КОМПАНИЯ ЕДИНОМЫШЛЕННИКОВ

Ян Шмиголь

На ИТ-рынке Украины работают разные компании. Некоторые из них, пусть уступая размерами признанным лидерам, успешно конкурируют с ними. В этот раз нашим собеседником стал Сергей Маковец, директор компании ISSP, специализирующейся на ИБ.

Приближается к концу, возможно, самый тяжелый год для ИТ-бизнеса Украины в этом веке. Расскажите в целом, как он для вас складывался.

Сергей Маковец: Согласен с тем, что этот год, наверное, оказался самым тяжелым – из последних пяти лет точно. ВВП упал на 18%, и в стране много системных проблем. ИТ-бизнес, который является частью, в чем-то даже краеугольным камнем современного бизнеса – в нем ситуация вполне соответствующая. Продажи, может быть, и не совсем просели, но это в гривневом исчислении. А ведь гривна, как мы все очень хорошо помним, «упала» к доллару в три раза за последние 2 года. И это не могло не ударить по ИТ-бизнесу. Все продукты по безопасности – это в основном импорт из США, Европы и Израиля. При текущем курсе доллара это очень и очень тяжело для заказчиков. Не скажу, что все совсем плохо, но в этом году действительно пришлось бороться со многими вызовами и менять подходы.

Сергей Маковец
Директор ISSP

С какими основными препятствиями для бизнеса, особенно неожиданными, Вы столкнулись в этом году?

С.М.: Неконтролируемый рост курса доллара стал большим ударом для наших заказчиков – банков, страховых, промышленных предприятий и т.д. Все они планируют свои бюджеты в гривне, и из-за падения курса проекты либо «схлопнулись», либо заморозились, либо просто не были реализованы. Сегодня все упирается в размер бюджета у заказчиков.

Видите ли Вы какие-то положительные тенденции на ИТ-рынке Украины?

С.М.: Из положительных тенденций можно отметить то, что наконец-то прогнозируется пусть небольшой, но рост ВВП, а это означает, что запланированные на 2016 год проекты имеют больше шансов на реализацию. Важной положительной тенденцией для нас является то, что происходит гармонизация стандартов безопасности. Государственная служба специальной связи и защиты информации наконец-то обратилась к использованию стандартов криптографии, которые применяются во всем мире, вместо того чтобы заново изобретать колесо и делать его квадратным – как происходило до этого. Это позволит нашим заказчикам шире использовать международные стандарты. Также в этом году мы все заметили, как участились кибератаки на бизнес – и не где-то в мире, а именно в Украине. Подчеркну: это уже нацеленные, четко спланированные атаки на определенные компании. Задача не просто что-то взломать, а добраться до самого существенного информационного актива. Это без сомнения станет драйвером развития отрасли информационной безопасности на ближайшие два-три года.

И насколько удается защитить от угроз информационные активы?

С.М.: Это зависит от того, насколько у предприятия выстроена система информационной безопасности. У многих до сих пор не существует отдельного подразделения по ИБ. И это очень большой минус, который «аукнет-

ся», если не сегодня, то завтра. По правилам, в том числе НБУ, служба ИБ не может быть подчинена ИТ-подразделению, а должна контролировать его, подчиняясь либо собственнику бизнеса, либо руководителю компании непосредственно. У нас же есть много предприятий, где безопасность либо часть ИТ, либо ИТ-подразделение само выполняет эти функции, что в корне неверно. Это скорее проблема организационного характера, и это реально плохо, особенно потому, что руководители могут быть просто не в курсе этого. Всем известно, что в компании должны быть отделы продаж, маркетинга, ИТ. Но о том, какая информация является критичной и какой ИТ-актив надо защищать, собственники бизнеса зачастую не представляют. Поэтому важно регулярно проводить аудит, оценку рисков, и тогда уже можно будет понимать, что и от кого защищать. Но часто этого нет даже у очень крупных предприятий.

Ваша компания специализируется на ИБ. Проводите ли Вы какие-то мероприятия по образованию рынка в этом направлении?

