Охрана предприятия

№1 (94), 2025

Оглавление

Банковская безопасность

«Денежные мулы или дропы: как с ними бороться

«Денежным мулом» или дропом называют тех, кто сознательно, за процент, или непреднамеренно предоставляет услугу (банковскую карту, счет) для перечисления мошенникам украденных денежных средств.

Эксперту Марути (graph.org) известны три основных вида дропов:

Используемые «в темную». Не подозревают, что участвуют в незаконной, криминальной деятельности.

Сознательные. Обычно догадываются, что делают нечто незаконное, но соглашаются за деньги.

Соучастники. Сознательно идут на преступление, более того, участвуют в планировании и совершении преступления.

Вербовка денежного мула обычно осуществляется через социальные медиа: онлайновые биржи труда и сайты знакомств. Его/ее уговаривают открыть банковский счет или предоставить имеющийся счет, карту. Затем мошенники проводят через карту или счет украденные, отмывочные трансакции на собственные счета. Они либо инструктируют дропов, откуда, куда и когда переводить деньги, либо сами используют полученные в свое распоряжение каналы для трансфера. Как правило, денежный мул получает свою долю прибыли.

Такие способы передачи средств бывает трудно отследить, поскольку они подвергаются верификации по категории «малого риска» как принадлежащие обычным банковским клиентам.

Участие дропов в отмывании денег – не только российская особенность, это мировая проблема. В конце 2023 года Европол опубликовал пресс-релиз о завершении очередной международной операции по пресечению деятельности «денежных мулов».

Операция продолжалась 6 месяцев при участии 26 стран, а также международных банковских организаций. По ее итогам выявлено около 11 тыс. «денежных мулов» и более 470 вербовщиков, из них арестовано более тысячи человек, вовлечённых в преступную деятельность, установлены убытки от преступной деятельности в размере 100 млн евро и предотвращен вывод в нелегальный оборот денежных средств на общую сумму более 30 млн евро. Следственными органами возбуждено более 4,6 тыс. уголовных дел.

На сайте SQN Banking Systems, провайдера продуктов для финансовой сферы по обнаружению и предотвращению мошенничества, опубликован ряд рекомендаций для банков относительно методов, помогающих определить активность дропов.

Наблюдайте за отличительными характеристиками подозрительных счетов. К примеру, за появлением одновременно нескольких банковских счетов на одно лицо. Криминальные действия здесь намного превышают среднестатистические показатели. В то же время фиксируйте скорость открытия. Мошенники нередко делают это замедленными темпами по сравнению с законопослушными клиентами, которые назубок знают собственные персональные данные.

Следите за активностью использования открывшихся счетов. Нередко дропы открывают счет и оставляют его в спящем режиме продолжительное время, но через несколько месяцев начинают с бешеной активностью проводить трансакции. Другой красный флажок: появление множества депозитов с последующим выведением денег за рубеж.

Берите на вооружение поведенческую биометрию. Она оценивает уникальное поведение и подсознательные движения человека в процессе воспроизведения каких-либо действий. При этом подозрительное поведение, свидетельствующее об отклонении от нормы, может быть признано как мошенническое. Такими сигналами могут быть нерешительность, колебание, раздражительность, смущение и другие моменты, свидетельствующие об отклонении от нормального поведения.

Учите банковский персонал распознавать сигналы и признаки возможного мошенничества в ходе общения с клиентами. Многие из тех, кто становится «денежным мулом», испытывают финансовые трудности или/и страдают от неустроенности личной жизни, любят поговорить с оператором, могут поделиться личной историей, например, рассказать, зачем открывают новый счет.

Чтобы не попасть случайно в ряды дропов, эксперты советуют:

- Никогда не реагируйте на предложение быстро и легко заработать
- Всегда отказывайтесь получать или переводить деньги за других (кроме, разве что, самых близких вам людей)
- Никогда не предоставляйте карту или банковский счет для использования посторонним
- Никогда не открываете совместные счета (за исключением родственников).

Управление рисками, связанными со сторонними поставщиками, в банковском секторе

Банковский сектор по природе бизнеса предполагает множество внешних взаимосвязей, что само по себе подразумевает высокие риски. К тому же сторонние поставщики (third party vendors) представляют собой, как правило, высокотехнологические компании, предлагающие инновационные решения. Растущая зависимость от внешних партнеров и поставщиков усложняет для банков ландшафт рисков и угроз.

В феврале 2024 года Bank of America объявил об утечке клиентских персональных данных по вине третьей стороны. С почти 70 миллионами клиентов в 35 странах мира Bank of America – лакомый кусочек для преступников. Криминальная группировка LockBit, взявшая на себя ответственность за утечку, не атаковала банк напрямую, осознавая трудности преодоления мощных рубежей киберзащиты финансовой организации. Злоумышленники нашли лазейку у менее защищенного партнера банка – индийской компания Infosys, крупного поставщика программного обеспечения.

Согласно официальному заявлению американского подразделения Infosys - Infosys McCamish Systems LLC (IMS) – компания столкнулась с серьезным инцидентом, с «внешним нарушением безопасности», из-за чего на время были отключены важнейшие системы и приложения. При этом системы самого Bank of America не подвергались прямому взлому.

