Инфозащита: специализация — как основной фактор успеха

>> Ведущий российский интегратор в области информационной безопасности компания «Инфозащита» отмечает в этом году 10-летний юбилей. Технический директор «Инфозащиты» **Дмитрий Новиков** рассказал редакции журнала «Банковские технологии» о влиянии на отрасль госрегулирования и блокчейна, обосновании затрат на защиту информации, подходах к оценке рисков и актуальных решениях информационной безопасности.

«Банковские технологии»: Дмитрий, как начинался бизнес компании и что представляет собой сейчас?

Дмитрий Новиков: Как во многих интеграторских бизнесах, 10 лет назад все начиналось с нескольких лояльных заказчиков и скромного набора предложений в продуктовой линейке компании. Сейчас в нашем, в хорошем смысле слова, разбухшем, портфеле сотни ИБ-продуктов от более 40 производителей. Приятно отметить, что постоянно нарастает доля отечественных разработчиков, практически во всех классах решений присутствуют конкурентоспособные российские продукты. Более 2500 организаций сотрудничают с «Инфозащитой» для создания современных эффективных систем информационной безопасности. Среди них крупные банки и страховые компании, госструктуры, оборонные и промышленные предприятия, торговля и телекоммуникации.

В компании работает сертифицированный проектный офис, в рамках которого внедрена собственная методология ведения проектов на основе лучших мировых практик. Вкупе с накопленным опытом и компетенциями сотрудников, проектная методология позволяет нам делать очень внятные предложения заказчикам, оптимальным соотношением качества, цены и сроков проекта.

Также у нас работает выделенное R&D подразделение, задачей которого является поиск новых технологий защиты, в том числе иностранных производителей, их тестирование и адаптация к задачам заказчиков. Мы посещаем многие специализированные ИБ-мероприятия, перенимаем мировой опыт, работаем над выводом перспективных решений на российский рынок.

В этом смысле «Инфозащита» не просто находится в тренде, а активно участвует в формировании рынка, способствуя появлению на нем новых высокоэффективных технологий и подходов.

«Б.Т.»: Информационная безопасность — довольно обширная область деятельности. В чем сильна «Инфозащита»?

Д.Н.: Главным образом, мы специализируемся на интеграционных проектах. Условно их можно поделить на 2 основных типа. Первый — это консалтинговые проекты в области информационной безопасности, куда относятся различные виды аудитов, соблюдение комплаенса и т. п. Второй — это собственно внедрение систем информационной безопасности, начиная от стандартной антивирусной защиты до сложнейших проектов мониторинга и управления инцидентами.

В специализированном интеграторском подходе и состоит наша сила и наше преимущество. Вендоры конкретных решений, при всем уважении, заинтересованы прежде всего в продаже своего продукта. Мы же выступаем на стороне заказчика, анализируем его инфраструктуру, оцениваем характер угроз и уровень риска. Исходя из этого, предлагаем комплексное решение, заточенное под задачи конкретной организации.

За последние годы компания успешно реализовала более 300 проектов в различных сферах информационной безопасности. Среди наиболее значимых можно назвать кейс, свя-

занный с созданием территориально-распределенной системы управления учетными записями и сессиями. Еще хотелось бы отметить масштабный проект одного из заказчиков по построению системы защиты от таргетированных атак, мониторинга и управления инцидентами.

«Б.Т.»: Как изменилась отрасль за последние несколько лет? Что в наибольшей степени влияет на решения заказчиков о внедрении систем информационной безопасности?

Д.Н.: Сильно меняется законодательное поле, нормативная база. В разное время рынок драйвили появление закона о персональных данных, различных требований Центробанка. Сейчас на повестке дня новый закон о безопасности критической информационной инфраструктуры, который затрагивает и финансовые организации: банки, страховые компании, платежные системы. Появились государственные информационные системы ГосСОПКА и ФинЦЕРТ, с которыми должны взаимодействовать финансово-кредитные организации при возникновении инцидентов. Это тоже требует автоматизации, проработки новых бизнес-процессов и внедрения новых подходов.

Взять такую актуальную технологию, как блокчейн, с которой экспериментируют в том числе банки. В прошлом году у всех на слуху были скандалы, связанные со взломом криптобирж. В этом перспективном направлении возникают, в том числе, свои специфические риски, о которых нужно задумываться, кстати, некоторые производители этим уже озадачились. Как минимум, уже сейчас можно работать с решениями по анализу кода в блокчейн-проектах.

«Б.Т.»: Если фокусироваться на функционале средств защиты, какие новации востребованы в отрасли?

Д.Н.: Если говорить о новых классах решений, за последние 2 года получили распространение deception-системы. Это своеобразные «ловушки», которые провоцируют проникновение в инфраструктуру, которая выглядит привлекательной для злоумышленников, но при этом существует параллельно от основной, и невидима для пользователей организации. В этой среде мы можем изучать поведение хакеров, их цели и методы.

Появились решения, связанные с поведенческим анализом, они уже внедрены в некоторых банках. Другой тренд — использование элементов искусственного интеллекта в целях информационной безопасности, такие проекты тоже есть в России. Вообще, всё чаще заказчики задумываются о проактивном подходе к защите информации, особенно коммерческие организации, достигшие определенного уровня развития бизнеса. В арсенале ИБ есть решения, позволяющие прогнозировать атаки и иметь наготове инструменты для эффективной защиты.

Среди других направлений — рынок «распробовал» решения по защите от направленных угроз, автоматизации и управлению инцидентами ИБ. Всё больше заказчиков, государственных и коммерческих организаций уже реализовали или планируют создание полноценных SOC-решений. Это центры обеспечения безопасности, в рамках которых организуется комплексный процесс защиты и увязываются воедино 3 ключевых компонента: процессы, люди и технологии. Также мы отмечаем живой интерес по тематике защиты АСУ ТП.

