения, помимо этого, он оборудован мощной системой слежения. Такой «полицейский» может атаковать цели на скорости до 35 км/ч и координировать действия с другими роботами для захвата объектов. Метод обезоруживания преступников — набрасывание сетки на правонарушителя.

В Швейцарии появился робот-охранник с искусственным интеллектом. «Он может двигаться по ровной местности, преодолевать препятствия, подниматься на одну или две ступеньки, потому что мы используем колеса и ноги», — говорит Алессандро Морра, генеральный директор и основатель фирмы-производителя Ascento. Его тепловизорная камера обнаруживает людей и транспортные средства, а 360-градусная камера захватывает изображения окружающей обстановки. Робот может общаться через прямую трансляцию с резервным оператором в центре управления. Сейчас готовится робот с компетенцией автоматических ежедневных отчетов о безопасности (по материалам веб-сайта guardinfo.online).

Российская компания по продаже компьютерной техники «Бион» наняла произведенного в Перми человекоподобного робота, который работает охранником и консьержем в одном из подмосковных офисов. В обязанности робота входит проверка наличия доступа у посетителей офиса. В его ПО предусмотрена система контроля и управления доступом, позволяющая сканировать паспорта людей и сверять документы с базой данных. В случае отсутствия разрешения гость может попросить робота позвонить секретарю. В этом случае робот

воспроизведет видеозвонок, после чего секретарь сам опознает человека, выяснит детали его визита и даст роботу команду пропустить гостя.

В Перми же разработан робот "Скорпион", созданный для патрулирования территории и охраны правопорядка в уличных и промышленных условиях. Для этого умный охранник оборудован гусеничной платформой, системами распознавания лиц и навигации. По словам разработчиков, робот способен передвигаться в антропогенной, то есть созданной для человека, среде: по лестницам, бордюрам, по снегу, песку, грязи и воде. Если на пути "Скорпиона" возникают препятствия, он распознает их с помощью лазерного сканера и ультразвуковых датчиков. Помимо этого, робот оснащен ГЛОНАСС-приемниками для локализации в пространстве и может патрулировать территорию в полностью автономном режиме. Им удаленно управляет оператор (rg.ru).

У. Планте обращает внимание, что интегрированные в роботы ИИ технологии, в первую очередь, упомянутая выше большая языковая модель LLM, помогают предотвращению инцидентов безопасности, поскольку обладают способностью улавливать и интерпретировать малейшие нюансы речи и поведения людей. Так они определяют состояние тревоги, беспокойства, страха как возможный показатель опасности.

Кроме того, LLM улучшает процессы принятия решений, наделяя робот компетенцией анализа сложной ситуации, в результате которого робот генерирует разные стратегии реагирования с учетом предполагаемых последствий каждой из стратегий.

Другая многообещающая характеристика роботов новейшего поколения – способность обучаться и адаптироваться к рабочим условиям. К примеру, робот фиксирует появление ящиков у запасного выхода, что может помешать экстренной эвакуации. Он отодвинет ящики в сторону и, запомнив эту операцию, проверит все другие двери, не забыв доложить о непорядке дежурному оператору охраны.

Такие вот чудеса!

Нужно ли вести переговоры и платить хакерам шантажистам?

Проводимые за рубежом опросы на эту тему демонстрируют растущую готовность организаций платить вымогателям выкуп, тратя на эти цели миллионы долларов. Компания ExtraHop (сетевой анализ на основе искусственного интеллекта) утверждает, что 83% корпораций, подвергшихся атаке шантажистов 2022 году, откупились, по меньшей мере, один раз.

Редакция Chief Security Magazine (CSO) собрала мнения разных экспертов.

Если хакерская атака угрожает самому существованию компании, пишет специалист по кибербезопасности Даниэль Меллен, то у нее просто нет иного выхода, как откупиться.

Леонард Клейман, директор отдела IT австралийской фирмы Enablis (кибербезопасность), утверждает, что решение принимается на основе анализа уравнения «цена – выгода», подсчета прямых и косвенных издержек, связанных с требованиями преступника. «Самый простой расчет позволяет сравнить ежегодный доход бизнеса с требуемой злоумышленниками суммой выкупа и сделать вывод».

Собственно, перед каждой из жертв вымогательской программы стоят два вопроса: идти ли на уступки шантажистам, и если да, то как вести переговоры?

Позиции экспертов разделились.

Одни настаивают, что нельзя идти на контакты с преступниками, как с практической, так и с этической точек зрения, тем более, соглашаться на их требования.

Другие допускают возможность переговоров и выкупа. При этом рекомендуют приглашать профессиональных переговорщиков, которые «собаку съели» на контактах с хакерами. Главные задачи в переговорах: сбор информации о злоумышленниках, изучение их требований, обсуждение условий, короче – торг.