Данный пример не единственный. В 2017 году из Scottrade Bank утекли данные 20 000 клиентов из-за поставщика, загрузившего в сервер файл без надлежащей киберзащиты. В том же году из-за партнера были взломаны 400 000 кредитных счетов итальянской банковской группы UniCredit.

Чтобы избежать повторения печального опыта упомянутых финансовых организаций, следует прислушаться к мнению экспертов, которые советуют сформировать специальную программу работы с партнерами (Third Party Vendor Management Program). Задача ее – управление рисками сторонних поставщиков. Этим делом должен заниматься назначенный специалист с соответствующими полномочиями и функциями, а именно: изучать и на постоянной основе отслеживать потенциальные риски и угрозы, могущие проявить себя в процессе взаимодействия с разными организациями.

В рамках программы регулярно, минимум раз в год, проводить независимый аудит состояния систем кибербезопасности и партнеров.

Кроме того, желательно по договоренности с партнерами осуществлять постоянный мониторинг их финансовой устойчивости и стабильности. Это важно, чтобы быть уверенным в том, что сторонние поставщики неукоснительно выполняют требования по защите данных, и их продукты или услуги для банка не несут неоправданных рисков.

Вопрос о мониторинге и контроле должен быть заранее обсужден в ходе переговоров о сделке и прописан в контрактах и договорах.

Время от времени важно проверять, следует ли поставщик документированным требованиям кибербезопасности. Если возникают сомнения, необходимо усилить мониторинг и контроль. Такой контроль охватывает и технические аспекты. Речь о проверке и тестировании инфраструктуры информационной защиты партнера, причем очень тщательной и глубокой, «до гайки и болта».

Важно не забывать и о рисках «четвертой стороны». Партнеры и поставщики банка имеют обычно собственных поставщиков, то есть еще один, дополнительный ряд организаций, чьи слабости и уязвимости могут опосредственно угрожать безопасности финансовой организации. Здесь эксперты советуют проследить, чтобы непосредственный партнер/поставщик в свою очередь организовал у своих партнеров/поставщиков аналогичную систему мониторинга и контроля безопасности.

В США задачи минимизации рисков третьей стороны рассматриваются на уровне федеральных регуляторов. Так, летом 2023 года Управление контролера (OCC), Федеральная корпорация страхования вкладов (FDIC) и Совет управляющих Федеральной резервной системы выпустили совместное руководство, в котором излагаются фундаментальные принципы управления банками своими отношениями с третьими сторонами и связанными с ними рисками.

Руководство во главу угла ставит соображения, касающиеся контрактов, призывая банки вести четкую документацию “исполненных контрактов” наряду с "текущим перечнем всех взаимоотношений с третьими сторонами” и обеспечивать, чтобы “контракты надлежащим образом проверялись, утверждались и исполнялись” (docusign.com).

Руководство также требует от банков сосредоточиться на решении следующих задач:

Четкая инвентаризация: Создать центральное хранилище данных о взаимоотношениях со сторонними организациями, в которое можно легко обращаться в любое время, особенно во время проверок.

Анализ пробелов: Проводить анализ всех существующих договоров со сторонними организациями, чтобы определить, содержат ли они пункты и положения, как соответствующие задачам безопасности банка, так и представляющие риски.

Меры по исправлению положения: Вносить исправления в контракты в масштабе выявленных пробелов и рисков.

Периодический обзор: Периодически пересматривать контракты для выявления отклонений от стандартных условий.

Текущие контракты: Улучшить существующие процессы адаптации для снижения рисков сторонних организаций и обеспечения надлежащего рассмотрения, согласования и утверждения условий всеми заинтересованными сторонами.

Риски дипфейков для финансовых организаций

Дипфейк как «сложный метод на базе искусственного интеллекта, который использует многоуровневые алгоритмы машинного обучения для извлечения все более сложных характеристик из необработанных входных данных» (kaspersky.ru), позволяет имитировать людей, материальные объекты, местности, иные сущности максимально приближая их к реальности.

Число инцидентов безопасности с использованием технологии и методов дипфейка в финансовом секторе России возросло в 2024 году на 13 процентов. А если верить данным зарубежных СМИ, то только в Европе (без России и некоторых других стран континента) аналогичный рост составил 780 процентов (cliffordchance.com).

Исследование «Тенденции дипфейка в 2024 году», проведенное в странах Запада компанией Regula (производитель экспертных продуктов для проверки подлинности документов, денежных знаков и ценных бумаг), показало, что только половина европейских и североамериканских банков (49%) ощущают готовность эффективно противостоять данным угрозам. В сегменте финтехнических компаний таких оказалось 63 процента.

Наиболее распространенные формы дипфейка к настоящему дню: а) воспроизведение характерных черт лица реального человека; б) воспроизведение речевых характеристик.

В этой статье мы не касаемся легального использования технологии дипфейка в рекламе или видеоиграх. Сосредоточим внимание на рисках дипфейка для банков и других финансовых организаций. Это *следующие риски*:

- неспособность отличить поддельную идентичность от реальной идентичности начальника, коллеги, партнера, чреватая угрозой финансового мошенничества;

- неспособность банковского работника обнаружить дипфейк клиента или, напротив, заблуждение клиента, вошедшего в контакт с имитацией реального банка;

- компрометация систем защиты данных банка, грозящая финансовым и репутационным уроном в результате фишинговых атак на организации – клиентов банка через электронную почту, телефонную связь, веб-сайт.

