TADVISER
Государство. Бизнес. ИТ

2016/10/11

ИНТЕРВЬЮ С НАЧАЛЬНИКОМ ОТДЕЛА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ «АМТЕЛ-СЕРВИС» АЛЕКСЕЕМ ЗАЛЕЦКИМ

Амтел Сервис

АЛЕКСЕЙ ЗАЛЕЦКИЙ: МЫ ПОМОГАЕМ ЗАКАЗЧИКУ УВИДЕТЬ ВСЮ КАРТИНУ БЕЗОПАСНОСТИ ОБЛАКА

Алексей Залецкий в интервью TAdviser рассказал о развитии рынка ИБ, изменениях российского законодательства в сфере ИБ и ключевых направлениях АМТЕЛ-СЕРВИС в этой области, в том числе о подходе к защите частного облака.

TADVISER: Каковы общие тенденции рынка информационной безопасности – в мире, в России?

Алексей Залецкий: Согласно данным аналитических агентств в мире наблюдается рост атаковой активности, причем растет процент атак, нацеленных на конкретные компании и организации. В ответ на это рынок информационной безопасности и разработчики средств защиты начали предоставлять узкоспециализированные средства – в противовес и в дополнение традиционным универсальным решениям. Например, появились межсетевые экраны прикладного уровня и средства защиты от таргетированных атак. Помимо специфических тенденций, связанных с эволюцией угроз, на рынок ИБ воздействуют и тенденции, наблюдаемые в целом на мировом ИТ-рынке: большие данные, мобильность, массовый переход компаний к использованию облаков. В результате на рынке появляются специализированные технологии, решения и продукты для защиты облаков, обеспечения безопасности мобильных коммуникаций, учета требований по работе с большими данными.

На российском рынке ИБ наблюдаются те же самые тенденции, что и на мировом. Особенности связаны, в основном, с требованиями регуляторов рынка, в том числе в части сертификации средств защиты информации, применением отечественной криптографии. Стоит отметить, что в России постепенно растет популярность услуг аутсорсинга ИБ и услуг по тестированию на проникновение, к которым в предыдущие годы отечественные организации относились весьма настороженно. В этом плане мы несколько отстаем от западных стран.

TADVISER: Какие новые ИБ-решения появились на рынке за минувшие два-три года?

Алексей Залецкий: За последние 2-3 года, на наш взгляд, не появились принципиально новые решения. Скорее можно констатировать более активное развитие технологий, уже представленных на рынке. Например, вырос спрос на специализированные экраны по защите от web-атак (Web-Application Firewall), что повлияло на появление новых интересных продуктов данного класса. Эволюционировали и классические средства защиты информации. Так, межсетевые экраны следующего поколения обеспечивают защиту, основываясь на пользователях и приложениях, к которым они обращаются. Производительность российских криптошлюзов увеличилась до 10 Гб/сек при использовании отечественной криптографии. Это то, чего давно ждали наши заказчики, обрабатывающие большие объемы данных, в том числе банки, энергетические компании, крупные государственные структуры.

В части облаков стали популярны средства защиты виртуальной среды от несанкционированного доступа, безагентные антивирусы и другие специализированные средства защиты информации. В этом сегменте появилось больше продуктов от разных производителей.

Широкое использование заказчиками мобильных устройств привело к потребности в решениях для управления мобильными данными – MDM (Mobile Device Management), которые позволяют реализовать защиту данных при использовании коммуникаторов, планшетов, смартфонов. Еще одно направление, где в последнее время появляются новые средства ИБ – защита АСУТП (автоматизированная система управления технологическими процессами). Что касается защиты сред больших данных, появление основных решений и продуктов, использующих данный подход, еще впереди.

TADVISER: Какие инновации российского законодательства заметно повлияли на рынок ИБ?

Алексей Залецкий: Нормативных инноваций, повлиявших на российский ИБ-рынок, в минувшее десятилетие появилось достаточно много. Из недавних документов – на активное развитие решений в области защиты АСУТП активно повлиял Приказ ФСТЭК №31 от 14.03.2014 года, расставивший приоритеты по защите информации на критически-важных объектах. Также стоит вспомнить и появление 10 лет назад Закона 152-ФЗ от 27.07.2006 года «О персональных данных». Хочу подчеркнуть, что этот закон – поворотный момент в развитии рынка информационной безопасности в России. Именно после его появления компании стали рассматривать ИБ не просто как подсистему внедряемых информационных систем, а как отдельную систему. В дальнейшем серьезное влияние на рынок оказали Приказ №21 от 18.02.2013, определявший как выполнять защиту персональных данных, Приказ №17 от 11.02.2013 о защите государственных информационных систем, Закон «О национальной платежной системе» от 27.06.2011.