«Согласие на контакты полезно по нескольким причинам, говорит Николсон из Pentest People (тестирование систем защиты сетей). Во-первых, тем самым выигрывается время для сбора дополнительной информации о масштабах атаки и подготовки к восстановлению заблокированной хакерами сети. Во-вторых, изучаются методы, уточняются требования преступников, их готовность к уступкам и тому подобное. В-третьих, специалисты по кибербезопасности получают возможность идентифицировать уязвимости в системах информзащиты, остановить распространение вредоносной программы, оценить состояние резервного копирования.

Коммуникация с хакером ведется, как правило, анонимно одним из сотрудников атакованной фирмы или приглашенным специалистом.

Случается, что в ходе переговоров хакеры непроизвольно выдают информацию, помогающую более точно оценить размеры зараженных/зашифрованных корпоративных данных, что очень важно для урегулирования кризиса и предотвращения подобных инцидентов в будущем.

Умелые переговорщики способны умерить запросы хакеров, получить ключ дешифровки до окончательного завершения сделки.

Важным аспектом переговоров является угроза оглашения вымогателями конфиденциальной информации, которой они овладели. Последние годы хакеры все чаще используют этот прием в качестве ультиматума, надо отметить, достаточно действенно.

Многие преступники перешли от блокировки корпоративных данных к прямой их краже, угрожая их оглаской. Последствия могут быть весьма удручающими для репутации компании-жертвы.

В ряде случаев хакеры делают ставку на информацию сугубо личного характера. Они охотятся за персональными данными акционеров и топ-менеджмента, за их перепиской в электронной почте, финансовой информацией.

Нельзя упускать из виду этический аспект, полагают эксперты, выступающие против переговоров и уступок хакерам, в первую очередь, тем злоумышленникам, которые представляют не криминал, а политические группировки и недружественные страны. В противном случае, утверждают они, наносится непоправимый репутационный ущерб в глазах как регуляторов, так и клиентов жертвы.

Противники любых контактов с шантажистами аргументируют позицию доводом: уступки только поощряют вымогателей на новые, еще более масштабные и изощренные преступления. «Не платите ни цента, - призывает Клейман, - откупные вознаграждают и вдохновляют на новые злодеяния».

Но практически все специалисты едины во мнении, что для защиты от хакеров-шантажистов целесообразно заблаговременно, не дожидаясь атаки, сформировать и иметь наготове «группу реагирования» из числа сотрудников компании, куда бы вошли айтишники, юристы, представители правления. Многое зависит от скорости реагирования на инцидент. Технари и юристы оценивают масштабы взлома баз данных, определяют вид и характер атаки, потенциальное воздействие на деятельность компании, взвешивают «за и против» переговоров и возможности откупиться, координируют свои планы и действия с акционерами, отраслевыми регуляторами, страховыми компаниями, органами правопорядка.

Банковская безопасность

Нулевое доверие для банковской безопасности

Zero Trust («нулевое доверие») – модель безопасности, разработанная аналитиком проекта компании Forrester Research Джоном Киндерваго еще в 2010 году. Изучая фундаментальные проблемы безопасности сетей, он убедился, что «доверие есть то, чем пользуются и что эксплуатируют люди». И в этом главная причина уязвимостей. Другим словами, доверие и есть уязвимость (paloaltonetworks.com).

Базовый принцип нулевого доверия – «никому не верьте, всё проверяйте» - означает постоянную оценку каждого соединения, будь то работники компании, клиенты, партнеры, либо приложения, мобильные гаджеты и другие устройства. Постоянный мониторинг сети, конечных точек, доступа пользователей позволяет своевременно вскрывать аномалии в трафике данных, странное, необычное поведение пользователя.

Нулевое доверие обязывает всех без исключения пользователей корпоративной сети проходить процедуру аутентификации, авторизации, прежде чем получить доступ к приложениям и базам данных.

Д. МакНайт, Т. Типтон и У. Томило, авторы публикации на веб-сайте консалтинговой компании Crowe LLP (crowe.com), рекомендуют следующие шаги для реализации принципа нулевого доверия в банковской сфере.

Анализ сети

Компания должна продумать четкую организацию потоков данных, всех цифровых материалов, банковских операций. Это необходимое условие для идентификации потенциальных уязвимостей. Данный шаг особенно значим для банковской среды, характеризуемой множеством взаимосвязанных систем и платформ.

Определение границ доступа для каждого пользователя

Нулевое доверие подразумевает правило «минимальной привилегии», означающее, что любой пользователь допущен только к тому объему данных, который необходим для выполнения служебных обязанностей.

Мультифакторная аутентификация

Это ключевой компонент концепции нулевого доверия.