Для минимизации банками рисков дипфека эксперты рекомендуют:

Сформировать и регулярно обновлять планы реагирования на инциденты безопасности, обусловленные возможными сценариями применения дипфейка.

Проследить, чтобы в этих планах, а также в политиках и инструкциях организации содержались конкретные меры и шаги по обнаружению, своевременному уведомлению и нейтрализации последствий таких инцидентов.

Предусмотреть тренинги для персонала финансовых организаций по выявлению признаков потенциальных угроз, связанных с дипфейками, с упором на верификацию аутентичности коммуникатора, трансакции, немедленное реагирование на сигнал о подозрительной активности.

Регулярно проводить аудиты и тестирование систем безопасности (как внутренние, так и партнеров, поставщиков), симуляционные игры инцидентов с дипфейками для отработки планов отражения угроз.

Обеспечить каналы обмена развединформацией между банками, регуляторами, органами правопорядка об инцидентах или угрозе таковых, равно как и обмен опытом, лучшими практиками между финансовыми организациями.

В марте 2024 года Центральный Банк России объявил об усилении борьбы с дипфейками путем обновления процедур информирования о мошеннических переводах в онлайн-сервисах для финансовых операций и обмене цифровыми финансовыми активами. С июня того же года операторы платежных систем и электронных платформ, включая банки и платежные системы, обязаны передавать данные об украденных средствах клиентов финансовому регулятору. Данные из реестра регулятора распространяются среди всех кредитных организаций через систему Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере.

В августе 2024 года Банк России выпустил рекомендации по выявлению дипфейков. Предупреждая о возросшей активности мошенников, которые начали использовать нейросети для генерации сообщений с использованием дипфейков, регулятор рекомендует проверять любые просьбы о переводе денег. Среди характерных признаков дипфейка в Банке России назвали, в частности, монотонную речь, неестественную мимику и дефекты звука.

В декабре 2024 года Сбербанк и Экспертно-криминалистический центр МВД России подписали соглашение о сотрудничестве, которое предусматривает совместную разработку высокотехнологичных решений для выявления дипфейков, совершенствование существующих решений и использование их для раскрытия преступлений (safe.cnews.ru).

Сбербанк, по словам заместителя председателя правления Станислава Кузнецова, еще два года назад запатентовал технологии по выявлению дипфейков, обеспечивающие 98% эффективности. Сбер готов делиться своими достижениями в этой сфере.

Безопасность дата-центров в банковской сфере

Центры по обработке данных (ЦОДы) как критически важный компонент современной экономики и бизнеса, переживают настоящий бум. Рост числа новых и расширение имеющихся в мире дата-центров в годовом исчислении измеряется двухзначной цифрой. Лидируют здесь Северная Америка и Азиатско-Тихоокеанский Регион (статистику см. https://www.cbre.com/insights/reports/global-data-center-trends-2024).

В России также увеличивается число крупных корпораций, арендующих или владеющих собственными дата-центрами. В их числе Яндекс, Рамблер, ММБ. В последнее время к ним присоединяются ведущие банки страны. Так, собственные дата-центры начали строить в «Сбере». Один из таких объектов возводится в особой экономической зоне (ОЭЗ) в Балаково, Саратовская область. В ВТБ пользуются услугами крупного провайдера ЦОД. В банке «Дом.РФ»применяют гибридный подход к инфраструктуре ЦОД, арендуя часть мощностей, а часть — используя собственные ресурсы. Т-Банк запустит к 2027 году два крупных дата-центра, а к 2031 году оба выйдут на полную мощность — 50 МВт каждый.

По своей структуре это сложные комплексы, включая серверы, устройства для накопления и хранения информации, сетевое оборудование, не говоря уже о системах энергопитания, климат контроля и прочем. Они различаются по размерам – от небольших комнат для нескольких серверов до крупных зданий, сопоставимых с производственными предприятиями. Некоторые ЦОД занимают территорию, равную сотням футбольным полям.

С точки зрения охраны и безопасности дата-центры подвергаются угрозам, аналогичным тем, с которыми сталкиваются другие объекты критической инфраструктуры: стихийные бедствия, вандализм, хищения, кибератаки.

Обеспечение безопасности дата-центра — это всегда большой и сложный проект. Он, как правило, включает систему контроля доступом СКУД, видеонаблюдение, охранную сигнализацию, системы противопожарной защиты и контроля безопасности жизнедеятельности.

Дата-центр, считают некоторые эксперты, это идеальный объект для иллюстрации ярусного подхода к защите. Карточный терминал + PIN-код + биометрический считыватель — надежное решение для охраны периметров. Есть некоторое условное правило: прежде чем добраться до ядра дата-центра, человек должен пройти авторизацию семь раз, читаем на сайте secfocus.ru. «Начните с карточного считывателя (или вахты с охранником) на внешнем периметре и повышайте строгость авторизации для каждого следующего уровня доступа. Используйте биометрию, считыватель карт и PIN-код для доступа к ядру дата-центра. Тщательно обсудите с вашим заказчиком разделение ЦОДа на зоны безопасности и ограничивайте права доступа пользователей только теми зонами, которыми им необходимо пользоваться». Попадать внутрь должны только авторизованные люди и проверенные объекты.