Из недавних инноваций – принятый этим летом ГОСТ Р 56938-2016 «Защита информации. Защита информации при использовании технологий виртуализации. Общие положения», впервые в российском законодательстве определивший каким образом необходимо обеспечивать защиту среды виртуализации, которая является основой создания частных облаков, различные аспекты по защите информации при переходе в облака. Данный стандарт, что радует, рассматривает не только защиту самой среды виртуализации, но и защиту виртуальных средств защиты информации и средств защиты информации, предназначенных для использования в среде виртуализации. Но если говорить про облака в целом, то стандарт не содержит информации о методах защиты в зависимости от типа используемых облачных сервисов (IaaS, PaaS или SaaS) и ряда других аспектов, в том числе защиты клиентского уровня. Думаю, это все найдет отражение в стандартах, которые мы ожидаем в ближайшие годы.

Появление отечественного стандарта ГОСТ Р 56938-2016 в первую очередь дало возможность сравнить прежние подходы с рекомендуемыми. Например, мы убедились, что подход и методология по защите облачных систем, применяемые нами, полностью соответствуют ГОСТ в части, которую он покрывает, в остальном мы продолжаем ориентироваться на иностранные стандарты и рекомендации.

TADVISER: Что можно сказать о менталитете российского заказчика решений по ИБ – есть ли стереотипы (заблуждения) о ситуации с ИБ и какова реальная ситуация?

Алексей Залецкий: Не думаю, что российские заказчики обладают неким особым менталитетом, но стереотипы в части ИБ имеются. И первый из них состоит в несколько пренебрежительном отношении к внутренним документам по ИБ – регламентам, правилам и т.п. Я не редко сталкиваюсь с мнением, что это лишь формальность, а основное для защиты информации – использование программно-аппаратных средств. На самом деле документы (разумеется, в связке с обучением персонала и контролем их исполнения) тоже крайне важны для создания эффективной системы ИБ. Например, можно прийти в компанию или позвонить по телефону, и при помощи методов социальной инженерии элементарно выудить у сотрудников конфиденциальную информацию. И от таких способов и путей проникновения за корпоративный периметр наличие специальных программно-аппаратных средств не защитит. Необходим комплексный подход, подразумевающий и разработку действенных, качественных документов по ИБ, и применение современных средств защиты информации.

TADVISER: Наверное, уместно в этом контексте упомянуть важность создания корпоративной культуры информационной безопасности…

Алексей Залецкий: Безусловно. Информационная безопасность – не разовая задача, не нечто статичное, это процесс, который должен быть встроен в общую систему управления организацией. И с появлением новых технологий – облачность, мобильность, большие данные – подходы к обеспечению

ИБ тоже должны меняться, документы совершенствоваться, система защиты эволюционировать.

TADVISER: Какие еще заблуждения по части ИБ имеются у российских заказчиков?

Алексей Залецкий: Второе заблуждение: защита персональных данных больше не актуальна. Такое мнение складывается из-за того, что тема ПДн ныне не занимает первое место в информационной повестке по ИБ. На самом же деле это не так, например, количество обращений физических и юридических лиц с жалобами по персональным данным в Роскомнадзор за прошлый год увеличилось на 60,44%. С каждым годом растет количество проверок и объемы штрафов за несоответствие процессов обработки персональных данных требованиям законодательства. Так, например, в нашей компании спрос на аудит и приведение процессов обработки персональных данных в соответствии с российским законодательством за последний год вырос более чем в два раза.

Третий стереотип касается облачных технологий. Многие по сей день считают, что информационную безопасность ИС при использовании облаков, в том числе – частных, невозможно обеспечить на том же уровне, что для классических ИТ-систем. На самом деле, современные средства защиты информации в облаках уже доказали свою высокую эффективность, и опыт нашей компании это подтверждает. Отмечу, что данный стереотип можно считать положительным, т.к. при переходе к использованию облачных технологий вопрос ИБ всегда поднимается на достаточно высоком уровне. Более того, многие реализованные в последние годы облачные решения более безопасны в использовании, чем традиционные.

И четвертый стереотип: информационная безопасность – это только затраты. Однако, как показывает практика, все больше компаний используют ИБ как способ получения конкурентного преимущества. Например, банк, внедряющий новые продвинутые технологии ИБ, может использовать этот факт в рекламных целях, привлекая клиентов, для которых вопросы безопасности особенно чувствительны.

TADVISER: А в целом, какие изменения произошли в отношении к ИБ за последние годы?

Алексей Залецкий: Если посмотреть на ситуацию в целом, то согласно оценкам зарубежных и российских аналитических агентств, заказчики стали несколько спокойнее относиться к публикации данных об инцидентах ИБ. Еще десять лет назад количество публикаций по инцидентам было крайне малым, в результате чего имевшиеся статистические данные были не пригодны для анализа. Большинство компаний скрывали информацию о взломах, часть компаний даже не знали о том, что их системы были взломаны – так как не обладали на тот момент средствами, позволяющими получать информацию о происходящих инцидентах. Сегодня есть и технологии и средства. Например, использование DLP-систем позволяет обнаруживать утечки конфиденциальной информации. Использование SIEM-систем кроме основной своей функции также позволяет получать статические данные по инцидентам ИБ. Данные инструменты, помимо всего прочего, еще повышают прозрачность и контролируемость бизнеса и, как мы уже говорили выше, способны предоставить дополнительное конкурентное преимущество.

TADVISER: Ключевые направления «Амтел-Сервис» в области ИБ?