Выбор программных решений, отвечающих требованиям нулевого доверия

Выбор зависит от организационной структуры банка, задач и характеристик. К примеру, финансовой организации требуется решение, предусматривающее микро-сегментацию сети, - способ предупредить захват злоумышленниками всей информационной инфраструктуры в случае взлома одного из сегментов. Сегментация чрезвычайно полезна для банка, где службы сталкиваются с разнородными рисками и угрозами.

Постоянный мониторинг безопасности сети

Только таким способом можно вовремя заметить необычное поведение в сети, а, кроме того, оценить эффективность влияния этого принципа на банковские операции.

Регулярные тренинги персонала и обучение клиентов

Внедрение принципа нулевого доверия чревато дополнительными неудобствами для работников банка и их клиентов. И это не единственное препятствие.

Переход от традиционной сетевой архитектуры к более современному, микро-сегментному дизайну требует времени, планирования, инвестиций в технологии, ресурсов, в том числе кадровых для управления ими. При этом некоторые финансовые организации пользуются устаревшими системами, которые невозможно адаптировать к новым требованиям, а надо полностью заменять, на что не всегда хватает средств и ресурсов.

Поскольку концепция нулевого доверия родилась в недрах кибербезопасности, то она и продолжает развиваться, практически не выходя за границы этой сравнительно молодой дисциплины. При этом бросается в глаза явная недооценка значения систем физической охраны в имплементации нулевого доверия.

Между тем, криминал с каждым годом все более изощренно комбинирует и сочетает цифровые и физические средства для достижения своих целей. Достаточно упомянуть приемы социальной инженерии. И банки здесь не исключение.

Хотя с точки зрения угроз для финансовой сферы кибербезопасность сегодня приоритетна, вложения в физическую охрану банков сродни хорошему кредиту: возврат с процентами гарантирован.

Даже для тех организаций, которые имеют в наличии квалифицированных охранников, разветвленное видеонаблюдение, систему электронных пропусков, всегда сохраняется риск несанкционированного проникновения. Например, испытанным методом прохода «паровозиком» двух и более лиц по одному предъявленному идентификатору.

Виктория Рис, постоянный автор статей в журнале Security Journal Americas (securityjournalamericas.com), указывает на три стратегии, абсолютно необходимые для защиты банков в контексте нулевого доверия:

- современные средства контроля на входе и выходе (система контроля и управления доступом – СКУД);

- надежный процесс проверки и выдачи разрешения на физический доступ;

- постоянная актуализация корпоративных инструкций и политик по вопросам безопасности.

Если, к примеру, банковский служащий увольняется, то в базах данных электронных пропусков, в программах распознавания по лицам, в режиме работы автоматических дверей, замковых ригелей и так далее должны быть своевременно и одновременно внесены изменения, исключающие его/ее возвращение к рабочему месту.

Технологии технологиями, но ключевая роль принадлежит не им, а тем, кто отвечает за безопасность. Сегодня эта ответственность, считает Вероника Рис, должна возлагаться на весь банковский коллектив – от директора банка до операционистов.

Пуш-платежи: преимущества и риски

Оплата через пуш — один из способов использования пуш-уведомлений, то есть коротких сообщений, всплывающих на экране компьютера или мобильного телефона с различной информацией. Она позволяет совершать платежи без ввода данных карты и паролей. К примеру, при совершении покупки в интернет-магазине на телефон приходит пуш-уведомление с запросом на подтверждение платежа. Нажимаете кнопку «подтвердить» и платеж проходит. Уведомления приходят моментально, что обеспечивает оперативность и удобство в управлении финансами.

Преимущества оплаты через пуш очевидны: быстрота и удобство, вы всегда в курсе своего финансового баланса.

С другой стороны, «санкционированное мошенничество с push-платежами» стало одним из новых опасных видов мошенничества, который заключается в манипуляциях с физическими лицами (но и организации среди жертв - не исключение) с целью кражи денежных средств. Преступники по телефону, по электронной почте убеждают потенциальную жертву перевести им деньги с помощью мгновенного платежа. Злоумышленники могут выдавать себя за легитимную организацию, подсовывают поддельные счета, убеждают приемами социальной инженерии, дабы люди поверили, что речь идет о добросовестной, легальной трансакции.

Ущерб от таких преступлений значителен и с каждым годом увеличивается быстрыми темпами. Рост только в одной Великобритании в 2023 году составил 12% и выразился суммой 459.7 миллионов фунтов стерлингов. Преступники предлагают сделки, которые выглядят слишком хорошо, рассчитывают на внезапность предложения, сулят высокую прибыль.

По данным СМИ, обманутым клиентам возвращается в среднем в мире не более 20% денег, утраченных в результате пуш-мошенничества.