Если ЦОД — хостинговая компания, то непростая задача разделить доступ клиентов в зоне серверов. В некоторых ЦОДах используются внутренние ограждения или даже стены между оборудованием разных клиентов.

Другое важнейшее направление – обеспечение безопасности информации от случайных и преднамеренных утечек, утраты данных в результате сбоя серверов, взлома баз данных извне, шифрования вымогательскими программами.

Мэт Расмуссен, доцент Военного колледжа армии США, рекомендует ряд мер, необходимых для минимизации потенциальных угроз дата-центрам.

Постоянно анализируйте и оценивайте потенциальные риски

Эта задача охватывает:

- физические ресурсы (серверы, источники энергопитания, кабельные коммуникации);

- кибер ресурсы (софты, облачная структура, компьютерные сети);

- массивы данных (клиентская информация, персональные данные, интеллектуальная собственность).

Регулярно проводите аудит среды и физических средств защиты

Контроль параметров окружающей среды, по мнению Расмуссена, относится к числу ключевых компонентов безопасности. Он включает аудит источников бесперебойного питания, запасных генераторов, систем водоснабжения, отопления, вентиляции, охлаждения. В числе мер физической охраны эксперт выделяет такие жесткие требования как биометрическая идентификация, пропуска с технологией радиочастотной идентификации, мощное видеонаблюдение.

Разработайте и неукоснительно следуйте инструкциям по защите данных и кибербезопасности

Противодействие киберугрозам требует многоуровнего подхода. Последний реализуется через сегментацию баз данных, постоянный мониторинг системы обнаружения и предотвращения несанкционированных вторжений, регулярное обновление программного обеспечения, неослабное изучение потенциальных брешей и уязвимостей систем физической охраны и кибербезопасности, серьезное и систематическое обучение персонала.

Шесть основных направлений информационной безопасности в финансовой отрасли

Ландшафт рисков и угроз для финансовых организаций динамично меняется. Кибератаки, в первую очередь, вымогательские и фишинговые схемы, становятся все более настойчивыми, сложными и изощренными. Уже ощутимое наступление эпохи квантовых вычислений ставит под вопрос надежность традиционных методов шифрования. Инсайдерские угрозы, уязвимости сторонних поставщиков по-прежнему остаются громадным вызовом для банков, всех финансовых институтов.

Эксперты выделяют следующие главные направления кибербезопасности в финансовом секторе, которыми характеризуется наступивший 2025 год:

Искусственный интеллект и машинное обучение

Эти технологии - на переднем фронте информационной защиты. Именно они способны в режиме реального времени обеспечивать своевременное обнаружение киберугроз, обрабатывая и анализируя огромные массивы данных, находя аномалии и иные предпосылки потенциальных вторжений. Финансовым организациям важно обновлять арсенал инструментов инновационными решениями на базе ИИ, которые автоматизируют процессы и радикально сокращают время, необходимое для предотвращения или минимизации киберугроз.

Архитектура нулевого доверия

Принцип нулевого доверия стал уже краеугольным камнем стратегии кибербезопасности. При надлежащем осуществлении он гарантирует, что любой пользователь, любой гаджет по умолчанию будет всегда подвергаться жесткой проверке и контролю. Постоянно действующая система верификации поможет снижению рисков.

Устойчивая в отношении квантовых вычислений криптография

Квантовые компьютеры уже не фантастика и не мечты. Квантовый вычислитель в 75 кубитов планируется создать в России в 2025 году, сообщил в интервью прессе советник гендиректора госкорпорации "Росатом", сооснователь Российского квантового центра Руслан Юнусов.

Недавно Google представил квантовый компьютер Willow. Правда, взламывать криптографию он еще не умеет. Предположительно такой прорыв произойдёт через несколько лет. Аналитики компании Gartner считают, что в 2029 году любая защита информации перестанет быть абсолютно безопасной перед квантовыми вычислениями. Но уже сегодня организации, в первую очередь, банки, должны задуматься о разработке и постепенном внедрении стратегии постквантовой криптографии, то есть алгоритмов, которые защищают от атак с квантовыми вычислениями.

Усиленное внимание к обучению и тренингам персонала

Статистика доказывает, что по-прежнему самым слабым звеном в системе кибербезопасности остается человек. Исследование инцидентов ИБ, с которыми столкнулись российские компании за первое полугодие 2024 года, показало, что в 80% случаев главной причиной проблем был человеческий фактор. Учебный фокус в финансовой сфере заточен на способы обнаружения дипфейков и фишинга, на выполнение требований регуляторов, на использование лучших практик защиты информации.

Работа с банковскими клиентами

Клиенты – составная часть экосистемы кибербезопасности. В 2025 году ожидается рост расходов финансовых организаций на разъяснительную работу среди населения относительно защиты от мошенников. В сочетании с превращением мультифакторной аутентификации и биометрической верификации в стандарт, в норму дня, такая работа должна уже в 2025 году начать приносить свои плоды.

Комплаенс программы и кооперация

Один из трендов 2025 года – ужесточение требований регуляторов к защите информации на международном и национальном уровнях. Другой тренд – коллаборация, в частности, высокий спрос на совместимость решений. Но кооперация нужна не только в области технологий. В России Центральный банк совместно с Росфинмониторингом, банками и экспертами разрабатывает платформу, которая позволит централизованно передавать в кредитные организации информацию о подозрительных операциях физических лиц для блокировки активности таких клиентов.

