информационные технологии

Постсноуденовская безопасность

Сегмент информационной безопасности — один из немногих оставшихся на ИТ-рынке, который продолжает показывать рост. Киберпреступность эволюционирует, вместе с ней приходится развивать и технологии защиты, менять подходы к информационной безопасности бизнеса, подстраиваться под новые угрозы и, главное, переходить от «бумажной» безопасности к реальным превентивным стратегиям защиты.

— сегмент рынка —

По оценкам Gartner, бизнес во всем мире потратил на информационную безопасность (ИБ) в 2015 году $75 млрд, что на 4,7% больше, чем годом ранее. В то же время мировой ИТ-рынок снизился на 5,8%. В РФ ситуация выглядит похоже, если учесть разницу в объемах и курсах валют. На фоне падения всего рынка информационно-коммуникационных технологий (ИКТ) сектор информационной безопасности можно назвать одним из самых перспективных. В марте аналитики IDC пересмотрели прогноз на 2016 год по рынку ИКТ в целом, заявив, что его падение составит порядка 13%, тогда как ранее ожидалось незначительное сокращение его объемов. На прошедшей в сентябре конференции по информационной безопасности IDC IT Security Roadshow 2016 старший аналитик IDC по направлению ИБ Денис Масленников сообщил, что в первом полугодии 2016 года рынок аппаратных решений для обеспечения ИБ вырос в долларах на 26,8% по сравнению с первым полугодием 2015 года и составил $68 млн. По его мнению, положительная тенденция сохранится. «Первая половина 2016 года показала, что спрос на решения для обеспечения информационной безопасности снова растет, ведь защита критически важных данных является крайне важной для большинства компаний любого размера»,— отметил Денис Масленников.

Евгений Дружинин, ведущий эксперт направления ИБ компании КРОК, описывает международный контекст: «Российский рынок ИБ показывает довольно стабильный рост в рублях, но, к сожалению, в пересчете на доллары динамика пока отрицательная. Виной тому нынешний курс валют, который повлиял на всю отечественную отрасль ИТ. Тем не менее на локальном рынке все довольно позитивно — например, по итогам 2015 года выручка по направлению информационной безопасности КРОК выросла почти на 20% в рублях».

Андрей Янкин, руководитель отдела консалтинга Центра информационной безопасности компании «Инфосистемы Джет», говорит, что в целом тенденции на рынке ИБ в России те же, что и на мировом, хотя и существует задержка в один-два года, но она уменьшилась: раньше мы отставали на четыре-пять лет. По его словам, общие для всего мира проблемы — целенаправленные атаки, защита веб-ресурсов, в том числе от DDoS-атак. «В России можно выделить также тенденции замены систем ИБ в рамках импортозамещения, но их уже нельзя считать уникальными, так как в постсноуденовскую эпоху многие государства задумались об этом»,— добавляет господин Янкин. Кирилл Керценбаум также видит рост интереса к отечественным решениям в сфере ИБ на волне импортозамещения. Регулятор продолжает воздействовать на рынок ИТ и через него на сегмент ИБ также путем обновления российского законодательства. Так, «закон Яровой» может повлиять на рынок строительства новых дата-центров, объем поставок систем хранения данных и другого оборудования, а также повлечь рост спроса на решения в области сетевой безопасности, включая межсетевые экраны, анти-DDoS системы и пр.

Как говорит Дмитрий Огородников, директор Центра компетенций по информационной безопасности компании «Техносерв», именно в сильном регулировании заключается принципиальное отличие российского рынка от общемирового. «Технологически это выражается в использовании некоторых уникальных решений, как-то средств АПМДЗ (аппаратный модуль доверенной загрузки.— **„Ъ“**) или отечественных криптоалгоритмов ГОСТ 28147-89 и последующего ГОСТ Р 34.12-2015. Законодательно это выражается в большом объеме различных руководящих документов в области защиты информации, которые по последним планам Федеральной службы по техническому и экспортному контролю (ФСТЭК) должны обновляться каждые три-четыре года,— объясняет он.— С другой стороны, наш рынок ИБ менее зрелый и многие процессы или технологии, которые на западном рынке уже широко используются, на нашем только делают первые шаги. Например, в этом году мы стали активного говорить о подходе Agile, о процессах ИБ и о решениях класса User and Entities Behavior Analysis (технологии анализа поведения пользователей и процессов в корпоративных системах на основе искусственного интеллекта.— **„Ъ“**)».