Западный эксперт Джессика Линдси называет причины, по которым банки могут принять решение не возмещать клиентам убытки:

- Если клиенты не прислушиваются к предупреждениям своего банка
- Если они опрометчиво делятся своими учетными данными
- Если они не предпринимают шагов, чтобы разобраться, что за человек обращается к ним с предложением
- Если они лгут банку
- Если они проявляют вопиющую халатность
- Если они не получат результат подтверждения получателя платежа. Это схема, при которой клиенты уведомляются об имени получателя платежа, а не только о номере счета и коде сортировки. (metro.co.uk)

Тристан Принц, эксперт по финансовому криминалу в кредитном бюро Experian, перечисляет ряд «ключевых моментов», которые следует, по его мнению, иметь в виду финансовым организациям, формулируя и осуществляя стратегию противодействия этому виду мошенничества.

Возросшая роль данных и технологий

Банкам необходимо форсировать внедрение продвинутой аналитики данных и машинного обучения алгоритмам. Именно новые технологии в состоянии помочь в идентификации подозрительных платежей в режиме реального времени. Анализируя обширные массивы трансакций, банки могут разрабатывать прогностические модели, мгновенно реагирующие на аномалии и предотвращающие обманные платежи.

Ощутимое влияние могут оказать технологии и на процессы верификации клиентов. Биометрическая аутентификация, включая отпечатки пальцев и распознавание по лицам, обеспечивают более высокий уровень безопасности по сравнению с традиционными паролями.

Единый для организаций подход к вопросу об информационном обмене

Полная и доступная для банков и правоохранительных органов картина мошеннической деятельности, банковских счетов криминала позволяет переходить от пассивной тактики реагирования к проактивным действиям. Более тесное взаимодействие банков и правоохранительных органов, прежде всего в обмене информацией, подчеркивает Тристан Принц, - «прямой путь к существенному снижению потерь как для финансовых организаций, так и для их клиентов» (finextra.com).

Другой эксперт, Кристиан Томс, партнер международной юридической компании Squire Patton Boggs, обращает внимание банковских клиентов на необходимость более внимательного отношения к электронным платежам. Особенно это касается тех случаев, когда запрос приходит по онлайновым коммуникациям. Хотя такой подход, возможно, и противоречит нынешней тенденции онлайновой культуры, но все же телефонный звонок в ваш банк с проверкой запроса не повредит, а, возможно, убережет ваши деньги (internarionalbanker.com).

Банки, со своей стороны, должны информировать клиентов о рисках и признаках мошенничества, учить их защищать себя. А именно:

Самостоятельно проверять все получаемые запросы на оплату, если они являются неожиданными или кажутся необычными.

Никогда не раскрывать персональную и финансовую информацию (данные банковского счёта, дата рождения, пароли) неизвестным или непроверенным лицам или организациям.

Обращать особое внимание на адреса электронной почты, номера телефонов или URL-адреса веб-сайтов, указанные в запросах на оплату. Мошенники могут использовать слегка измененные или вводящие в заблуждение контактные данные, чтобы создать ощущение подлинности.

Доверять своей интуиции, если что-то покажется необычным или «слишком хорошим».

Основные правила безопасности интернет-банка

Проводимые банками и исследовательскими центрами опросы россиян относительно пользования интернет-банком сильно разнятся. Отчасти из-за путаницы в терминах (интернет-банк, мобильный банк, банковские приложения). По данным исследовательского центра НАФИ, достаточно консервативным, доля пользователей интернет-банком среди взрослого населения России в 2018 году составляла 17%, в 2020 году – 39%, сегодня близка к цифре 50%.

В США, где 78% взрослого населения пользуются онлайн банкингом, каждый третий из них испытывал проблемы с безопасностью своих аккаунтов. Главные риски – фишинг, вредоносы, кражи персональных данных, хакерские атаки. Их можно было бы избежать, по крайней мере, ощутимо минимизировать, если бы все пользователи онлайн банкинга прислушивались к советам экспертов.

Самый простой, и, тем не менее, наиболее часто игнорируемый способ защиты – надежный пароль.

Тони Каккаво, блогер, в недавнем прошлом глава компании по управлению паролями (teampassword.com), напоминает, что хорошо защищенный пароль состоит минимум из 12 знаков, а лучше из 16 и более, обязательно включая выбранные наугад заглавные и строчные буквы, цифры, знаки препинания, символы разных классов.

Парольные фразы (фразы-пароли) могут быть полезны, если ими правильно пользоваться, но важно помнить, что хакеры держат в уме возможность взлома через тестирование популярных выражений, пословиц, стихов.

