Антон Замараев (ОТП Банк): Участие ИБ начинается задолго до реализации идеи

Антон Замараев, начальник Управления информационной безопасности ОТП Банка, рассказал «Б.О» о том, что причиной наиболее часто случающихся ИБ-инцидентов продолжает оставаться человеческий фактор

Текст
ВАДИМ ФЕРЕНЕЦ,
ОБОЗРЕВАТЕЛЬ **«Б.О»**

— Антон, что представляет собой команда кибербезопасности ОТП Банка? Какая задача стоит перед ней?

— В банке функционирует Управление ИБ, в которое входят несколько ключевых подразделений. Во-первых, Центр развития процессов кибербезопасности — набор отделов и команд, которые обеспечивают основные процессы информационной безопасности: управление доступом, рисками, защиту данных и контроль соответствия внутренним и регуляторным требованиям. Во-вторых, подразделение технической и инфраструктурной защиты, где коллеги внедряют и развивают средства защиты информации, криптографические сервисы, обеспечивают безопасность периметра и внутренней сети банка. Отдельной командой выступает SOC, ведущий непрерывный мониторинг угроз и реагирующий на внешние и внутренние инциденты безопасности. Силами команды AppSec мы в полной мере участвуем в процессах разработки и внедрения информационных систем, предоставляя экспертизу безопасности на всех этапах жизненного цикла систем, от проектирования требований до вывода системы из эксплуатации, делая акцент на необходимость снижения метрики time to market, автоматизацию инструментария ИБ и предоставление его как набора селф-сервисов для команд. В завершение отмечу Центр безопасности банковских операций, подразделение транзакционного антифрода, призванное защищать клиентов банка и их транзакции от осуществления несанкционированных операций.

Выделить какую-то одну ключевую задачу в области кибербезопасности невозможно, ведь речь идет о комплексе взаимосвязанных процессов. Если бы мы фокусировались только на определенных областях безопасности, то другие оставались бы «западающими» и неразвитыми, были бы местом приложения наиболее вероятных векторов угроз.

Вообще, взаимная интеграция процессов не только кибербезопасности, а безопасности в целом — наш «конек» и всегда потенциал для получения синергетического эффекта. К примеру, антифрод интегрирован в общую систему кибербезопасности и тесно работает с подразделением SOC. В случае если мы регистрируем попытки несанкционированного использования мобильного приложения, автоматизированные действия и манипуляцию параметрами в авторизованной зоне, SOC посредством подразделения антифрода оперативно блокируют клиентский аккаунт. Бывает, что клиент теряет средства в результате успешной атаки с использованием социальной инженерии, тогда подключается подразделение банковской безопасности, помогающее минимизировать последствия возможного мошенничества и в том числе вернуть клиентские средства.

— Какие топ-3 киберугрозы можно выделить?

— Наиболее серьезной угрозой остается человеческий фактор. По статистике, значительная доля нарушений ИБ связана не с намеренными, а с ошибочными действиями сотрудников. Человек по-прежнему остается наиболее уязвимым звеном в системе защиты. Рядовые специалисты могут допускать ошибки, приводящие к рискам компрометации данных, возникновения технологических недостатков внутри инфраструктуры.

Вторая тенденция касается быстрого развития продуктов и технологий. Современные организации, особенно банки и IT-компании, ведут жесткую конкуренцию между собой, стремясь оперативно внедрять инновационные решения и новые функциональные возможности. Агрессивный темп интеграции нововведений, поддерживаемый методологией Agile, создает риски возникновения технических проблем и уязвимостей в ПО.

Третий важный тренд, который нельзя игнорировать подразделению ИБ, — это активное внедрение искусственного интеллекта (ИИ). Сегодня практически каждая крупная организация стремится воспользоваться возможностями ИИ, зачастую недооценивая потенциальные угрозы, возникающие вместе с этими технологиями. Недостаточная продуманность подходов, отсутствие необходимых механизмов контроля и проверки безопасности используемых моделей могут создать серьезные проблемы.

Фото: ОТП Банк

Таким образом, главными ИБ-вызовами остаются управление человеческим фактором, обеспечение качества разработки новых решений и грамотное применение возможностей ИИ.

— Какую долю в первом тренде занимают злонамеренные действия инсайдеров?

— Какие-то целенаправленные нарушения со стороны сотрудников — редкое явление, потому что люди уже хорошо понимают специфику работы подразделения ИБ и знают о работе систем мониторинга, в том числе посредством наших дайджестов и сарафанного радио. Более 90% всех инцидентов связаны именно с ошибками сотрудников, которые без злого умысла, например, делают попытку переслать себе на домашнюю почту файл с информацией для внутреннего пользования, просто чтобы поработать над ним на выходных.

Среди оставшихся 10% потенциальных внутренних злоумышленнников экспертно я бы отнес долю более чем 80% «в пользу» сотрудников массовых функций, где есть потенциал и мотив, связанные со злоупотреблением служебными полномочиями. Эти риски должны митигироваться путем максимальной автоматизации рутинных операций и проектирования контролируемых операционных процессов внутри информационных систем.

Так или иначе, программа повышения осведомленности (Awareness) остается наиболее эффективной мерой для снижения количества внутренних нарушений.

— При работе с IT-разработчиками есть ли место концепции Security by design?

— Наш путь к созданию продуктов с учетом этого подхода начался благодаря инициативе команды безопасности. Вообще, мы убеждены, что внедряемые средства защиты, какими бы хорошими они ни были (а их нужно еще правильно настроить), не закрывают и 30% угроз финтех-организации. Можно сколько угодно защищать периметр, внедрять современные межсетевые экраны и WAF, но пропустить проблему ПО, возникшую в результате внутренней разработки. Поэтому с целью избежать разночтений в требованиях и архитектуре, несогласованности при выпуске очередного инкремента в продуктив был внедрен процесс безопасной разработки ПО (SDLC)

Наши участие и роль начинаются задолго до реализации идеи. Уже на стадии Discovery, когда появляется новая концепция, мы активно включаемся в обсуждение, совместно с IT и бизнесом формулируем требования к продукту, определяя необходимые и компенсирующие меры защиты.

Через команду AppSec ежемесячно проходит несколько тысяч задач в таск-трекере. Чтобы не стать бутылочным горлышком в процессе и не замедлить выпуск новых функций, мы сосредоточились на автоматизации проверок безопасности. Например, инструменты автоматического анализа кода в пайплайнах позволяют разработчикам самостоятельно выявлять уязвимости и исправлять их без привлечения ресурсов службы ИБ. Это помогает сократить time to market, трудозатраты команды и направить их на дальнейшее совершенствование процессов автоматизации.

— С какими вызовами вам предстоит встретиться в ближайшем будущем?

— И технологии, и банковские продукты развиваются очень быстро. Где-то драйвером изменений являются продуктовые команды, как в случае с AI и OpenAPI. Где-то технологии заставляют двигаться быстрее и переосмысливать подход к обеспечению безопасности, как в случае с постквантовой криптографией. Где-то регуляторы меняют платежный ландшафт, внедряя цифровой рубль. Мы же движемся по всем этим направлениям, стараясь выдерживать здоровый баланс между бизнесом и безопасностью. Б.О