«УСТОЯТЬ ПРИ ВЫСОКОМ УРОВНЕ КИБЕРАТАК В ОДИНОЧКУ ДОРОГО, А ИНОГДА НЕВОЗМОЖНО»

В СЛОЖИВШЕЙСЯ ГЕОПОЛИТИЧЕСКОЙ СИТУАЦИИ РОССИЙСКИЕ ГОСОРГАНИЗАЦИИ И БИЗНЕС ПРОДОЛЖАЮТ ПОДВЕРГАТЬСЯ МАССИРОВАННЫМ КИБЕРАТАКАМ, ЧТО ЗАСТАВЛЯЕТ IT-КОМПАНИИ МАКСИМАЛЬНО БЫСТРО ИСКАТЬ И ВНЕДРЯТЬ ЭФФЕКТИВНЫЕ РЕШЕНИЯ ДЛЯ ОТРАЖЕНИЯ ТАКИХ УГРОЗ. КОРРЕСПОНДЕНТ GUIDE ПОГОВОРИЛ С ЗАМГЕНДИРЕКТОРА — ТЕХНИЧЕСКИМ ДИРЕКТОРОМ КОМПАНИИ «ГАЗИНФОРМСЕРВИС» НИКОЛАЕМ НАШИВОЧНИКОВЫМ О ТРЕНДАХ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (ИБ) В 2024 ГОДУ, СТРАТЕГИЯХ И СПОСОБАХ ЗАЩИТЫ ИНФРАСТРУКТУРЫ КЛИЕНТОВ, АУТСОРСИНГЕ И МОДЕЛЯХ ВЗАИМОДЕЙСТВИЯ ЗАКАЗЧИКОВ И ИСПОЛНИТЕЛЕЙ В ИБ. ВЛАДИМИР КОЛОДЧУК



«ГАЗИНФОРМСЕРВИС»

GUIDE: Какие тенденции сейчас актуальны в сфере информационной безопасности? С какими проблемами сталкивается отрасль?

НИКОЛАЙ НАШИВОЧНИКОВ: Чем сильнее цифровизация и автоматизация проникают во все сферы жизни, тем больше становится угроз информационной безопасности для государства и бизнеса. В процессе поиска универсальных решений директора по информационной безопасности (CISO) пересматривают привычные, а иногда и устаревшие стратегии, выбирая новые концепции. Появляется множество новых угроз, нарушающих устойчивость функционирования цифровых экосистем. Россия — один из лидеров среди стран мира по уровню проникновения IT-технологий во все сферы жизни общества. И любой современный бизнес в нашей стране сегодня является по-своему полнофункциональной цифровой экосистемой. Но за плюсы иногда приходится платить. С 2022 года поднялась волна кибератак на государственные организации, частные компании, но и простые люди тоже от этого страдают.

G: Могли бы привести примеры?

Н. Н.: В новостях часто передают громкие истории о кибератаках на компании. Возьмем, например, СДЭК — это гигантский игрок, который недавно из-за атаки на цифровую платформу потерял примерно 1 млрд рублей за пять дней. Или была хакерская атака на сеть магазинов «Верный»: сопоставимые потери в денежном эквиваленте. А ведь это только два резонансных случая за май — июнь 2024 года.

Согласно отчету Аналитического центра кибербезопасности «Газинформсервиса», в 2022–2023 годах в России массово происходили утечки данных и основные удары злоумышленников за это время приходились на сферы доставки, ритейла и финансов. Жизненный цикл атаки содержит этап разведки, подготовки — именно на этом этапе происходят утечки, а потом злоумышленник проникает в цифровую экосистему и закрепляется. В мае и июне вторжения произошли после утечек, то есть исполнители вначале собрали информацию, проникли в инфраструктуру, закрепились, создали для себя внутри цифровой платформы все необходимые опорные точки — и атаковали… А в 2024-м мы увидим еще больше финансовых потерь и отказов систем. Потому что сейчас хакеры перешли от утечек к закреплению и будут все чаще наносить удары по бизнесу.

G: Как бизнесу защитить себя от киберугроз? Какие стратегии выбирают CISO?

Н. Н.: Традиционный путь защиты известен всем директорам ИБ, и практика показала, что при больших бюджетах держать оборону можно очень долго даже крупному бизнесу с распределенной по всей России инфраструктурой. Конечно, приходится строже контролировать сотрудников, инвестировать в обучение и внедрять новые решения, но есть еще одна проблема, о которой все знают. Бюджеты на ИБ сокращаются — это факт. Да и как им не сокращаться, когда многим компаниям в короткие сроки приходится перестраивать IT-инфраструктуру на новые решения, в том числе под давлением вопросов технологического суверенитета? Еще один вызов — развитие цифровых экосистем. Вместе с ним растет уровень внедрения технологий, меняющих архитектуру и принципы, на которых строится информационная безопасность, меняются правила организации рынка труда и нарастает дефицит кадров в сфере информационной безопасности,— это тоже признанный факт.