Что еще надо иметь в виду, составляя пароль? Не практиковать легко разгадываемые данные, такие как годы своего рождения или клички домашних животных. Хранить пароли в недоступном для посторонних месте, если их не удерживает память. Но уж точно не на клочках бумаги на рабочем столе.

Другие рекомендации экспертов:

Регулярно меняйте пароли. Раз в несколько месяцев, используя парольные генераторы («менеджеры паролей»).

Не пренебрегайте двухфакторной аутентификацией. При этом желательно избегать СМС-сообщений, учитывая рост SIM-swapping – атак с подменой сим-карты.

Воздерживайтесь от Wi-Fi услуги в общественных местах для операций со своими банковскими счетами.

Следите за появлением новых мошеннических схем.

Регулярно проверяйте банковские счета, по меньшей мере, раз в неделю.

Проявляйте бдительность в отношении всего того, что вам покажется необычным, аномальным, подозрительным.

Что касается последнего предупреждения, то это может быть «любой непонятный человек, текст, сообщение, СМС или входящий звонок, который вам не нравится… Стопроцентная паранойя, стопроцентная аккуратность и стопроцентное недоверие. Вот единственный ключ сегодня, в 2024 году, чтобы спастись от киберпреступников. То же самое относится к корпорациям», – отметил

Евгений Питолин, сопредседатель комитета по ИБ ассоциации QazTech, выступая на конференции Kursiv Ecosystems Forum в Алма-Ате, октябрь 2024.

Общение с банком не должно проходить целиком через одно устройство – телефон, считает Питолин. «Если он окажется заражён трояном (а такое случается, трой может оказаться даже в заводской прошивке), то будет показывать тебе всё правильно (оплата коммуналки 2712,65 р.), а отправит в банк совсем другое (на какую-то левую карту 10 000 р.). Поэтому вместо приложений используй сайт онлайн-банка на компе/планшете/телефоне, а на другой телефон получай смс от банка с уведомлениями и кодами подтверждения».

Подробные разъяснения и рекомендации предлагает Лаборатория Касперского. В частности:

- Будьте бдительны при получении сообщений, в которых банк просит вас предоставить персональные данные или перейти по ссылке в свою учетную запись, – банки никогда не запрашивают конфиденциальных данных.
- Не переходите по ссылкам, которые предположительно ведут на сайт банка. Вместо этого введите веб-адрес сайта прямо в браузере и убедитесь, что перешли на реальный, защищенный сайт.
- Обращайте внимание на подозрительную активность во время работы с интернет-банком: например, если увидите странные всплывающие окна, блокируйте их немедленно.
- Включите многофакторную или биометрическую аутентификацию, если это возможно.
- По возможности используйте одноразовые пароли для подтверждения переводов, платежей и изменения настроек.
- Используйте только официальный сайт или приложение банка.
- Всегда завершайте сеанс работы с онлайн-банком и настройте автоматический выход из учетной записи в случае бездействия, если он не включен по умолчанию.
- Никогда не передавайте конфиденциальную информацию – банки не запрашивают таких сведений, как номер социального страхования или PIN-код.
- Анализируйте историю операций, чтобы не пропустить подозрительную активность – платежи или переводы, которых вы не совершали, – и немедленно сообщайте в банк о таких транзакциях.
- В случае потери или кражи банковской карты сразу же сообщите об этом в банк.
- Регулярно обновляйте все приложения на устройстве.

Финансовые расследования

Впервые в истории США крупный банк признал участие в отмывании грязных денег

Toronto-Dominion Bank (TD Bank), десятый по величине в США и второй в Канаде, признал вину в отмывании денег наркобизнеса и согласился на рекордный в истории Америки штраф в размере более 3 миллиардов долларов.

В течение почти 10 лет TD Bank не предпринимал мер по улучшению программы противодействия отмыванию денег, констатировала заместитель помощника генерального прокурора США Николь Аржентиери. В результате банк стал легкой приманкой для злоумышленников.
Коррумпированные банковские работники помогли «промыть» десятки миллионов грязных денег криминальных организаций.

Согласно судебным документам, в период между январем 2014 г. и октябрем 2023 г. банк допускал всеобъемлющие и системные недочеты в процедурах, предусмотренных антиотмывочным законодательством, и не принимал никаких мер по исправлению ситуации. В частности, в материалах расследования говорится о недофинансировании программы борьбы с отмыванием. Топ-менеджмент следовал бюджетной стратегии, предусматривающей замораживание уровня расходов от года к году, несмотря на рост прибылей и профиля рисков (risk profile) в течение всего этого времени.

В вину TD Bank поставлено отсутствие автоматического непрерывного мониторинга электронных денежных переводов и других видов банковской активности. Так, 92% общего объема трансакций в период с 1 января 2018 г. по 12 апреля 2024 г. практически не отслеживались. Речь идет о сумме 18.3 триллионов долларов.