С.М.: Мы участвуем в конференциях, связанных с ИТ и ИБ, проводим семинары, на которых пытаемся доносить правильные мысли до руководителей компаний. Также мы проводим специализированные тренинги по отдельным направлениям ИБ, по классическим подходам, по различным методикам и т. д. Но, очевидно в силу нашей ментальности, руководство многих наших компаний не считает, что надо тратить деньги на обучение. «Google-а хватит». Поэтому многие специалисты получают свои знания хаотично и несистемно. А вот в Грузии, где у нас тоже есть подразделение по тренингам, к специализированному обучению относятся на порядок серьезнее. И это правильно. От человека без соответствующего обучения и сертификации нельзя ожидать качественного результата. Каждый год мы принимаем до 10-12 студентов КПИ на практику. Желающих много, мы даже не всех можем принять. Кроме того, те студенты, которые пойдут на работу в крупные компании Украины, уже будут знать о тех или иных технологиях, решениях и с большой вероятностью придут к нам. Мы смотрим в будущее, так как бизнес «на один день» не выживает, особенно в условиях кризиса.

Мы смотрим в будущее, так как бизнес «на один день» не выживает, особенно в условиях кризиса

ISSP родилась в 2009 году, когда уже была первая волна кризиса. Некоторые спрашивали: вы что, сумасшедшие, начинать в кризис? А мы просто смотрели в будущее, запланировали определенные сценарии развития. И сегодня мы работаем в соответствии с теми ценностями, которыми руководствовались при основании компании.

Каковы эти ценности?

С.М.: Наша основная ценность – профессионализм. Мы не просто продаем какой-то продукт, занимаясь box moving. Мы предлагаем решения, позволяющие решить конкретные проблемы заказчика, и делаем нашу работу профессионально и «под ключ». Мы собрали, наверное, одну из лучших команд инженеров по ИБ, которой заслуженно гордимся. Второе – бизнес-этика. Мы не пытаемся заказчику «продать» то, что нам «нужно» продать. Мы приходим к заказчику с вопросом о том, что ему нужно, и уже на основании этого делаем свои предложения. Третье – ориентированность на клиента. Мы не оставляем его на произвол судьбы и всегда ориентируемся на сервисную поддержку, тесное взаимодействие и до, и во время, и после проекта.

Какие решения по ИБ наиболее востребованы в этом году?

С.М.: С нашей точки зрения интегратора мы видим, что из года в год растет количество проектов по защите информации от утечек – DLP. Кстати, одна из востребованных функций – «защита от дурака», ошибочных действий. В этой области работаем с системами DLP от McAfee и Raytheon-Websense.

Два года назад компания Cisco купила нишевую, но очень сильную в своей сфере компанию SourceFire, которая занимается сетевой безопасностью. Cisco очень серьезно отнеслась к этой технологии и за год внедрила ее в свои фаерволы Cisco ASA, вложив очень много денег в их продвижение. В этом году была масса проектов по внедрению этого продукта. Думаю, это тренд будет актуальным и в 2016 году, а другим вендорам, работающим в области сетевой безопасности, придется задуматься, как увеличить свой процент на рынке Украины или хотя бы сохранить.

Остальные направления, пусть не в таких масштабах, но также развиваются, в частности – направление двухфакторной аутентификации. Возможно, ситуация была бы более радужной, если бы не кризис.

Определенный тренд на сегодня и на ближайшее будущее задает указ Президента, запрещающий использование продуктов по безопасности российского производства, в связи с чем в украинских организациях идет замена, в частности, антивирусов из РФ. Касперский – хороший антивирус, но государственные предприятия будут вынуждены заменить его на продукцию других стран.

Как изменились ИТ-предпочтения украинских компаний в этом году? Работаете ли вы с госсектором и стало ли легче сейчас сотрудничать с государством?