«Бумажная» безопасность подорожала

Еще одна из отличительных особенностей российского рынка ИБ, по словам господина Дружинина,— существенный рост средней стоимости ущерба от инцидентов. Так, в 2015 году по данным IDC она выросла почти в полтора раза, в то время как на мировой арене этот показатель уменьшился на 5%. Это заставляет бизнес более тщательно работать над стратегиями защиты, привлекать внешних специалистов. Соответственно, серьезный рост показывает сектор услуг в области ИБ. Господин Янкин комментирует: «Если с „железом“ у нас все более ил менее неплохо, то в области выстраивания процессов ИБ и встраивания их в бизнес наблюдается явное отставание. Консалтинг в области ИБ в коммерческом секторе показывает хороший рост, но во многом это эффект низкой базы. Интересная тенденция на рынке ИБ, к которой скептически относились многие эксперты еще три-четыре года назад,— это существенный рост рынка аутсорсинга, как качественный, так и количественный. В целом рынок ИБ в России бурно развивается даже в условиях экономического спада».

Евгений Дружинин также видит тенденцию по смещению акцентов в сторону услуг, включая аутсорсинг ИБ и облачные сервисы типа Security as a Service (SECaaS). «Заказчики все активнее ищут помощи внешних подрядчиков в вопросах выстраивания контура безопасности. Например, спрос на облачные сервисы растет, а вместе с этим формализуются и требования к их безопасности. Например, услугу Security as a Service крайне желательно выстраивать на базе сертифицированных ФСТЭК и ФСБ средств. Как раз таким сервисом мы сейчас защищаем ряд IaaS-сервисов, арендуемых в нашем публичном облаке автомобильной компанией. Защита реализуется в соответствии с индивидуальной моделью угроз заказчика и с учетом требований 152-ФЗ»,— говорит он.

Из-за тог, что последствия киберугроз становятся все более разрушительными, бизнес стал более внимательно относиться к защите. Господин Янкин говорит, что от формального выполнения требований регуляторов и отношения к ИБ как к некоторой экзотике бизнес перешел к восприятию рисков ИБ как к будничной и неотъемлемой части использования ИТ-технологий. «Конечно, в этой области все еще сохраняется правило о том, что пока гром не грянет, мужик не перекрестится, но гром стал греметь так часто и так у многих над головами, что большинство зрелых компаний перешли к плановому обеспечению ИБ, а не латанию дыр после инцидентов. Это приводит к росту роли ИБ в компаниях, выведению подразделений ИБ из-под ИТ или СБ в отдельные независимые структуры с мощными контрольными функциями, собственными бюджетами, дифференциацией персонала»,— говорит он.

Кирилл Керценбаум, менеджер по развитию бизнеса «Лаборатории Касперского», добавляет, что в связи с сокращением или оптимизацией бюджетов на ИБ российские компании стали уделять внимание более интенсивному использованию уже внедренных средств защиты, а не массовой закупке новых. В связи с этим и наблюдается рост спроса на сервисы Security & Threat Intelligence (интеллектуальные услуги по предотвращению угроз), которые позволяют повысить эффективность процессов ИБ за счет более качественной организации процессов мониторинга защищенности инфраструктуры. А также растет спрос на аудит безопасности, тесты на проникновение, данные по актуальным угрозам и услуги SECaaS, которые позволяют оптимизировать расходы на ИБ за счет аутсорсинга крупных инфраструктурных решений на сторону сервис-провайдера. Из этой категории услуги по защите от DDoS-атак — антивирусные решения по подписке, защита от взлома и т. д.