Итак, на фоне динамического развития киберугроз финансовая индустрия должна проявлять гибкость, маневренность, изобретательность и проактивность в своих усилиях по их обнаружению и предупреждению. Стремлением на шаг опережать киберкриминал финансовые организации смогут обезопасить свой бизнес, защитить клиентов, укрепить репутацию в современном цифровом мире.

Риски и угрозы безопасности бизнеса

Системы идентификации, аутентификации и авторизации машин – новая большая цель для киберкриминала

Компания Venafi, разработчик и поставщик услуг по управлению идентификацией компьютерной техники, провела опрос 800 специалистов по кибербезопасности в США и Европе относительно влияния Machine Identities (цифровые системы для идентификации, аутентификации и авторизации машин, устройств и IT-инфраструктуры, не связанные с человеком) на комплексную безопасность облачных данных, приложений и инфраструктуры.

« Спящий дракон просыпается» - так охарактеризовал участившиеся атаки на облачную архитектуру (cloud native infrastructure) Кевин Бочек, директор по инновациям Venafi. Массивные волны кибератак накрывают самые продвинутые сферы облачных приложений. Что хуже всего, киберпреступники все активнее применяют технологии искусственного интеллекта для получения несанкционированного доступа и злонамеренного использования систем идентификации, аутентификации и авторизации машин. 77% опрошенных выражают тревогу попытками хакеров манипулировать системами ввода-вывода данных на основе ИИ. 73% обеспокоены применением ИИ в социальной инженерии.

Главный вывод: 86% опрошенных заявили, что испытали в 2024 году как минимум один инцидент безопасности, связанный с облачными хранилищами данных. В результате 53% пострадавших организаций были вынуждены отложить запуск приложений или снизить темпы проводимых операций. 45% прерывали работу с приложениями. 30% допустили возможность несанкционированного доступа хакеров к корпоративным данным, сетям и системам.

Другие результаты исследования:

Сервисные аккаунты, предназначенные для представления не являющегося человеком пользователя, которому необходимо пройти аутентификацию и получить разрешение на доступ к данным, рискуют превратиться в новый фронт киберугроз. Так считают 88% респондентов.

Для атак на цепочки поставок будут использоваться преимущественно технологии искусственного интеллекта (77%).

Разногласия между специалистами по безопасности, с одной стороны, разработчиками и поставщиками технологических машин, систем и устройств, - с другой, никуда не исчезнут (68%). Более половины респондентов считают проигранной ими битву за то, чтобы производители думали в первую очередь о безопасности выпускаемой продукции, а не только о барышах.

Опрос помог определить зоны облачной архитектуры, подвергаемые наиболее интенсивным атакам. Список здесь возглавляют токены доступа (последовательность символов, используемая для идентификации устройства в рамках системы, средство аутентификации и авторизации, часто применяемое в веб-приложениях и API для управления доступом к защищённым ресурсам). Связанные с ними инциденты кибербезопасности отметили 56% респондентов. 53% обозначили

другие цифровые сущности, как, например, сертификаты доступа - цифровые удостоверения, подтверждающие, что соединение между сайтом и устройством пользователя защищено, а информация передается в зашифрованном виде.

Рост инцидентов отчасти связан с тем, что облачная среда с каждым днем усложняется, генерируя для специалистов кибербезопасности все новые вызовы и головоломки.

69% считают «кошмаром» управление доступом между облачной инфраструктурой и дата-центрами.

74% начальников по кибербезопасности уверены, что человеческий фактор по-прежнему остается наиболее уязвимым звеном.

83% опрошенных рассматривают как растущую проблему множественность приложений. При этом подавляющее большинство признают, что сервисные аккаунты облегчают работу в облаках.

Основной вывод опроса, сформулированный Бочеком: «Службы корпоративной безопасности должны усилить внимание к защите систем идентификации, аутентификации и авторизации машин, уравняв ее в правах с безопасностью систем идентификации, аутентификации и авторизации человека».

Атаки инсайдеров: тенденции и меры противодействия

Сегодня, когда бизнес охотно примеряет на себя гибридные облачные модели, головная боль у специалистов по кибербезопасности только усиливается. Cybersecurity Insiders - онлайн сообщество (новый вид деятельности, в том числе и бизнеса) – опросило более 400 айтишников и специалистов по кибербезопасности относительно воздействия инсайдерских угроз на их организации.

Авторы опроса немало удивились, обнаружив существенную эскалацию таких угроз за последние годы. Анализируя причины опасного тренда, они выделили основные факторы:

Усложняющаяся IT среда. Распространение удаленных и гибридных моделей работы, массовое вторжение бизнеса в облачные вычисления поспособствовали формированию громоздкой операционной структуры, которой все труднее управлять и контролировать.

Неадекватные угрозам меры безопасности. Многие компании пользуются устаревшими протоколами защиты цифровых ресурсов.

Недостаточное либо отсутствующее обучение персонала. Далеко не все инсайдерские угрозы носят преднамеренный характер. Во многих случаях они возникают из-за того, что сотрудники компании не имеют ни знаний, ни навыков распознавать и предотвращать такие угрозы.

Слабая технологическая оснащенность. Только каждая третья компания имеет в своем распоряжение эффективные инструменты борьбы с инсайдерскими угрозами.

