Леонид Ухлинов: Мы помогаем сохранить бизнес – это наш девиз на ближайшие годы

Издание: Anti-Malware.ru, 5 декабря 2018 г.

Спикер: Леонид Ухлинов, вице-президент «Информзащиты»

Вице-президент компании «Информзащита» Леонид Ухлинов рассказал читателям Anti-Malware.ru об обстановке на рынке информационной безопасности, обозначил позиции «Информзащиты», ближайшие перспективы развития компании и поведал о трудностях, с которыми она столкнулась в 2018 году, а также поделился секретами поиска и мотивации ценных специалистов.

Что, на ваш взгляд, повлияет на российский рынок ИБ в ближайшие 2-3 года?

Л.У.: За последнее время серьезно усилилось понимание у руководителей бизнеса, особенно крупного, что информационная безопасность обеспечивает им правильное выполнение внутренних бизнес-процессов. Это важно, потому что раньше приходилось постоянно объяснять, что ИБ — неотрывная часть информатизации в целом. Но в большинстве случаев мы слышали в ответ «Да от кого нам защищаться!» или «Не такие уж и большие угрозы» и даже «Ну и что я могу потерять».

Сейчас разговор строится совершенно в другом русле, потому что вся деятельность компаний, особенно при переходе на цифровую экономику, переводится в цифровой формат. И само существование бизнеса сильно зависит от того, насколько достоверно, правильно и своевременно предоставляется информация в те или иные системы предприятия. Идет активный переход на цифровую экономику, и это серьезно усложняет жизнь самого бизнеса с точки зрения возможного вмешательства в этот бизнес со стороны. Те, чьи предприятия тесно завязаны на непрерывных технологических процессах, понимали это давно. Приход же понимания у руководителей любого бизнеса, что без ИБ уже никуда — основной фактор развития рынка на ближайшие 2-3 года.

В прошлом году в интервью для Anti-Malware.ru вы говорили как раз, что это понимание только началось зарождаться у руководителей бизнеса. Сейчас же вы утверждаете, что это уже тенденция. За счет чего она закрепилась?

Л. У.: Во-первых, количество атак на бизнес-структуры увеличилась не в разы, а на порядок. Во-вторых, число выявляемых случаев несанкционированного доступа к информации также возросло за счет внедрения средств защиты, которые об этом оповещают. И поскольку эта информация становится публичной, она выходит на рынок, то руководителям, которые получают такую информацию, никто не дает забыть о том, что проблема с ИБ есть или обнаружена. То есть руководитель уже не может сказать: «Я этого не знал». И когда начальник его службы безопасности говорит, что нужно провести такие-то мероприятия по ИБ, вариантов ответа становится только два: «пока нет денег на эти мероприятия» или «какие наши дальнейшие действия?»

Еще один фактор — появление новых государственных законодательных инициатив в области ИБ. Прежде всего здесь нужно отметить вступление в силу Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» 187-ФЗ, выход комплекса документов, связанных с подключением к ГосСОПКА, появление новых регулятивных документов со стороны ЦБ и многое другое. Всё это приводит к тому, что появляются новые требования к защите информации.

Есть и негативные факторы, влияющие на рынок. Вижу совершенно отчетливо отрицательную тенденцию в том, что очень многие сферы деятельности отдаются единственному исполнителю работ без должного на то обоснования. И что такие исполнители получают львиную долю государственных инвестиций на якобы развитие средств ИБ для цифровой экономики. В частности, сейчас на базе Сбербанка формируется Центр компетенций по ИБ в рамках программы цифровой экономики. А я всё же за то, чтобы Сбербанк занимался финансовой деятельностью, привлекал инвестиции и сам вкладывал средства в развитие российской экономики. И против того, чтобы, совершенно не имея никаких преимуществ перед компаниями, которые работают на этом рынке по 20-25 лет, они позиционировали себя как Центр компетенций.

Какие сейчас главные тренды на рынке?