Михал Салат, ведущий вирусный аналитик Avast Software, добавляет: «Простого антивируса уже недостаточно для обеспечения корпоративной информационной безопасности, нужно использовать несколько уровней защиты, включая антивирус, межсетевой экран, системы обнаружения взломов, регулярное обновление аппаратного и программного обеспечения и надлежащее использование прав доступа сотрудниками. Важно помнить про человеческий фактор. Люди совершают ошибки, и хакеры знают, как их использовать. Поэтому важно, что организации осуществляют новую политику, например устанавливая ограничения на использование документов внутри компании для предотвращения фишинговых атак. Тестовые взломы — это отличный способ узнать слабые места, которые хакеры потенциально могут использовать. Тестирования на проникновение в идеале нужно делать несколько раз в год, так как хакеры постоянно ищут и находят новые способы взлома».

Бизнес реагирует на нарастающие угрозы — с существенным отставанием от развитых стран в России появился интерес к системам автоматического предотвращения мошенничества в ИТ-системах. Как говорят эксперты, сейчас в этой области настоящий бум.

Антон Карданов, руководитель сектора ИБ компании AT Consulting, говорит, что целью злоумышленников сегодня часто являются веб-приложения, которые обладают достаточным количеством уязвимостей, позволяющих реализовать такие атаки, как межсайтовый скриптинг (XSS), SQL-инъекции, уязвимости конкретных плагинов. Господин Карданов рекомендует: «Чтобы минимизировать ущерб бизнеса при построении превентивной системы информационной безопасности, развивающейся параллельно с инфраструктурой и технологиями, необходимо заранее быть готовым к предотвращению наиболее вероятных атак и уходить от убежденности, что какой-то конкретный ресурс полностью защищен. Создайте центр мониторинга и реагирования на инциденты информационной безопасности: подразделения, имеющие возможность в режиме реального времени отслеживать защищенность ресурсов и принимать адекватные и соответствующие текущей ситуации меры. Проведите инструментальный аудит практической защищенности ресурсов, он выявит наиболее уязвимые места и сформирует предположение о вероятных атаках. Таким образом, у вас будет заранее спланированный план действий, следуя которому вы сможете быстро восстановить работоспособность системы в случае взлома».

Андрей Бершадский, директор центра компетенции компании Positive Technologies, также подтверждает, что безопасность приложений — одна из главных проблем заказчиков в РФ в текущем году. За год продажи продукта Web Application Firewall компании в России дали выручку, которая вдвое превышает продажи экранов прикладного уровня за все предыдущие годы.

Также он отмечает, что за последний год стало активнее происходить строительство центров мониторинга и управления информационной безопасностью (SOC). «Именно центры мониторинга начали мирить два противоборствующих лагеря: так называемых бумажных безопасников и ИБ-практиков. Ведь SOC — это люди, регламенты и технические средства. И без правильно выстроенных процессов реализовать практическую составляющую мониторинга и реагирования вряд ли представится возможным. Интерес к SOC подтолкнул интерес к SIEM-решениям (Security information and event management — управление информационной безопасностью и событиями ИБ.— **„Ъ“**). Многие сильно удивились, что, оказывается, однажды купленный и даже внедренный SIEM на практике не всегда способен решать те задачи, которые стоят перед специалистами SOC. В первую очередь ввиду неспособности оперативно подстраиваться под динамичную инфраструктуру и отсутствия серьезной встроенной экспертизы. Рынок SIEM в России фактически переживает вторую молодость, и вряд ли стоит ожидать его спада, ведь потребности заказчиков давно уже выходят за рамки классического решения SIEM»,— рассказывает он.