Имея ввиду немалые финансовые и репутационные потери, которые несет бизнес в результате инсайдерской активности, эксперты призывают организации к их минимизации с помощью лучших практик. К ним, в частности, относятся:

Продвинутые мониторинговые решения

Инсайдерские угрозы намного сложнее выявлять, чем внешние. Рынок сегодня предлагает ассортимент решений UEBA (User and Entity Behavior Analytics) на основе поведенческой аналитики, алгоритмов машинного обучения, помогающих идентифицировать аномальные, потенциально опасные отклонения в поведении людей и дивайсов. Это своего рода система раннего предупреждения об угрозах.

Нецифровые источники данных

Речь идет о расширении спектра разведки рисков и угроз за счет таких данных как юридическая информация, кадровая документация, результаты мониторинга социальных сетей. Разнообразные источники информации в совокупности способствуют раннему обнаружению инсайдерской угрозы, значимо снижают риски.

Автоматизированные системы обнаружения и реагирования

Необходимы для кардинального (по сравнению с ручными способами) сокращения времени на анализ, выявление и реагирование на угрозы.

Принцип нулевого доверия

Наиболее надежный способ лишить злоумышленника возможности неавторизованного доступа к сетям и базам данных.

Программы ознакомления и тренинги

Практически все исследования по проблеме инсайдеров указывают на критическую необходимость регулярных занятий с персоналом, где работников обучают своевременно распознавать и сообщать о подозрительном поведении или иных тревожных сигналах как признаков потенциальных угроз. В конечном счете, речь идет о формировании в коллективе культуры высокой бдительности.

Регулярные аудиты, проверки и тестирование систем безопасности

Должны охватывать не только средства физической и кибербезопасности, но также и корпоративные политики, инструкции, планы.

Заблаговременное планирование мер реагирования

Компании должны быть готовы к самым худшим сценариям инсайдерской активности. Между тем, упомянутый выше опрос демонстрирует обескураживающую неподготовленность многих компаний к сюрпризам, которые им могут преподнести инсайдеры.

Почему компании «зевают» утечки информации

Согласно последнему исследованию IBM «Cost of a Data Breach Report 2024» (IBM.com), организациям в среднем требуется 207 дней, чтобы обнаружить утечку данных и еще 70 дней на то, чтобы залатать дыру. Треть компаний не понимают причин инцидента безопасности, а три четверти заявляют, что им с каждым годом все труднее контролировать насыщаемую сложными технологиями систему информационной защиты.

По данным другого исследования – «Security Priorities Study 2024» (foundryco.com/research/security-priorities), только 67% руководителей служб кибербезопасности доискиваются до причин утечек.

Джон Лейден, автор ряда публикаций в онлайн издании Chief Security Officer, разбирался в этой проблеме с помощью практиков кибербезопасности и сформулировал 7 основных причин слабой работы по предотвращению информационных утечек.

Отсутствие надежной системы мониторинга информационных рисков и угроз

Автор ссылается на замечание Брайана Джека из компании KnowBe4, специализирующейся на проведении тренингов по кибербезопасности: «Я не раз наблюдал запоздалое обнаружение и реагирование на утечку по причине передачи функции отслеживания на аутсорсинг компании, которая явно не справлялась с задачей».

Неудовлетворительное планирование мер по реагированию на инциденты безопасности

Неэффективный план, плохо проработанные действия и меры, слабый анализ произошедшего инцидента – все это ведет к провалам. Нередко организации, торопясь возобновить нормальные операции, не додумывают до конца причины утечки, лишая себя возможности избавиться от уязвимостей.

Бюджетные ограничения

Оборачиваются дефицитом специалистов высокой квалификации и адекватных систем кибербезопасности, процедурными изъянами. Испытывая нехватку необходимых ресурсов, организации, обнаружив утечку, спешно гасят огонь, ликвидируют последствия, и только потом, слишком поздно, пытаются разобраться, что, как и почему произошло. Такой подход характерен для компаний малого и среднего бизнеса.

Растущие изощренность и скрытность атак

Хакеры удивительно изобретательны, ухитряются находить все новые возможности и способы взламывать корпоративные сети, в то время как обновление и модернизация противостоящих им систем защиты постоянно запаздывает.

Непомерно громоздкие и часто разъединенные между собой системы безопасности

Многие компании пользуются разнофункциональными системами, приложениями, инструментами, которые либо слабо, либо вовсе не интегрированы в единый механизм. Утечки остаются незамеченными долгие месяцы по одной лишь причине, что система мониторинга практически отделена от остальной инфраструктуры безопасности. Но даже наличие интегрированной платформы не решает проблему, если она плохо настроена, регулярно не обновляется, не обслуживается классными специалистами.

Профессиональная усталость

Современная мониторинговая система ежедневно выдает миллионы разных данных, перегружая операторов и аналитиков, затрудняя фильтрацию информационного шума, избавление от ложных сигналов угроз.

Корпоративная культура, где кибербезопасность не в приоритете

Признавая на словах важное значение кибербезопасности, на деле многие организации вкладывают в нее недостаточно средств, ограничиваясь минимумом требований регулятора, не заглядывая вперед на перспективу. Здесь определенную ответственность несут начальники служб IT и корпоративной безопасности, которые не достаточно убедительно разъясняют лицам, принимающим стратегические решения, серьезные потенциальные последствия недооценки этого направления для бизнеса.