В итоге одной только отмывочной сети удалось за три года (2018 – 2021) прокачать через TD Bank 470 миллионов долларов. Личность, стоящая за ее организацией, известна в банке под именем Давид. Расследование показало, что Давид пытался использовать для преступных целей разные финансовые институты и пришел к заключению, что легче всего это делать через TD Bank. Разумеется, не без помощи банковских работников, которые за обработку вне правил 470 млн. долларов были вознаграждены подарочными картами общим номиналом 57 тыс. долларов.

Всего раскрыты три преступные сети с участием более 20 человек, включая банковских инсайдеров. Во второй мошеннической схеме 5 служащих TD Bank помогли отмыть 39 миллионов долларов для колумбийских наркодельцов. Третья отмывочная сеть благополучно прокачала через банк 120 миллионов долларов.

Скандал вокруг TD Bank примечателен тем, что банк первым в истории страны признал свою вину в сговоре для отмывания денег. Он также признал свою вину в нарушении закона о банковской тайне.

Несмотря на исторический прецедент, критика в адрес финансовых организаций США со стороны политиков и прессы не ослабевает, отмечают авторы публикации в The Hill (печатное и интернет-издание о политике) Дж. Шапиро и С. Лейн.

Сенатор Элизабет Уоррен, известный критик больших банков, считает назначенный TD Bank трехмиллиардный штраф не более чем «обычной ценой за бизнес». Уоррен и ее сторонники в правящем классе давно требуют более суровых мер к крупным банкам, замеченным в нарушении законодательства, вплоть до закрытия.

Проблема отмывания денег в Америке имеет давнюю историю. Вашингтонский журналист Питер Стоун напоминал, что осенью 2020 года интернет медиа-компания BuzzFeed и Международный консорциум журналистов-расследователей опубликовали документы, свидетельствующие, что с 1999 по 2017 год банки подавали отчеты в подразделение Министерства финансов, которое называется «Сеть по борьбе с финансовыми преступлениями» или FinCEN, о подозрительной деятельности на сумму 2 триллиона долларов.

США стали магнитом для отмывателей денег со всего мира, в значительной степени из-за системных проблем регулирования. «США по-прежнему являются предпочтительным местом для отмывания денег, картелей и коррумпированных политиков во всем мире», – рассказывает Росс Делстон, независимый эксперт. «Наша система борьбы с отмыванием денег заполнена не трещинами или щелями, а, скорее, изобилует открытыми дверями, окнами и дырами» (katehon.com/ru).

Риски и угрозы

Цена информационных утечек в финансовой сфере

Цену, которую платят организации за утечки информации, определить не просто. Ясно одно – она невероятно высока.

Последнее исследование IBM «Cost of a Data Breach Report 2024» показывает, что с марта 2023 года по февраль 2024 года средняя в мире цифра потерь для одной организации составляет 4.88 миллионов долларов США. Она на 10% больше показателя за соответствующий предшествующий период времени (март 2022 – февраль 2023).

В опросе участвовали 604 компании (включая банки), представляющие бизнес 16 регионов и стран мира. Из них 70% испытали «существенные и очень существенные» потери в результате утечек.

Наибольший урон несут американские компании (в среднем 9.36 миллионов долларов). На втором месте – Саудовская Аравия и Эмираты (8.75 миллионов). Далее идут Канада, Великобритания, страны АСЕАН, Италия, Германия, Бразилия и другие государства по списку, в котором России нет.

По размерам ущерба финансовый сектор прочно удерживает второе место после здравоохранения. Но если в здравоохранении потери снизились по сравнению с предшествующим годом на 10%, то в финансовой сфере они возросли более чем на 3% и составили в среднем 6.08 миллионов долларов на каждую организацию.

Что касается причин утечек и сливов данных о клиентах в банках, то здесь первое место за злоумышленными хакерскими атаками (более половины инцидентов). Каждый четвертый успешный взлом происходит из-за слабой информзащиты и/или ошибок со стороны персонала. При этом айтишникам требуется (опять же в среднем) 168 дней на обнаружение утечки. Это меньше, чем в целом по всем организациям (194 дня), но, отмечают эксперты, слишком большой промежуток времени – чуть меньше полугода!

Чтобы справиться с проблемой, финансовые организации вынуждены увеличивать расходы по таким статьям бюджета как «реагирование на инциденты безопасности» и «управление идентификацией и контролем доступа» (IAM - Identity and Access Management). Упор – на внедрение технологии искусственного интеллекта и роботизацию.