В сфере защиты государственных учреждений господин Бершадский видит прогресс: «Сразу несколько ведомств начали создание первых центров ГосСОПКА (Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак.— **„Ъ“**), что должно крайне положительно сказаться на безопасности государственных учреждений и подтолкнет других участников рынка присоединиться к программе».

Мария Анастасьева

«Работаем над тем, чтобы изменить восприятие ИБ в сознании людей»

— отраслевой опыт —

Сеть магазинов бытовой техники, электроники и товаров для дома «Эльдорадо» активно развивает бизнес в интернете. Это сопряжено с рисками для информационной безопасности (ИБ). ФЕДОР КУРНОСОВ, менеджер по ИБ «Эльдорадо», рассказывает, как формируется стратегия компании в этой сфере.

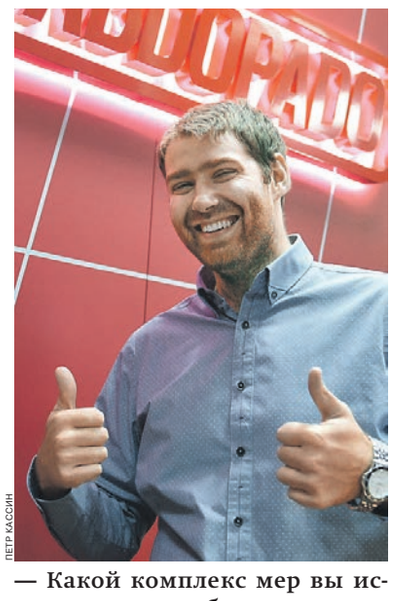
— Часто компании начинают думать о том, что нужно использовать какие-то средства защиты, только в тот момент, когда проблема уже возникла. Как у вас это происходит?

— Стараемся рассматривать возможные проблемы ИБ превентивно: когда интернет-магазин был в самом начале развития и в это развитие вкладывались серьезные средства, необходимо было позаботиться о защите инвестиций. Мы хотели быть уверены, что интернет-магазин будет доступен 24 часа в сутки 7 дней в неделю. В этом нам помогает то, что мы приверженцы рисковой модели: просчитываем риски в деньгах и именно эти цифры доносим до менеджмента компании, когда закладываем бюджет на ИБ. Руководство понимает язык денег. Если дать им возможность взвесить на одной чаше весов потенциальные потери от реализованной угрозы, а на второй — стоимость защиты, то возникает отчетливое понимание оправданности этих вложений.

— Насколько важен интернет-магазин для бизнеса компании?

— Трафик на сайте постоянно растет. Мы делаем ставку на онлайн, потому что все меньше людей готово идти в магазин и что-то там покупать. Особенно это касается крупных городов, жители которых хотят получать все, не вставая с дивана. Интернет-магазин, по сути,— это «лицо» компании, которое должно быть аккуратным и дружелюбным.

Оффлайновые магазины также перестраиваются. Мы не считаем, что они полностью умрут. Меняется формат, люди приходят туда уже больше для развлечения, чтобы изучить какие-то новинки. Им интересна уже не только техника, но и другие категории товаров.


ПЕТР КАССИН

— Какой комплекс мер вы используете для обеспечения доступности?

— Обеспечивая доступность, решаем две задачи: отказоустойчивость и катастрофоустойчивость. Для решения первой используются средства распределения нагрузки внутри ЦОДа (центр обработки данных). Для решения второй в зависимости от стратегии обеспечения катастрофоустойчивости дублируем бизнес-процессы и поддерживающую их ИТ-инфраструктуру в двух географически распределенных ЦОДах.

— Какие угрозы вы учитываете?

— Учитываем как внешние, так и внутренние угрозы. Для защиты от DDoS-атак используем внешний облачный сервис. Проводим регулярный анализ имеющихся уязвимостей, которые могут эксплуатироваться злоумышленниками как извне, так и изнутри. В частности, осуществляем аудит на нарушение бизнес-логики — это когда атаку можно устроить, используя стандартный функционал, в котором не все риски учтены.