Эксперты призывают фокусировать больше внимания на предотвращении информационных утечек, используя такие инструменты как сканеры уязвимостей, системы тестирования, способные вовремя обнаружить бреши и слабости, а, следовательно, предупредить возможные взломы.

Опасные нарушения правил экстренной эвакуации и как их предотвратить

Старший научный работник бизнес-школы при университете в британском городе Лидс Натали ван дер Вал провела исследование поведения людей во время внезапной эвакуации из здания/помещения в форс-мажорной ситуации. Она опросила десяток специалистов по безопасности массовых скоплений людей, чтобы ответить на два главных вопроса:

- Какие наиболее характерные нарушения допускают люди во время экстренной эвакуации?
- Какие решения позволяют их предотвратить?

Вал обнаружила, что чаще всего люди совершают следующие 5 ошибок:

1. *Замедленное реагирование на оповещение об эвакуации*

Множество причин объясняют такое поведение. Главная – недооценка опасности ситуации, особенно когда люди не видят, физически не ощущают опасность. Некоторые спешат завершить работу. Другие просто не знают, что делать, куда идти. Кто-то названивает в службы экстренной помощи, теряя драгоценные минуты. Часто оповещение воспринимается как очередная тренировка, тем более, если голос звучит слишком спокойно и даже дружественно.

Возможные решения:

- Исключить ложные сигналы тревоги, к которым привыкают и не воспринимают адекватно.
- Оповещать спокойно, но настоятельно, упирая на крайнюю срочность.
- Особое внимание – посетителям, которые нуждаются в подсказке относительно маршрута эвакуации
- Главное – настойчиво повторять, повторять, и еще раз повторять оповещение во всех его формах.

2. *Выбор не ближайшего выхода, а привычного маршрута*

Большинство в экстремальной ситуации стремятся покинуть здание, помещение тем же маршрутом, каким пришли, несмотря даже на известные им более близкие и короткие пути эвакуации. Кроме того, действует правило толпы: куда кинутся первые, туда же вслед и остальные. Спеша, многие просто не замечают (да и не ищут) указатели эвакуации, тем более, если они неверно размещены и малозаметны.

Возможные решения:

- Размещение знаков должно быть осуществлено таким образом, чтобы маршрут эвакуации был непрерывным.
- При возможности использовать напольное проецирование знаков эвакуации, которые можно менять, регулировать во время форс-мажора, указывая на ближайший выход.
- Заранее, в процессе подготовки плана эвакуации, назначать ответственных за определенные участки, на которых возлагается руководство эвакуацией.
- Развешиваемые на стене планы эвакуации обычно никто не читает и не изучает. Поэтому так важно привлечь внимание людей звуковым, речевым, визуальным, иными видам оповещения, включая непосредственное управление процессом на местах.

3. *Паническое бегство*

Оно происходит, когда люди сами видят (или слышат) опасность. Бегство – проявление паники. Реальную опасность представляет переход в режим, при котором человек частично или полностью утрачивает самоконтроль. Именно в таком состоянии люди получают физические травмы.

Возможные решения:

Конкретная ситуация определяет, что лучше в данной ситуации – стоять, идти или бежать. Последнее допустимо и даже необходимо при условии непосредственной угрозы, опасности. Поэтому эксперты советуют принимать решение по реальному раскладу, побуждая людей бежать, или, напротив, их сдерживать. Главный мотив – сохранение жизни людей.

4. *Съемка/фотографирование инцидента вместо эвакуации*

Такое происходит сегодня везде и всегда во время инцидента безопасности. Если люди видят угрозу, но не ощущают ее непосредственно для себя, они начинают заниматься фото и видео съемкой вместо того, чтобы попытаться спастись, при этом нередко мешая другим эвакуироваться. Катастрофы, несчастные случаи со смертельным исходом, к сожалению, не являются чем-то новым. Новое в том, что люди достают свои смартфоны, чтобы сфотографировать тела мертвых. (Доктор Ласана Харрис, доцент кафедры экспериментальной психологии в Университетском колледже Лондона, исследует поведение людей в чрезвычайных ситуациях и говорит: «Мы живем в культуре, где фотография трагедий на телефонах стала нормативным поведением. Люди автоматически вынимают свои телефоны для сцен «хорошо, плохо или безразлично»).

Эффективные решения здесь не просматриваются. Запреты не помогают. Воздействовать может только личное вмешательство человека, ответственного за эвакуацию.

Сбор вещей, замедляющий эвакуацию

Многие, получив оповещение, лихорадочно начинают собирать свои вещи. У одних это занимает минуту, у других – больше времени. Случается, даже возвращаются, чтобы захватить забытые ключи от дома или важные документы.

Возможные решения:

В зависимости от конкретной обстановки в тексте оповещения указывать, сколько времени (минут) отводится на сбор личных и служебных вещей. В отдельных критических ситуациях настоятельно рекомендуется все бросить (кроме верхней одежды в зимнее время) и покинуть помещение, здание.

Понятно, что как бы серьезно ни были продуманы инструкции и памятки, в реальной ситуации приходится импровизировать и менять решения на ходу.