С.М.: Особо не изменились. Как я указывал раньше – все смотрят на безопасность, но не все отдают себе отчет в том, что это надо. В госсекторе пока все плохо. За этот год я видел там такие вещи, от которых буквально «волосы вставали дыбом». Наверное, есть смысл меньше растрачивать казенные средства впустую и больше инвестировать в проекты по ИБ. Антивирусы, конечно, есть у всех, но что-то более продвинутое пока встречается только эпизодически. Этого мало – антивирусы позволяют «отловить» очень немного угроз, особенно сейчас, когда направленные атаки стали повседневностью.

Я считаю, что должна измениться доктрина на государственном уровне. Стратегия есть, а вот средств выделяется недостаточно.

В целом, с госсектором мы работаем, но немного. В основном наши клиенты – коммерческие структуры. С ними работать и проще, и безопаснее, так как они всегда платят.

Кто входит в вашу партнерскую сеть?

С.М.: В настоящее время мы преимущественно работаем с 4-мя вендорами, которые закрывают практически все вопросы в области ИБ. Это Cisco, Websense, McAfee, а также Hewlett Packard Enterprise – в основном, по направлению SIEM.

Пришлось ли Вам идти на сокращения персонала в этом году, или наоборот?

С.М.: Мы гордимся тем, что в этом году никого не сократили, хотя маржинальность многих проектов упала. Каждый заказчик хочет купить что-то хорошее и подешевле – и это понятно в связи с курсом доллара. В 2016 г. мы планируем небольшое расширение.

Какие из направлений будут наиболее перспективными в ближайшие 2-3 года на рынке информационной безопасности Украины?

С.М.: Мы видим тенденцию к тому, что безопасность будет уходить в облака. Безопасность как сервис, аутсорсинговая услуга. Реальный сектор экономики лихорадит, и многие сейчас вынуждены сокращать свой персонал, а ведь задачи никто не отменял. Поэтому компаниям становится проще отдать, допустим, свои внутренние подразделения по безопасности на аутсорсинг. Мы готовимся к этому, в частности, подписали контракты с HP и McAfee. У нас это поле просто непаханое, а перспективы – огромные. Заказчик сможет каждый месяц покупать нужный ему объем услуг. Это очень удобно, так как отпадает необходимость в покупке лицензий на весь год.

Мы запустили в промышленную эксплуатацию SOC – Security Operation Center, – к которому могут подключаться любые организации и пользоваться услугами облачного ArcSight на ежемесячной основе.

Можете описать, как происходит защита из облака?

С.М.: Почти так же, как и в традиционной модели. Антивирус как стоял на вашей машине, так и будет стоять. Но вот управление уходит в облако и осуществляется через интернет. Вы сможете управлять им самостоятельно или отдать на аутсорсинг интегратору. Тогда мы будем осуществлять мониторинг и управление, присылать отчеты, сообщать, на каких хостах были проблемы и т.д. По сути, просто изменилась система лицензирования. Все вендоры четко поняли, что заказчики хотят экономить деньги.

Вы руководите относительно небольшой компанией. Как Вам удается успешно конкурировать с намного более крупными компаниями, обладающими существенными ресурсами?

С.М.: Да, мы компания небольшая, но профильная. Поэтому мы нормально конкурируем с крупными интеграторами, основываясь на том, что в области конкретных технологий у нас экспертиза лучше, чем у них. К тому же сейчас, в момент кризиса, управлять небольшой компанией намного проще. Нам даже проекты выполнять проще. У нас не бывает

такого, что менеджер по продажам что-то продал, о чем-то договорился, а консультанты об этом даже не подозревают. В крупных компаниях заказчик часто обезличен. А вот у нас заказчиков знает каждый. К тому же мы быстрее можем откликнуться на новые интересные тренды, по сравнению с крупной компанией.

Расскажите о ключевых моментах истории компании.

С.М.: Компанию создала группа единомышленников, связанных общим представлением о том, как нужно делать бизнес. Возникла идея о том, что в ближайшие годы будет активно развиваться направление ИБ, а поскольку мы почти все из КПИ и у нас хороший бэкграунд в ИТ, вот мы и решили попробовать. Наше название – ISSP – расшифровывается как Information Systems Security Partners. Вызревало оно довольно долго, но отлично отражает суть компании – особенно то, что мы единомышленники.