Л. У.: На мой взгляд, основной тренд сегодня на рынке ИТ и ИБ — это появление серьезнейших разработок российских компаний в области вычисленной техники: российских компьютеров на отечественных процессорах «Эльбрус», персональных компьютеров и серверов на процессорах Т1 линейки «Байкал». Появились яркие и перспективные разработки в области мобильных устройств и VDI молодых и дерзких коллективов, не признающих зарубежных авторитетов, например, компании GetMobit. И, конечно же, сильно развились российские разработки в области ИБ. В частности, компания «Код Безопасности», которая входит в группу компаний «Информзащита», усилила свои позиции на рынке не потому, что пропали конкуренты из числа западных, попавших под санкции, а потому что качество их продукции достигло того же уровня, что и у импортных.

Что в ближайших планах по развитию у компании «Информзащита»?
Л. У.: Мы постоянно мониторим рынок и смотрим, какие появляются новые направления, требующие использования средств ИБ и тех технологий и услуг, которые мы продвигаем. При выявлении таких направлений мы формируем их в Центры компетенций. Например, наш относительно молодой Центр промышленной безопасности на сегодняшний день очень плотно работает по всем направлениям, связанным с информационной безопасностью предприятий оборонно-промышленного комплекса.

Следующие направления — это SOC, реализация 187-го закона о КИИ и ГосСОПКА. Для проработки этих трех тем мы создали единый Центр обнаружения, предупреждения и ликвидации последствий компьютерных атак. Это важнейшее направление для нас сегодня, потому что, не понимая, откуда придет угроза, не понимая, как она может распространяться, не ведя соответствующую аналитическую работу, мы не сможем правильно выстраивать свои проекты. А мы хотим, чтобы наши компетенции и разработки были на высочайшем уровне, а наши заказчики — всегда уверены в том, что для их проектов будут применены лучшие практики.

А можете привести пример достижений в этих направлениях?

Л. У.: Нас начинают воспринимать как компанию, которая разбирается в промышленной безопасности. Не так давно мы были в одной крупной добывающей компании, где по итогу двухчасового плодотворного диалога вице-президент по ИТ сказал, что хочет с нами поработать, так как видно, что мы разбираемся в теме КИИ. Хотя до этого он выгнал из кабинета несколько компаний, которые тоже утверждали, что готовы что-то сделать по КИИ, но на его взгляд совсем не понимали, о чем говорят. Аргументом в пользу нас стали наши технологические и методические наработки и наличие у нас штата людей, которые абсолютно четко представляют себе последовательность действий в процессе проведения процедуры защиты КИИ. В результате сейчас мы согласовываем задачи и проекты, для которых планируется привлечение нашей компании.

Для ПАО «Магнитогорский металлургический комбинат» мы, совместно с компанией КРОК, проводим категорирование объектов КИИ и обследование доменного цеха металлургической компании. Проект перспективный и трудоемкий, связанный, в том числе с изучением внутренних технологических процессов комбината. Работа требует знаний в области металлургии и АСУ ТП и серьезного погружения в специфику предприятия. Высокие компетенции наших специалистов и наличие профильных экспертов по теме помогают нашему эффективному взаимодействию и работе на результат.

Вы не рассказали о других Центрах вашей компании — Центрах противодействия мошенничеству и разработки программного обеспечения. Какие там есть тенденции и изменения?

Л. У.: Мы развиваем комплексные проекты: в рамках того же закона о КИИ проекты начинаются с аудита безопасности и заканчиваются реализацией всех мероприятий, связанных с защитой. В том числе и созданием информационной структуры с функцией противодействия мошенничеству.

Что касается Центра разработки ПО, то он у нас ориентирован на перспективу. Это внутренняя структура, которая работает над реализацией разработок под нужны нашей компании. Кроме того, этот Центр занимается разработкой новых продуктов, кастомизацией решений, которые мы внедряем у клиентов. В целом направление выделено в обособленное для повышения нашей конкурентоспособности.

Расскажите чуть подробнее про услуги, оказываемые Вашей компанией. Как они трансформировались за последнее время?