Алексей Залецкий: Информационная безопасность – одно из ключевых направлений «Амтел-Сервис», сейчас его доля в выручке компании составляет порядка 20%. Портфель услуг по ИБ мы условно разделяем на 4 группы. Первое и основное направление – обеспечение ИБ, куда входят услуги и решения, необходимые как для создания комплексных систем защиты информации, так и отдельных подсистем. Каждый второй такой проект является частью комплексного инфраструктурного проекта. Стоит отметить, что на данный момент сохраняется спрос на СОИБ для классических ИТ-систем, но при этом растет доля проектов по защите частных облаков. К этой же группе мы относим услуги по аутсорсингу ИБ, реализация которых происходит на базе Сервисного центра компании, где хорошо отлажены все процессы и методология реализации SLA-проектов разного масштаба.

Вторая группа услуг – обеспечение соответствия организаций требованиям российских регуляторов, в т.ч. 152-ФЗ, которые часто сопряжены с услугами по построению соответствующих систем. Третье направление включает услуги по разработке документов по ИБ, инструментальный аудит информационных систем, включая активный (проведение пентестов), спрос на который стремительно растет. И четвертое направление – аттестация объектов информатизации и лицензионная работа.

По предварительным итогам 2016 года первое место по востребованности, а также реализации среди наших заказчиков делят услуги по ЗПДн, включая аттестацию, и защита облачных сред – как корпоративных, так и помощь в обеспечении защиты инфраструктуры облачных провайдеров.

TADVISER: Расскажите чуть подробней о проблематике защиты частных облаков – как повлиял новый ГОСТ на рынок, каковы проблемы продуктового подхода, пример проекта по защите частного облака?

Алексей Залецкий: Новый ГОСТ по защите средств виртуализации не охватывает всех аспектов защиты облаков, и в силу того, что был принят недавно – в июне этого года, существенно сказаться на рынке еще не успел. До появления данного ГОСТ российские заказчики ориентировались на западные стандарты, но чаще всего использовался продуктовый подход, основанный на лучших практиках, представленных на рынке. Основная проблема продуктового подхода – невозможность обеспечить комплексную систему защиты в облаке. Так, проводя аудит, мы зачастую сталкиваемся с тем, что заказчик делает большой упор на один из уровней защиты: клиентский, приложения, платформы/инфраструктуры. Например, на высоком уровне выполнена защита среды виртуализации, но при этом не решен вопрос по защите на клиентском уровне, не решены вопросы с обеспечением безопасности при получении доступа с мобильных устройств к облаку, что приводит в целом к крайне низкому уровню защищенности. Собственно, мы помогаем заказчику увидеть всю картину безопасности облака и устранить уязвимости.

TADVISER: Для каких заказчиков вы реализовали проекты по защите частного облака?

Алексей Залецкий: За последний год мы реализовали проекты по обеспечению защиты при переводе ИС на облачную платформу для нескольких операторов связи, а также в ряде финансовых организаций, у которых были построены частные облака с комплексной защитой информации. Каждый проект по-своему уникален. Они отличались используемыми облачными сервисами (IaaS, PaaS или SaaS) и моделями их предоставления пользователям. В каждом из данных проектов система защита частного облака зависела от применяемой среды виртуализации и системы управления облачными сервисами. Решения отличались на всех уровнях: клиентском, приложения, платформы/инфраструктуры. Однако, методология во всех проектах единая: проводится детальное обследование с анализом угроз для каждого уровня (это важнейший этап, так как при всем многообразии реализации облаков, прорабатываемое техническое решение сильно зависит от модели угроз), прорабатывается техническое решение, которое в дальнейшем реализуется. Наиважнейшие задачи, которые приходилось решать в процессе данных проектов – это обеспечение конфиденциальности обрабатываемых в частных облаках данных, разграничение доступа, защиты от вредоносного кода и различных типов атак, а также управления системой и событиями безопасности облака.

Универсального типового решения здесь нет и вряд ли появится в ближайшие годы. Это обусловлено разными причинами, в том числе недостаточностью стандартов в области защиты облаков, средствами защиты информации, нацеленными на разные аспекты защиты, но пересекающиеся по части функций, нацеленностью средств защиты лишь на крайне ограниченный набор сред виртуализации.

TADVISER: Как вы оцениваете перспективы рынка ИБ? Каковы планы компании?

Алексей Залецкий: Рынок ИБ растет, несмотря на кризис – это можно констатировать, основываясь на информации аналитических агентств и нашем собственном опыте. По результатам трех кварталов мы рассчитываем на 25% рост выручки по направлению по результатам текущего года в сравнении с 2015 годом, а также планируем сохранять положительную динамику и в дальнейшем. Ключевыми нашими заказчиками по ИБ являются банки, ритейл, операторы связи, также на 2017 год планируется ряд масштабных проектов для госсектора.

«Амтел-Сервис» будет и дальше предлагать услуги по защите информации как для традиционных ИТ-систем, так и с учетом трех главных технологических трендов современного ИТ-рынка – облачные технологии, мобильность, большие данные. Продолжим совершенствовать и развивать услуги по защите персональных данных, аттестации систем на соответствие требованиям законодательства.