«Б.Т.»: Какие изменения происходят на «темной стороне», в стане киберпреступников?

Д.Н.: Злоумышленники становятся более изощренными, растет число атак, направленных на конкретных заказчиков. Это уже не партизанская война, вылазки в попытках нащупать брешь, а стратегические боевые действия: с предварительной разведкой, своим продвинутым инструментарием и т. д. В этой связи у безопасников появляются новые задачи — не только защититься от взлома, но и грамотно реагировать на выявленные инциденты, минимизировать последствия. Часто бывает, что злоумышленник уже проник в инфраструктуру, но пока явно себя не проявляет, ведет разведку и готовится нанести удар. Deception-решения позволяют предотвратить такие угрозы — причем как от внешних, так и от внутренних злоумышленников.

По нашим наблюдениям, более чем в половине случаев злоумышленниками являются именно внутренние пользователи, то есть недобросовестные сотрудники организации. Для снижения таких рисков существуют свои инструменты, например, система по контролю привилегированных учетных записей. Такой класс решений, PIM (Privileged Identity Management), востребован у крупных компаний, у нас довольно много проектов по их внедрению.

Практика последнего времени показала, что уязвимы абсолютно все сферы. Если раньше злоумышленники нацеливались главным образом на IT-процессы бизнеса, нарушение функционирования, похищение денег со счетов или кражу данных, то в последнее время их внимание привлекли технологические процессы. Злоумышленники понимают, что нарушить производственные процессы сейчас намного более критично, чем зашифровать обычный офисный ПК.

«Б.Т.»: Как обосновать экономическую целесообразность того или иного ИБ-решения в организации, существуют какие-то сложившиеся подходы? Обосновать ценность предотвращения убытков, вероятно, сложнее, чем дополнительного дохода или экономии при покупке IT-систем бизнес-назначения...

Д.Н.: Такой запрос часто возникает у крупных компаний, которые уже используют достаточно много ИБ-инструментов, и необходимость внедрения какого-то нового решения требует серьезного обоснования. Пока драйвером новых проектов чаще выступают всё-таки требования регуляторов, или в худшем случае — произошедшие инциденты.

Вместе с тем вопрос оценки рисков информационной безопасности чрезвычайно актуален. Упрощенно подход можно описать так. Специалисты по рискам анализируют ситуацию в части защиты информации, оценивают вероятность возникновения различных инцидентов и возможные убытки. К основным рискам относятся прямые финансовые потери — как в результате хищения средств, так и простоя критических для бизнеса IT-систем.

Какова ценность той или иной информации и возможный ущерб в случае ее кражи или уничтожения? Какие репутационные риски возникают у компании, насколько серьезное влияние окажут на бизнес, отношения с клиентами и партнерами киберпреступления, если они произойдут? Дать оценку при ответе на вопросы о косвенных убытках непросто, но полезно — в итоге происходит некое моделирование рисков. Мы внедряем систему стоимостью, скажем, 1 миллион, благодаря которой уменьшаем вероятность возникновения таких-то рисков на 70%, в итоге мы получаем защиту от возможных убытков на сумму в 20 раз больше. Это понятная постановка вопроса для топ-менеджмента и акционеров.

В идеале взаимодействие безопасников и рисковиков должно привести к появлению комплексной системы оценки рисков, которую нужно постоянно актуализировать под влиянием регуляторных требований, изменений инфраструктуры, выявления новых угроз и т. д. Такая система может быть увязана с SOC-центром, ее данные позволят принимать решения о внедрении той или иной системы (как и другие управленческие вопросы в области ИБ и в целом IT) более обоснованно и, в конечном счете, эффективно.

В этой части есть еще одна тема — страхование рисков в области информационной безопасности. Этот сервис распространен во многих странах с развитой экономикой. Периодически разговоры о нем возникают у нас, но большой популярности пока нет, в первую очередь из-за отсутствия адекватных предложений со стороны страховщиков. Отчасти это связано с недостатком статистики, на которой базируется любое страхование, компании ведь неохотно делятся данными по инцидентам. Хотя, скажем, в банковской сфере ФинЦЕРТ Центробанка, куда финансовые организации передают данные об инцидентах, может выступить источником такой статистики, что станет стимулом развития страхования рисков.

>>Уязвимы абсолютно все сферы. Если раньше злоумышленники нацеливались главным образом на IT-процессы бизнеса, нарушение функционирования, похищение денег со счетов или кражу данных, то в последнее время их внимание привлекли технологические процессы.

«Б.Т.»: Чего ждать отрасли в ближайшие годы, какие угрозы и решения будут актуальными?

Д.Н.: Если говорить о ближайшем будущем, будет много внедрений, связанных с регулированием, прежде всего законом о КИИ — критической информационной инфраструктуре. Мы видим, что появляются новые угрозы, связанные с распространением многообещающей технологии интернета вещей. Повсеместное увлечение блокчейном тоже порождает совершенно новые риски. С новыми угрозами разрабатываются и новые решения, на фоне общего технического прогресса развиваются и средства защиты. Соответственно, и мы, как интегратор, наращиваем экспертизу и арсенал инструментов обеспечения безопасности.

Я уже упоминал о нашем R&D подразделении, которое целенаправленно работает с вендорами на глобальном рынке ИБ-решений. Его миссия состоит в том, чтобы находить и предлагать нашим заказчикам новые, наиболее эффективные решения, в том числе для защиты от только зарождающихся киберугроз.