— Многие компании, как правило, испытывают сложности с тем, чтобы пересчитать риски в возможные денежные потери. С доступностью понятно: можно вычислить оборот интернет-магазина за определенный период. А как обращаться с другими рисками?

— Думаю, сложности возникают у специалистов, которые еще не поняли, как построить разговор с бизнесом, как объяснить менеджменту, что такое доступность, конфиденциальность, целостность и почему это важно. Потери от проблем с доступностью ресурса действительно весьма просто оценить в деньгах: либо бизнес работает, либо нет. Но как оценить потери от нарушения конфиденциальности? Со временем пришло понимание и по этому вопросу. Наш отдел маркетинга заранее просчитывает ожидаемый эффект от акции: насколько она будет выгодна, сколько денег принесет. Если конфиденциальность нарушена, о планах узнал широкий круг лиц (включая конкурентов), акция уже не принесет ожидаемых доходов. Разница между запланированным объемом выручки по акции и тем, что получилось по факту из-за нарушения конфиденциальности,— это и есть риск, выраженный в деньгах.

Этот же принцип мы пытаемся перенести и на другие отделы: просчитываем, как может повлиять разглашение определенной информации на взаимодействие с вендорами, партнерами, поставщиками. По многим подразделениям у нас уже есть ясная картина.

С целостностью тоже научились работать. Есть понимание, что определенные данные не должны измениться, пока они проходят через бизнес-процессы. Можем посчитать, сколько компания потеряет, если это случится. К примеру, потери из-за ошибки в цене мы можем вычислить практически моментально: видим, сколько людей успели сделать предзаказ по меньшей стоимости или купить этот товар. Собираем информацию о таких инцидентах и можем оценить в итоге средние потери.

— То есть вы изучаете исторические данные по конкретным инцидентам?

— Да, мы берем реальную историю инцидентов и рассчитываем вероятность наступления тех или иных потерь на основе этих статистических данных. Плюс к этому считаем потери от каждого подобного случая и, как следствие, получаем риск, рассчитанный в деньгах. С помощью этих данных мы ведем диалог с бизнесом. Менеджеру понятны те категории потерь и рисков, с которыми он сталкивается каждый день: во сколько обойдется час простоя, какими будут потери от срыва маркетинговой акции и т. д.

— Как вы относитесь к облакам?

— «Эльдорадо» — продвинутая компания: мы используем все продукты SAP для ритейла, при этом размещаем их на облачных ресурсах. Конечно, это выделенные именно под нас облачные ресурсы — так называемое частное облако, размещенное на оборудовании подрядчика. Зачем? Нам важно, чтобы высоконагруженные системы были обеспечены поддержкой 24/7. Не всегда это можно сделать собственными силами. В этом смысле контракт с поставщиком облачных ресурсов — удобный вариант.

— Учитываете ли риски, связанные с использованием облаков при формировании стратегии ИБ?

— У нас разработана большая карта всевозможных рисков, включая те, что связаны с законодательством. В нее включены в том числе риски, связанные с облачными ресурсами. Каждый год мы проводим актуализацию этой карты, которая ориентирована на бизнес-цели компании. Мы следуем стандарту ISO 27001 от 2013 года, в котором есть целый раздел о том, что нужно рассматривать риски в соответствии с видением общего развития компании. Так что мы смотрим на то, в каком направлении развивается бизнес, включаем в карту новые риски, которые являются актуальными для этого направления развития.

— Чтобы все эти риски просчитать, вам необходима собственная статистика по инцидентам. Но как быть с новыми угрозами?

— Если появляется новая угроза, мы сразу ее учитываем, присваиваем определенную вероятность ее реализации и применяем превентивные меры защиты. Если инцидентов в течение года не происходит, выводим эту угрозу из актуальных. При этом мы стараемся использовать имеющиеся средства защиты, если же они не позволяют предотвратить реализацию новой угрозы, то, как я говорил ранее, взвешиваем на одной чаше весов потенциальные потери от реализации угрозы, а на второй — стоимость защиты. Так можем быть постоянно в тренде.