Л. У.: Главный тренд **—** органическое соединение ИТ- и ИБ-инфраструктур. То есть сегодня сделать четкую границу между «это задача ИТ, а это задача ИБ» невозможно, потому как многие функции очень сильно пересекаются. Например, возьмем те же самые SIEM. Какая разница, что мониторить: работоспособность инфраструктуры, если мы их настроим на эту функциональность, или работоспособность и событие безопасности? Поэтому, когда происходит взаимопроникновение информационных технологий и технологий ИБ, трансформируются и наши услуги.

Мы сегодня предлагаем не просто услуги ИБ, но поддержку и защиту бизнеса и бизнес-процессов от влияния внешних угроз безопасности. Если эти внешние угрозы достаточно обширны, то потребуется перестраивать в том числе информационно-техническую инфраструктуру заказчика, то есть сами информационные системы, проводить переконфигурацию, либо даже серьезную модернизацию ИТ-инфраструктуры. Мы предлагаем объединять мониторинг состояния ИТ- и ИБ-инфраструктур и на этой основе проводить сервисное обслуживание всех систем, которые находятся у пользователя.
У нас есть Сервисный центр, который работает 24/7 и в котором у нас есть более 60 стендов, предназначенных для моделирования любых ситуаций, которые могут произойти у наших клиентов. Если говорить о трансформации работы данного подразделения, то стоит отметить, что мы отходим от просто технической поддержки каких-то средств и систем защиты к их полному аутсорсингу. Сегодня немногие компании, особенно из сегмента малого и среднего бизнеса, готовы создавать у себя внутреннюю службу ИБ и содержать штат специалистов, а также осуществлять своими силами постоянный мониторинг состояния всех ИБ-систем. Поэтому они обращаются к нам. На сегодняшний день мы провели подготовку наших специалистов и выстроили бизнес-процессы Сервисного центра таким образом, что время реакции на событие безопасности составляло не более 20 минут. Назначение инженера, который разбирается в проблеме и будет ее устранять, происходит в течение получаса, а среднее время решения проблем, не требующих выезда специалиста на объект заказчика, — от 3 до 5 часов.

Через какие трудности пришлось пройти вашей компании в 2018 году?

Л. У.: Главные заказчики в нашей стране в области ИТ и ИБ — государство и компании с государственным участием. Поскольку развитие государственных систем идет по четко выстроенным планам и регулируется соответствующими федеральными органами исполнительной власти, то здесь мы очень зависим от скорости принятия тех или иных решений и законов.

Так, в этом году прошли выборы президента и вместе с ними — переконфигурация нашего правительства. В результате чего с февраля по июль шла перестройка структур федеральных органов исполнительной власти. Никакие конкурсы в этот период в части ИБ практически не проводились. А вот с конца лета началось движение, но времени на реализацию проектов осталось крайне мало. Финансовая дисциплина требует от всех получателей бюджетных денег закрыть проекты текущим годом, а мы же, в свою очередь, не может подписаться под тем, что реализация комплексного проекта по защите, например, государственной информационной системы займет один месяц. Это, на мой взгляд, основная причина, которая вызвала сложности с работой интеграторов на рынке ИБ и ИТ в текущем году.

Для уравновешивания нагрузки по проектам в течение года мы переориентировали часть наших подразделений на работу с сектором малого и среднего бизнеса и стали брать больше контрактов с меньшей стоимостью, но с более коротким сроком выполнения. Пусть они не всегда такие интересные, как большие, но они позволили нам в этом году чувствовать себя уверенно с точки зрения финансового планирования. Мы с оптимизмом смотрим в будущее, поскольку за этот год мы наработали хорошую практику, позволяющую нам диверсифицировать бизнес и в дальнейшем.

В каких направлениях компания «Информзащита» уже вышла вперед, а в каких хочется усилиться?