В финансовом секторе России картина достаточно противоречивая. За 2023 год в общей сложности по всем отраслям утекла информация о 170,3 миллионов человек, что превышает значение 2022 года в 3,2 раза, писала весной 2024 года gazeta.ru со ссылкой на РБК и исследование InfoWatch. Примерно половина сливов персональных данных пришлась на банки.

Однако, в первой половине 2024 года количество утечек данных из российского финсектора сократилось на 62%. К такому выводу пришли аналитики экспертно-аналитического центра ГК InfoWatch в исследовании «Утечки конфиденциальной информации из финансовых организаций, первое полугодие 2024 г.» (https://www.infowatch.ru/analytics/analitika/utechki-konfidentsialnoy-informatsii-v-finansovoy-sfere-za-polgoda).

Объем утекших из российских финансовых организаций персональных данных тоже снизился, как и число инцидентов, однако по-прежнему остается значительным – за первые шесть месяцев

текущего года было скомпрометировано 49,5 млн записей (51,1 млн за такой же период годом ранее).

На МФО, МФК и другие кредитные небанковские организации пришлось 35,7% от всего объема утечек в российском финсекторе. Таким образом, по итогам первой половины 2024 года именно компании микрофинансового сектора можно признать наиболее уязвимыми с точки зрения информационной безопасности среди всех финансовых организаций в России, говорится в исследовании InfoWatch.

Отмеченная в текущем году тенденция не повод к успокоению. Время от времени о сливах и утечках появляются сообщения в разных источниках, чаще всего на Телеграм-канале «Утечки информации». Так, в октябре 2024 канал сообщил о появлении в открытом доступе базы под названием «ВТБ-клиенты». В нем говорится, что утечка включает 6,1 млн строк с личной информацией: фамилии и имена, номера телефонов, адреса электронной почты и даты рождения. Сам банк данное сведение опроверг: ««Появившаяся на отдельных сомнительных ресурсах очередная «база данных» не является базой данных банка ВТБ. Это скомпилированная из открытых источников и данных сторонних организаций информация от 2022 года», — заявили в финансовой организации.

В сентябре 2024 года СМИ сообщили об утечке персональных данных десятков тысяч клиентов банка «Зенит». За взломом стоит хакерская группировка DumpForums, представители которой признались, что получили доступ к базе данных сайта, принадлежащего банку «Зенит». Банк позднее сообщил о двойном списании средств клиентов из-за ошибки на стороне банка-эквайера: «Мы фиксируем обращения об ошибочном повторном списании средств не по вине банка "Зенит". Причина сложившейся ситуации – ошибка со стороны банка-эквайера (банк, через терминал которого проводилась оплата картой в торговой точке). Он ошибочно осуществил повторные списания по уже проведенным ранее операциям, и пострадали клиенты нескольких банков" (Интерфакс, 2 октября 2024).

Анализ проблемы в России и за рубежом позволяет утверждать, что в противодействии информационным утечкам решающими факторами являются инновационные технологии и подготовка персонала компаний.

Искусственный интеллект и роботизация лежат в основе современных программ: «системы управления инцидентами информационной безопасности»; «планирование мер реагирования на инциденты» **(**incident response planning); «разведка угроз» **(**threat intelligence); «управление идентификацией и контролем доступа» (Identity and Access Management) и другие инструменты.

Они помогают сокращать время, затрачиваемое как на обнаружение уязвимостей, так и на выявление инцидентов безопасности, следовательно, уменьшают совокупные потери (прямые финансовые, репутационные, страховые и прочие). «Наибольший урон несет бизнес тогда, когда утечки остаются незамеченными долгое время или по причине слишком медленного и неэффективного реагирования на них», замечает старший менеджер инженерной компании UST Боб Дьютайл.

Но и технологии не выручат в случае непреднамеренной ошибки или злоумышленной акции сотрудника организации. Поэтому не меньше внимания следует уделять работе с персоналом. Но это уже тема отдельной статьи.

Интервью

Интерпол против киберпреступников

Интервью директора Управления киберкриминала Интерпола Нила Джеттона онлайн изданию Chief Security Officer (25 октября 2024 г.).

Кибератаки осуществляются все чаще и становятся все более опасными. Как эти тенденции влияют на работу Интерпола?

Частота, интенсивность кибератак увеличиваются, и это представляет серьезную угрозу. В 2025 году урон от киберкриминала в мире превысит 10 триллионов долларов США. А к 2029 году, как ожидается, достигнет 15 триллионов. Для эффективной борьбы с этим злом нужны более совершенные технологии. Сегодня преступники по части применения инструментов на базе искусственного интеллекта имеют перед нами преимущество. А на пороге квантовые вычисления.

