**Андрей Лупешко, Compliance Control: Консалтинг – явление разностороннее**

На вопросы организаторов IT-SECURITY CONFERENCE о состоянии рынка информационной безопасности в России и Республике Беларусь, о вызовах, стоящих сегодня перед компаниями в финансовой и банковской сферах, и об особенностях реализации проектов в направлении SSDLC рассказал директор по развитию бизнеса Compliance Control Андрей Лупешко.

**О компании**

Compliance Control – одна из первых консалтинговых компаний в сфере информационной безопасности в России и некоторых странах СНГ, включая Республику Беларусь. С 2012 года её эксперты оказывают услуги по сертификации платёжной инфраструктуры и аудиту защищённости сервисов и приложений. Опыту компании доверяют представители ведущих компаний из банковской сферы, FinTech и ритейла.

– **Андрей, добрый день, для начала расскажите немного о деятельности Вашей компании, в частности о развитии бизнеса в Республике Беларусь.**

– Добрый день!

Уже более 10 лет наша компания оказывает консалтинговые услуги для заказчиков в Республике Беларусь, нашими клиентами являются в первую очередь представители банковского сектора, а также отрасли финтеха в целом.

Если выделять направления, в которых мы традиционно сильны, следует отметить проведение аудитов ИБ по требованиям различных стандартов (PCI DSS, ISO, SWIFT), а также оказание услуг по тестированию на проникновение инфраструктуры и анализ защищенности приложений.

– **Поговорим о состоянии рынка ИБ в Республике Беларусь. Какие тенденции развития мы наблюдаем сегодня? Чем ситуация в РБ отличается от ситуации в России или других регионах?**

– Отвечая на данный вопрос, хотелось бы прежде всего подчеркнуть, что мы описываем ситуацию именно со стороны консалтинговой компании, так как наше видение может отличаться от видения вендоров ПО и интеграторов.

Что касается состояния и потребностей рынка ИБ, в первую очередь можно отметить ограниченность ресурсов на рынке – заказчики часто сталкиваются с кадровым голодом. Если же говорить о перспективе, мы видим заметное повышение актуальности темы построения процессов безопасной разработки ПО, в чём наша компания за последние годы нарастила значительную экспертизу благодаря успешным проектам в РФ, Азербайджане, Казахстане и Беларуси.

В совокупности эти два фактора – потребность в построении процессов безопасной разработки ПО и ограниченность ресурсов на рынке (а в области SSDLC недостаток экспертов ощущается еще сильнее) – формируют наше предложение по развитию в регионе.

Мы готовы оказывать полный комплекс консалтинговых услуг, включая аудит текущего состояния процесса разработки с точки зрения ИБ, создание долгосрочного плана построения и повышения зрелости процессов SSDLC, а также дальнейшей поэтапной реализации данного плана совместно со специалистами заказчика.

– **К вопросу о ресурсах заказчика: Вы сказали ранее, что нужных специалистов крайне мало. Как же тогда заниматься выстраиванием процессов?**

– Да, всё верно. За время нашей работы по данному направлению мы собрали огромный объем обратной связи от клиентов. Их основной мотив: «Мы готовы выстраивать процессы, но у нас нет человека, который будет заниматься этим проектом».

Это проблема, решить которую можно только при тесном взаимодействии консультанта и заказчика. В ходе проекта, помимо непосредственного выстраивания процессов, мы занимаемся обучением и погружением разных специалистов заказчика в область SSDLC.

Зачастую удается начать уверенно двигаться по проекту, когда на стороне заказчика находится энтузиаст со скилами в разработке senior, а главное – с желанием развиваться в безопасной разработке. Далее за дело принимаются уже наши эксперты-консультанты.

Но, отвечая на изначальный вопрос, должен уточнить, что обязательно должен быть человек на стороне клиента. Профильного специалиста найти крайне сложно и дорого, в связи с чем мы готовы заниматься переобучением имеющихся ресурсов клиента и имеем опыт в содействии при собеседовании претендентов на должность. В общем, консалтинг – явление разностороннее.

– **Какие еще есть факторы, тормозящие развитие направления безопасной разработки, и что Ваша компания может предложить в этой части?**

– Помимо проблемы с экспертами, есть сложности и с инструментами ИБ, а именно с традиционным набором сканеров (SAST, DAST, SCA), которые должны быть встроены в процесс разработки.

Здесь мы приходим к классической развилке: использовать платные инструменты - дорого, а бесплатные – сложно и неудобно.

Мы, как консультанты, имеем всесторонний опыт: если у заказчика есть платное решение, но не хватает ресурсов и/или экспертизы, чтобы с ним работать, мы поможем

с его корректной интеграцией в pipeline разработки, выстроим процесс тестирования, обучим людей и опишем весь процесс.

Если же платного решения нет и, в связи с ограниченностью бюджета, его приобретение не планируется, мы подберем оптимальный набор open source-решений под конкретный технологический стек клиента. В данной модели нашим основным активом является экспертиза в части настройки инструментов. Каждый, кто сталкивался с работой open source-решения, знает, что провести сканирование просто – сложно работать с его результатами.

Эксперты нашей компании осуществляют настройку инструментария, затем проводится ряд этапов отработки ложных срабатываний, и на выходе, после нескольких месяцев работы системы и ее «тюнинга» в боевых условиях, мы добиваемся результатов в части тестирования ПО и статистики по ложным срабатываниям на уровне платных сканеров, а зачастую превосходим их.

Подводя итоги, отмечу, что мы имеем опыт и экспертизу и планируем активно делиться ей с рынком.

– **Большое спасибо за информацию по этой теме. Может быть, есть еще направление, которое вы планируете развивать на рынке Республики Беларусь?**

– Да, помимо экспертизы в части SSDLC мы планируем заниматься облегчением жизни заказчиков в области ИБ-комплаенса.

Поскольку compliance – исторически наше основное направление бизнеса, мы прекрасно понимаем, сколько сил уходит у заказчиков на поддержание процессов в соответствии с требованиями различных внешних и внутренних стандартов в части обеспечения ИБ.

С целью автоматизации данных процессов мы создали платформу Compliance App – инструмент, который по нашей экспертной оценке помогает CISO и Compliance-менеджерам экономить до 30% времени, расходуемого на периодические задачи в рамках поддержания соответствия требованиям, что в текущих экономических реалиях крайне актуально для рынка как РФ, так и РБ.

Подробно говорить о функционале решения в рамках нашей беседы я не буду, скажу лишь, что для рынка РБ, помимо базовых шаблонов проектов по международным стандартам, таким как PCI DSS, ISO и SWIFT, мы добавили готовые шаблоны по локальным требованиям в области обработки персональных данных и постановлений Оперативно-аналитического центра при Президенте Республики Беларусь.

В заключение хотелось бы отметить, что, получая обратную связь от рынка, мы видим, насколько актуально данное направление для наших коллег, имеющих большую комплаенс-нагрузку.

Мы в свою очередь фиксируем все пожелания по функционалу от коллег и включаем их в план развития продукта, чтобы сделать его еще более полезным с прикладной точки зрения.

Подробнее о продукте Compliance App мы будем рады рассказать на вебинаре, который состоится 1 апреля.

COMPLIANCE CONTROL