Борьба с преступлениями среди персонала

«Стукачество» как часть британской корпоративной культуры

В Великобритании доносительство в качестве инструмента борьбы с инсайдерами регулируется Управлением по финансовому поведению (FCA) и Управлением пруденциального регулирования (PRA) Банка Англии. На этот счет в Руководстве FCA имеется даже специальный раздел, который предписывает более 50 000 финансовым организациям страны:

- Иметь в своей структуре топ-менеджера, отвечающего за функционирование института доносительства. Он/она может входить в правление директоров, принимать участие в выработке стратегических решений.

- Иметь в наличии прописанные в инструкции процедуры.

- Владеть методологией конфиденциального и анонимного разоблачения нарушителей корпоративных правил.

- Использовать надлежащие коммуникации (телефон, имейл, «горячая линия).

- Обеспечивать обратную связь, когда это возможно и целесообразно.

- Принимать разумные меры по недопущению актов мести в отношении информаторов.

- Проводить с персоналом занятия по ознакомлению с задачами, правилами и процессами системы внутреннего информирования. На тренингах разъяснять, что если работник организации заметил или заподозрил нечто неладное, то он обязать об этом доложить своему прямому начальнику или менеджеру, который курирует систему доносительства.

Отсутствие такой системы – повод для разбирательства Управлением по финансовому поведению.

Компания может заключать соглашение с информатором, в котором предусмотрены взаимные обязательства. К примеру, неразглашение информатором данных о своей активности даже после своего увольнения.

Руководство также рассматривает любую попытку воспрепятствовать прохождению информации как незаконную, нарушающую внутренние правила.

Всякий раз, когда речь идет о внутрикорпоративном доносительстве, неизбежно возникает вопрос об этической стороне данного способа борьбы с мошенничеством и прочими преступлениями. Для информатора это не праздный вопрос. Он нередко оказывается в ситуации, когда, совершая полезное со всех точек зрения дело, сообщая о неправильном, подозрительном поведении коллеги, понимает, что ставит под удар собственное реноме в коллективе. Надо иметь мужество, считает эксперт Ри Халлада, чтобы совершить шаг с риском для репутации, для перспективы дальнейшей работы в компании.

Разоблачение неправомерных действий в организации через доносительство рассматривается специалистами как «жизненно необходимый механизм, позволяющий вскрывать множество проблем – от рабочих несостыковок до хищений и коррупции - когда другие способы бессильны» (faceup.com/en/blog/dilemma-and-issues-of-whistleblowing).

В то же время многие затрудняются говорить о моральной, этической стороне доносительства. Фактически система человеческих ценностей, в центре которой – честность, справедливость, принципиальность - приходит в противоречие с потенциальными последствиями, среди которых: месть коллег, враждебность начальника, вынужденное увольнение.

Это настоящая дилемма, однако не неразрешимая. Эксперты рекомендуют:

Главное – обеспечение полной конфиденциальности благодаря заранее определенным каналам информирования, не исключая и возможность шифрования сообщений. Информатор должен быть уверенным, что его/ее репутация не пострадает.

Важно определиться о способе коммуникации: внутри организации, например, через кадровиков или юристов, или вне компании, обращаясь к регуляторам и другим надзирающим органам. В первом варианте проблему можно разрешить быстро, предупредив ее разрастание, безболезненно для информатора и компании в целом. Второй вариант больше подходит для тяжких преступлений.

Нельзя пренебрегать и мотивацией в виде бонусов. Надо, чтобы «стучать» было выгодно. В принципе доносительство, несмотря на негативную (особенно для русского человека) коннотацию этого слова, действительно представляет часть корпоративной культуры.

Книжное обозрение

Corporate Security Management: Challenges, Risks, and Strategies
by Marko Cabric

Книга представляет собой практические советы, как эффективно обеспечивать защиту бизнес процессов, материальной и виртуальной (цифровой) собственности компаний и их персонала.

Автор увязывает воедино собственно бизнес и его безопасность, показывая, как эти два нередко конфликтующие между собой направления деятельности компании можно и нужно трансформировать в плодотворное сотрудничество. Именно в гармоничном сочетании приоритетов бизнеса, стратегии безопасности и лучших практик удается найти единственно точный и правильный ответ на вопросы «Кто, Что, Где, Почему, Когда и Как» относительно корпоративной безопасности.

Автор анализирует проблемы на примерах охранных предприятий и корпоративных служб безопасности, действующих в разных отраслях бизнеса и экономики. Он знакомит читателей с ключевыми компетенциями корпоративной безопасности и объясняет их адаптацию под профильные задачи, функции и компетенции организации в целом.

В книге рассказывается, как следует идентифицировать, понимать, оценивать, анализировать риски, с которыми сталкиваются компании, выстраивать эффективную стратегию их предупреждения и минимизации. Детально характеризуется систематический подход к проверке, анализу, планированию, измерению и администрированию охранной функции.

Монография доходчиво и убедительно освещает и анализирует:

- Часто не совпадающие задачи и приоритеты службы безопасности, с одной стороны, и остальных подразделений, с другой, относительно управления рисками, аутсорсинга и других вопросов, требующих кооперации и партнерства.
- Способы культивирования и поддержки в компании высокой культуры безопасности.
- Компетенции, необходимые для начальника охраны (службы безопасности).
- Трудности работы охранной службы в коммерческой среде и способы их преодоления.
- Множество подходов и требований к охране и безопасности в различных отраслях экономики и бизнеса.

Книга содержит терминологический словарь, практические примеры и упражнения, дискуссионные вопросы.