— Какие угрозы становятся более актуальными?

— Основной тип угроз, который сейчас активно обсуждается,— это таргетированные, направленные атаки (APT — advanced persistent threats). Общий тренд такой, что защита должна становиться более эшелонированной. То есть должны быть стандартный антивирус, инструменты противодействия DDoS-атакам, Web Application Firewall от взлома, средства против внутренних атак. И, конечно же, многое очень зависит от обучения людей.

В последнее время вижу очень много всяких средств защиты, которые помогают от того или иного вида угроз. Но их эффективность будет низкой, если не ликвидировать пробел в обучении людей.

Моя личная рекомендация коллегам — в первую очередь заниматься этим вопросом. «Железок» и ПО, которые много чего умеют, на рынке полно. Но людей, которые находятся внутри периметра либо с ноутбуком перемещаются за пределы компании, нужно обязательно учить информационной безопасности, тому, как противостоять определенным угрозам. Технологии усложнились, компании используют целые арсеналы средств защиты, но вопросам социальной инженерии уделяют крайне мало внимания.

Допустим, компания использует систему защиты от таргетированных атак. И трафик просматривает, и компьютеры, а также каждый запущенный сервис мониторит. Вроде бы все хорошо. Но вот пользователь решил поработать дома, берет с собой документы на флешке, приносит обратно в офис. Воткнул ее в рабочий компьютер, всего лишь считал информацию и заразил машину. Да, проблема будет обнаружена, но до того может произойти заражение сети, да все что угодно.

— Вы проводите обучение в компании?

— У нас постоянно идут образовательные программы. При приеме на работу новый сотрудник проходит первичное обучение, затем всех приглашают на дистанционные курсы. Мы создали пять-шесть видов образовательных дистанционных программ по информационной безопасности, по ним нужно сдавать зачет. Это дает большой положительный эффект. Да, все еще бывают проблемы, когда люди не действуют в соответствии с тем, что они прочитали. Но некоторые инциденты были предотвращены именно потому, что человек вспомнил, что было написано в обучающих материалах, сделал все, как нужно, чтобы проблему предотвратить. В итоге не произошло массового заражения компьютеров.

Помимо обучения важно показать людям, что требования информационной безопасности — это не палка в колеса, что бизнес и ИБ могут сосуществовать. Да, какие-то процессы могут стать чуть медленнее, потому что все-таки средства защиты нужно использовать. Да, это может как-то ограничивать бизнес. Но эти ограничения приносят дополнительную выгоду из-за того, что снижают риски. Иначе говоря, мы поворачиваемся лицом к бизнесу, бизнес лицом — к нам и происходит взаимодействие. Мы работаем над тем, чтобы изменить восприятие ИБ в сознании людей.

Много слов сказано о том, что ИБ должна быть частью корпоративной культуры. Но я все-таки исхожу из того, чтобы инструмент, который предлагается для обеспечения информационной безопасности, был удобным. Если это удобно, то не возникает мысли, как-то это ограничение обойти. Всегда есть альтернатива публичным слабозащищенным сервисам типа Dropbox и пр. Можно развернуть удобные сервисы внутри защищенного периметра, если их функциональность нужна бизнесу.

Конечно, чтобы получилось людей склонить к альтернативе, нужны сильная воля и возможности руководителя по ИБ, а также поддержка от генерального директора, чтобы не произошло первичного отторжения. Если первичное отторжение у людей удается преодолеть, то обычно они начинают сотрудничать. Ну и, конечно, специалистам по ИБ нужно не бояться влезать в процессы, пытаться почувствовать, чем живет компания. Разумеется, не сразу, но обязательно получится добиться эффективного взаимодействия на всех уровнях.

Интервью взяла Светлана Рагимова