Существует ли идеальный заказчик?

С.М.: Наверное, да (улыбается). Идеальный заказчик не будет торговаться, понимая, что продукт стоит столько, сколько указано в прайс-листе, и что услуги поддержки и сопровождения также надо оплачивать. У идеального заказчика в штате работают квалифицированные специалисты, которые не будут донимать нашу службу поддержки десятками звонков по пустячным поводам. Идеальный заказчик доверяет нам как своему партнеру и выстраивает с нами долгие бизнес-отношения, порой перерастающие в дружбу. Неидеальный заказчик – это тот, кто хочет быстро, дешево и качественно, т. е. того, чего в природе не существует.

Какие качества, по Вашему мнению, должны быть присущи руководителю? Что Вам помогает вести бизнес?

С.М.: Сильно помогает вера в то, что мы делаем полезное и нужное дело. Помогает упрямство, нужное для того, чтобы вести за собой людей, а также, я бы сказал, «инертность», хладнокровие – когда ты не бросаешься из стороны в сторону. Нужны знания – работать без знаний в предметной области и экономике это все равно, что плыть с закрытыми глазами в реке с крокодилами. В нашем деле надо предвидеть все на несколько шагов вперед.

Надо уметь отвлекаться от работы. Мое хобби для этого – чтение, причем с детства. Предпочтения за это время, конечно, менялись. В последнее время я в основном читаю детективы, в которых много экшена. Это позволяет отвлечься, выключить мозг. Час-два – и уже все хорошо, можно возвращаться к работе (улыбается). На остальное времени практически не хватает.

Каков Ваш взгляд на сегодняшний день с точки зрения эксперта в области ИБ?

С.М.: Во-первых, у каждого человека сейчас 2-3 компьютерных устройства – ноутбук, планшет, телефон. На каждом устройстве хранится важная информация, но люди в основном не задумываются о ее защите. Во-вторых, люди слишком беспечны в отношении социальных сетей. Человек может боятся лишний раз показать паспорт, даже полицейскому, а вот сообщить всем, что он сейчас находится в каком-то кафе, показать всех своих детей, расписать, кто в какую школу ходит, – это считается нормальным. А это в корне неправильно. Нужно повышать User Awareness, связанную с безопасностью вообще и информационной безопасностью, в частности. Правильным шагом будет включить это в школьную программу, параллельно с информатикой или ОБЖ. Хочешь похвастаться, что едешь за границу, – расскажи еще раз себе или ближайшим друзьям, но не сообщай об этом всем. В-третьих, об ИБ забывают не только частные лица, но и предприятия. Есть расхожее выражение, гласящее, что все компании делятся на две группы: те, кого уже взломали, и те, кто об этом еще не узнал. А ведь потеря важной информации совершенно спокойно может вести к банкротству бизнеса.

У нас на регулярной основе происходят ситуации, когда кто-то приходит и говорит: у нас была утечка/взлом/кража – нужно внедрить систему ИБ. Для бизнеса ISSP это вроде бы очень хорошо, но как человек я подчеркиваю: к сожалению, очень часто к нам обращаются после того, как что-то произошло. На Западе менталитет немного другой, там есть стандарты, необходимость соответствовать регуляторным требованиям в области ИБ, и бизнес их соблюдает. Плюс, они более открытые. Если у западного банка произошел инцидент, он обязан опубликовать об этом информацию, иначе будет серьезно оштрафован государством. У нас же все по-другому, поэтому об утечках мы обычно просто не знаем. В свете всего этого на Западе тратится намного больше средств на ИБ – опять же, внимание хакеров к тамошним финансовым организациям более пристальное. Мы к этому, пусть позже, но придем – уже сейчас многие украинские банки испытывают серьезнейшее давление со стороны киберпреступников. C4IT