Есть санкции и новая реальность, а есть новый виток промышленной революции (Индустрия 5.0), цифровая платформенная революция. Устоять при высоком уровне кибератак в одиночку для компании очень дорого, а иногда и невозможно. Поэтому в информационной безопасности все чаще используется аутсорсинг. Многие компании выбирают тестирование своей инфраструктуры и приглашают команды red-team (этичные хакеры), регулярно проверяя киберустойчивость. Кто-то выстраивает модель взаимодействия с центрами мониторинга (security operations centers). Эффективных решений для обеспечения должного уровня информационной безопасности на самом деле достаточно.

G: Насколько мне известно, аутсорсинг в IT провести сложнее, чем в других сферах. Почему? Не могли бы объяснить его основные принципы в ИБ?

Н. Н.: Я бы выделил не столько принципы, сколько этапы. Вначале руководство компании должно осознать риски и уровень угрозы. А потом оценить их,— для этого есть механизмы и алгоритмы действий. На втором этапе выбирается поставщик. Однако, если обращаться к опытному и надежному партнеру, то аудит информационной безопасности и оценку рисков он должен также брать на себя. Поэтому тут, конечно, многое зависит от опыта и компетенций специалистов ИБ-компании. Если она крупная, известная, давно существует на рынке, то как минимум не станет рисковать репутацией, именем и обязательно проведет аудит, совместно с бизнесом оценит риски и предложит максимально эффективное решение.

На третьем этапе уже определяются границы и условия сотрудничества, разрабатываются и внедряются регламенты, настраивается инфраструктура и выстраиваются бизнес-процессы. Каким бы хорошим ни был специалист по ИБ в SOC, он не сможет гарантировать безопасность, если на стороне бизнеса в критический момент пропадет обратная связь и не будут вовремя предприняты рекомендуемые контрмеры. А дальше, на следующих этапах, — мониторинг, контроль, управление инцидентами и восстановление, обеспечение киберустойчивости и поддержка непрерывности бизнес-процессов.

G: Есть ли взвешенная и наиболее эффективная модель взаимодействия заказчиков и исполнителей в ИБ?

Н. Н.: Глобально их всего три. Создание собственного SOC, но это долго и очень затратно. Второй вариант — использование услуг «внешнего SOC», когда вы просто платите, а компания-подрядчик работает в соответствии с вашими запросами. Это самый простой и экономичный путь. Еще один способ — гибрид: у вас собственный SOC, но для исполнения некоторых функций вы привлекаете специалистов извне. Это, пожалуй, самый сложный способ организации, однако его недостатки (высокая стоимость, скорость развертывания, согласование зон ответственности специалистов) уравновешиваются достоинствами. Такой подход — оптимальное решение для крупных компаний с распределенной инфраструктурой.

Чем хорош «внешний SOC»? Эта модель обеспечивает доступ к передовым технологиям и экспертизе компаниям, которым требуется быстрое развертывание безопасности здесь и сейчас. Конечно же, такая модель еще и приводит к снижению затрат, так как закупка оборудования, построение своего SOC — дело не самое простое. Мы в «Газинформсервисе» как раз работаем по такой модели. Создали свой внутренний SOC, разрабатываем киберполигон и программы для обучения и тренировок специалистов по ИБ и готовы предоставлять ресурсы и услуги на аутсорсинг.

G: Какие еще инструменты можно эффективно использовать в ИБ?

Н. Н.: С уверенностью могу сказать, что услуги Red Teaming (этичный хакинг), Purple Teaming (кибертренировки и киберучения) уже доказали свою эффективность, а иногда это единственный инструмент, который покажет бизнесу, чего на самом деле стоит его команда ИБ.

G: Предоставляет ли «Газинформсервис» такие услуги? Как вы собрали свой SOC и проводите ли тестирование на прочность безопасности инфраструктуры клиентов?

Н. Н.: Да, конечно, мы достаточно давно оказываем услуги тестирования на проникновение, накопили богатый опыт, который пригодился нам сейчас,— когда спрос на них бьет все рекорды.

Часть заказчиков приходит, когда нужно удовлетворить требования регуляторов, но многие, что отрадно видеть,— с целью выявить слабые места в своей информационной безопасности и устранить соответствующие риски для бизнеса. С ростом информатизации начинает расти и грамотность в области ИБ. Тем не менее даже заказчики с тщательно выстроенной системой защиты часто оказываются уязвимы перед целевыми атаками, а мы показываем, где именно.

Новой же услугой для нас стал SOC. Если до недавнего времени компании скептически смотрели на возможность отдать собственную информационную безопасность в руки сторонних профессионалов, то в последние два года большинству стало понятно, что реализовать такую защиту своими же силами — сложно, длительно и дорого. Скажу честно, когда мы увидели зарождающуюся волну интереса к услугам SOC и приняли решение строить собственный, то питали иллюзии, что, имея богатый практический опыт, сможем решить задачу за полгода. Однако даже при всех вводных пришлось потратить больше года, чтобы быть готовыми предоставить рынку результат.

При разработке мы выбирали традиционный подход, который гарантирует надежность решения. Но и от современных трендов, таких как искусственный интеллект (ИИ), мы не отказались, а переложили на машинное обучение рутинные функции и задачи, где применение ИИ дает рост эффективности при детектировании угроз.

В основу легли как наши разработки, так и продукты других отечественных лидеров рынка информационной безопасности. Здесь же пригодился опыт тестирования на проникновение: мы проверяем защищенность нашего SOC, чтобы быть уверенными в безопасности данных своих заказчиков. ■