ИБ-маневры

Новый подход к управлению информационной безопасностью на базе «цифровых двойников», или Как быстро, недорого и качественно автоматизировать процессы ИБ

Текст
РУСТАМ ГУСЕЙНОВ,
ПРЕДСЕДАТЕЛЬ RAD COP
НИКОЛАЙ КАЗАНЦЕВ,
ОСНОВАТЕЛЬ SECURITM

Рустам Гусейнов

Николай Казанцев

Любая область деятельности, любая сфера знаний переживают свои этапы развития. Фаза «алхимии и волшебства», где доминируют творчество и эксперименты, сменяется фазой зрелости и становления лучших практик, на которой формируются общепринятые подходы и стандарты. Затем, если развитие не останавливается, появляются автоматизация и шаблонизация, снятие рутинных задач с человека и в идеале освобождение времени на решение новых творческих задач, обучение, стратегические проекты. Наконец, если все получается, область становится настолько привычной и понятной, что мы просто перестаем осознавать, что происходит и как это работает. Почти все знают азы арифметики и умеют читать, но мало кто сходу сможет осознанно рассказать про устройство языка и математики. И уж тем более мало кто помнит, как тяжело происходило становление соответствующих наук: одно изобретение привычного нам алфавита заняло сотни и тысячи лет, но вот он есть, и мы играючи решаем с его помощью сложнейшие вопросы, даже не осознавая этого колоссального пути. К счастью, в XXI веке многие процессы протекают значительно быстрее, и сегодня на наших глазах описанная выше эволюция происходит с информационной безопасностью.

Ключом к пониманию нового подхода является появление платформ автоматизации процессов ИБ, нового витка развития систем класса SGRC[1], которые представляют собой что-то вроде корпоративного органайзера. Только в отличие от GTD-ежедневника[2] мы управляем не «входящими» задачами и портфелем проектов, разбитым на категории и контексты, а процессами информационной безопасности в разрезе сформированного «цифрового двойника» предприятия, куда зашиты не только активы (информационные системы, серверы, средства защиты), но и существующие политики и процедуры компании, задающие «правила игры» и вписывающие ИБ в общую стратегию развития организации. Причем львиная доля задач, начиная с инвентаризации активов и агрегации событий и заканчивая динамической оценкой уровня зрелости ИБ и сопоставлением требований различных стандартов/требований друг с другом, снимается с живых людей и передается самой платформе. А задачи и коммуникации, которые нельзя полностью авто-

[1] Security Governance, Risk, Compliance — класс решений, обеспечивающих управление информационной безопасностью.

[2] Getting_Things_Done — методология, сформулированная Дэвидом Алленом.

матизировать, оптимизируются, потому что на смену различным каналам коммуникаций и инструментам (мессенджерам, почте, календарям, неадаптированным тикетным системам и т.п.) приходит специализированный инструмент, который к тому же обладает информацией об устройстве комплексной системы защиты компании, ее текущем состоянии и непрерывно обновляет ее.

Представьте себе образ спокойного CISO (директора по информационной безопасности), который понимает, что контролирует ситуацию и осознанно приоритизирует задачи ИБ, не утопая в текучке и не сгорая в пожарах. Представьте его коллег и сотрудников, которые могут «сверять часы» и управлять задачами на централизованной платформе, минуя джунгли мессенджеров и почтовых программ и не теряя важных «входящих». Представьте, что вся рутинная работа по анализу требований и поиску типовых решений автоматизирована, и у вас остается время на изучение нового и обдумывание важных, но не срочных задач. Представьте, наконец, что и у руководства компании, и у внешних/внутренних аудиторов есть доступ к динамическим показателям оценки зрелости ИБ, уверенность в понятной отчетности, которой можно доверять, и четкое понимание, что ИБ движется в правильном направлении.

За счет чего это оказывается возможным и какие здесь есть подводные камни, можно посмотреть в ролике (см. QR-код справа), но суть проста:

- организация запускает внедрение платформы для автоматизации процессов ИБ;
- внедрение сопровождается аудитом и консалтингом, которые проводятся на базе SGRC; на ней же оцифровываются все результаты аудита, параллельно система интегрируется с технической инфраструктурой компании, создавая в итоге «цифровой двойник» инфраструктуры и процессов организации;
- по окончании и в процессе работ проводится обучение сотрудников в части последующего использования платформы, консультанты помогают договориться внутренним подразделениям и сотрудникам о зонах ответственности, решают каверзные проблемы и обеспечивают «жизнь системы» после своего ухода;

В результате синергии профессионального аудита и платформы автоматизации у службы ИБ появляется не только видение текущей ситуации, но и «цифровой двойник» всей системы безопасности, на базе которого продолжают строиться и улучшаться процессы ИБ. А все последующие контрольные мероприятия сводятся к выгрузке из системы отчетов о текущем состоянии дел.

Если, дочитав до этого места, читатель думает, что такой подход — удел крупного бизнеса с многомиллионными бюджетами на ИБ и десятками сотрудников службы безопасности, то он ошибается. Вернемся к началу: времена меняются, и наша отрасль становится более зрелой, что проявляется в появлении недорогих и качественных решений, гарантированно внедряемых в адекватные сроки. Мы научились запускать подобные проекты менее чем за полгода с бюджетом от 1 до 5 млн рублей, что позволяет даже небольшим организациям оценить преимущества правильно внедренных и грамотно эксплуатируемых SGRC-платформ.

Это стало возможным с появлением на рынке сервиса управления информационной безопасностью SECURITM — нового отечественного решения для управления всеми организационными процессами в службах ИБ: управление рисками, аудитами и соответствием (комплаенс), активами (ITAM), техническими уязвимостями (VM), автоматизацией процессов (RPA), инцидентами, обучением, задачами, планированием, метриками и отчетностью.

Миссия, заложенная в SECURITM, — дать в руки каждой службе безопасности простой, удобный и в то же время мощный инструмент для автоматизации процессов вне зависимости от текущего уровня зрелости и имеющегося бюджета. Для этого система обладает как простыми функциями, так и сложными автоматизациями, собраны готовые базы знаний, помогающие с быстрым стартом, сделаны понятное ценообразование и открытый прайс, выпущена комьюнити-версия и обеспечена возможность работы как облачной, так и локальной инсталляции. А для финансовой отрасли особенно ценны автоматический комплаенс по ГОСТ 57580 и отчетность по положениям Банка России. Все возможности платформы можно изучить в комьюнити-версии по адресу https://service.securitm.ru.

Объединяя экспертизу профессиональных аудиторов и мощь платформы автоматизации, наши проекты помогают службам безопасности вырваться из «дня сурка», наполненного рутиной задач, и начать управлять своей системой безопасности.

Если вы дочитали до этих строк, то, вероятно, подход заинтересовал вас настолько, что стоит связаться с нами и, не откладывая на будущее, обсудить возможные сценарии быстрого, качественного и недорогого внедрения SGRC. Б.О