Л. У.: Мы традиционно лидеры в области ИБ, но при необходимости изучаем и разные ИТ-решения, чтобы проводить конвергенцию в этом плане. Однако существует множество проектов, связанных конкретно с развитием ИТ, где ИБ только одна из составляющих проекта. В таких больших проектах мы готовы взаимодействовать с крупными интеграторами в области ИТ. В том числе, с государственными корпорациями и созданными в их составе собственными ИТ-компаниями. Мы активно работаем с Ростехом, Роскосмосом и Росатомом. Поэтому здесь мы готовы идти в фарватере крупных разработчиков ИТ-проектов и помогать им решать вопросы по информационной безопасности.

Известно, что компания «Информзащита» сейчас находится в стадии трансформации. Что изменилось?

Л. У.: Мы сейчас наводим порядок во внутренних бизнес-процессах, чтобы максимально соответствовать динамике рынка. Взять хотя бы годами выстроенный процесс участия в конкурсах, подготовки документации, коммерческих предложений, расчетов и спецификаций и т. п. Эта работа была выстроена много лет назад, но сегодня качество выполнения этих процедур нас уже не устраивает, и мы принимаем ряд мер, чтобы выполнять эти задачи в два раза быстрее. Раньше, чтобы создать спецификацию под конкретный конкурс, мы обсуждали предварительную спецификацию с вендором, договаривались о ценах и сроках поставки и после этого направляли коммерческое предложение заказчику. Сегодня же нам нужно быть очень оперативными, так как сроки проведения конкурсов сокращаются. И если раньше нам давалось 5-6 дней, то теперь нам на подготовку коммерческих предложений могут дать 2-3 дня. Мы не можем себе позволить несколько раз встречаться с поставщиком того или иного решения, поэтому мы по каждой конфигурации проводим предварительные переговоры и нарабатываем нашу внутреннюю базу знаний, которую постоянно актуализируем и затем используем для ускорения данного процесса.

Получается, что вы делаете большую ставку на сотрудников. Как в «Информзащите» удерживают ценных специалистов?

Л. У.: Чем привлекательна «Информзащита» на сегодняшний день для людей? Прежде всего тем, что мы находимся на переднем рубеже современных технологий защиты информации, постоянно работаем с ведущими мировыми и российскими вендорами в области информационной безопасности, участвуем в большинстве форумов по данной тематике, выполняем крупные государственные проекты, предоставляем услуги по обеспечению безопасности информации крупнейшим компаниям практически во всех отраслях экономики. Мы постоянно работаем над созданием комфортных рабочих условий для наших сотрудников. На протяжении последних лет мы сформировали в офисе практически «домашний» климат: у нас нет административного давления на людей, мы стараемся создать такие условия, чтобы человеку было интересно приходить на эту работу, чтобы было вокруг как можно больше интересных проектов и людей. У каждого нашего технического эксперта есть личный план развития, который включает план по обучению новым перспективным направлениям. Таким образом, мы создаем людям среду для творческого и личностного развития.

Также в компании принято решение о создании так называемого «инкубатора» молодых специалистов. Он работает с такими вузами, как МГТУ им. Баумана, МФТИ, МИИТ, ВШЭ, и мы привлекаем студентов 4-5-х курсов на практику, а затем часть из них остается работать в компании. За этот год к нам пришло 15 стажеров, 8 из них взяли в штат. Считаю, что это высокий показатель.
Кроме того, у нас хороший соцпакет. Когда реальные доходы населения, к сожалению, падают, наличие оплаченной медицинской страховки — важный критерий для тех людей, кто смотрит чуть-чуть вперед. Услуги по нашей страховке оказывают лучшие клиники, в том числе стоматологические. По нашей страховке оплачиваются даже операции. Также есть бесплатная страховка для выезда за рубеж.

Пресса о нас

Плюс мы в целом создаем комфортные условия — переехали в комфортабельный офис, проводим яркие праздники и бесплатно обучаем. В общем, мы стараемся, чтобы нашим сотрудникам было у нас приятно работать, и взамен получаем высокую отдачу и лояльность наших специалистов.

Подробнее: http://clc.am/ZMwG0g