Здесь, в Интерполе, мы фокусируем внимание на трех направлениях противостояния транснациональному криминалу: наращиваем потенциал через различные формы тренингов, охватывающих широчайший спектр проблем и вопросов; совершенствуем сбор разведданных; развиваем сотрудничество с партнерами из частного сектора, предоставляющими ценную информацию, когда происходят крупные инциденты или когда замечают нечто интересующее нас. Они (партнеры) доносят до нас эту информацию, а мы, в свою очередь, делимся с органами правопорядка.

Вы упомянули технологии на базе ИИ. Считается, что преступники на шаг опережают нас. Как вы считаете, этот разрыв растет?

Киберкриминал ищет уязвимости, беря на вооружение инновационные технологии. Но из этого не следует считать, что ИИ – нечто плохое. У него масса позитивных приложений. Нам надо смотреть вперед и стараться опережать преступный мир, а не просто обороняться. Возвращаясь к вашему вопросу, хочу подчеркнуть, что нет хороших и плохих технологий. Важно, в чьих они руках.

Мы на пороге постквантовой эпохи. Что изменится в области кибербезопасности?

Я не специалист в этой узкой области. Но по опыту работы не понаслышке знаю, что такое квантовые вычисления. В настоящее время мы ведет тщательное изучение данной инновации, отдавая себе отчет в том, что в процессе реализации она станет для нас серьезной проблемой.

В этом контексте какое место занимает взаимодействие Интерпола с государственными и частными структурами?

Ни одно агентство, или правительство, или компания не могут в одиночку справиться с международным по характеру киберкриминалом. Для успеха требуется команда из представителей частного сектора и структур правопорядка. Не существует уникальной стратегии противодействия. Чтобы усложнить хакерам жизнь, нужны коллективные усилия, разносторонний опыт и компетенции.

Партнерство – в основе всего, что делает Интерпол. В Интерполе 196 стран-членов, каждая со своими особенностями. Поэтому мы берем за приоритет региональный подход к решению задач. В Сингапуре находится возглавляемое мной управление. Здесь я работаю. В управлении две оперативные группы. Одна ориентируется на Африку, вторая – на южную часть Тихоокеанского региона. Несколько раз в год мы предпринимаем операции, опираясь на полученные разведданные, в отношении какого-то определенного вида киберпреступности или группировки.

Успех обеспечивается хорошим взаимодействием с полицией и частными компаниями расположенных в этих районах государств. Опыт полезный. Мы хотим распространить его также на Ближний Восток, Северную Африку, возможно, другие регионы мира.

Вы сказали о формировании межнациональной команды. Но в то же время не секрет, что многие страны спонсируют и занимаются государственным киберкриминалом. Нет ли здесь противоречия?

Возможно то, что я скажу, смутит многих, но факт остается фактом: в течение всех лет существования Интерпола, в соответствии со статьей 3 Устава, мы совершенно не касаемся предметов, связанных с политикой, армией, расой или религией. Мы успешны именно благодаря тому, что действуем вне геополитических игр. Мы знаем о проблемах, упомянутых вами. Мы совсем не наивны. И когда мы сидим за столом, обсуждая свою стратегию, мы, конечно, учитываем этот момент. Способность эффективно взаимодействовать с представителями разных стран во многом обусловлена тем, что мы вне политики. Наша цель – бороться с киберкриминалом, преследовать преступников и помогать их жертвам.

Другая проблема состоит в том, что разоблаченная, обезоруженная кибергруппировка быстро меняет название и бренд

Это сложный вопрос, особенно применительно к хакерам шантажистам. Разные игроки сплачивают в группу, потом рассыпаются и быстро создают новое объединение. Есть наработанные стратегии охоты за ними. Посадить за решетку – один из самых надежных способов пресечь преступление, одновременно продолжая разрушать преступную инфраструктуру.

Киберпреступные группировки имеют в своем распоряжении настоящие таланты. Ведь многие идут на сотрудничество с преступным миром?

Дело в высоких доходах. Для нас вопрос заключается в том, как убедить таланты отказаться от сотрудничества с криминалом, обратить свои способности на пользу общества. Для этой цели у нас есть специальная программа «Intercop», заточенная под работу с молодежью. В то же время понимаем, что 99% всех преступлений совершаются ради барыша. Полностью это явление не уничтожить, но можно его ограничивать. Над этим мы и работаем.

В заключение: сможем ли мы когда-нибудь жить в «кибербезопасном» мире?

Опять же хочу повторить: фишка в том, как мы используем новые технологии, во зло или добро. Мы должны проявлять повышенную ответственность относительно существующих рисков, особенно в связи с молодежью и социальными медиа. Мы видим, как легко люди поддаются на обман и становятся жертвами преступлений. Но имею смелость утверждать, что мир, в котором живем, становится безопаснее, во многом благодаря таким организациям как Интерпол.