информационные технологии

Предчувствие апокалипсиса

Из-за экономического кризиса многие компании сокращают бюджеты на информационную безопасность (ИБ), подвергая себя немалому риску. С другой стороны, сегодня хорошо продаются решения, позволяющие сэкономить на ИБ, не теряя в качестве защиты. Но грядущее развитие интернета вещей и распространение протокола IPv6 несет новые угрозы, к которым индустрия ИБ не готова.

— сегмент рынка —

Рынок информационной безопасности сильно сегментирован, поэтому развивается неравномерно. По словам заместителя генерального директора компании InfoWatch Рустэма Хайретдинова, сейчас на рынке информационной безопасности общий спад, связанный с непростой экономической ситуацией. «Продуктовые линейки, которые напрямую зависят от размеров защищаемой инфраструктуры, например антивирусы, переживают спад, поскольку количество компьютеров, которые надо защищать, не растет»,— замечает эксперт. Борьба со спамом в последнее время уже не является ни мировым, ни российским трендом. Доля спама в почтовом трафике в прошлом году значительно упала — в частности, по данным компании Symantec, она приблизилась к показателям 2003 года.

Александр Лямин, основатель и CEO компании Qrator Labs, специализирующейся на противодействии DDoS-атакам, соглашается, что рынок ИБ напрямую зависит от состояния экономики. «Конечно, у многих владельцев и управленцев компаний в этой ситуации возникает желание экономить на всем, что не имеет отношения к прямой коммерческой деятельности, в том числе на безопасности. Бюджеты на ИБ сокращаются, что не может не привести к росту числа успешных атак. Банковская сфера яркий тому пример»,— говорит он. Руководитель отдела расследований компании Group-IB Дмитрий Волков рассказывает, что преступная группа Anunak, которая атаковала 50 банков и 5 платежных систем, нанесла ущерб около 1 млрд руб. «Позже у них появились последователи — группа Buhtrap, которая похитила у 13 банков уже 1,8 млрд руб. Группа Corkow атаковала брокера „Энергобанк“ и от его имени начала совершать валютные операции на бирже. В результате атакующие добились аномальной волатильности, что позволило покупать доллар за 55 руб., а продавать— за 62 руб.»,— перечисляет Дмитрий Волков. «Если у вас есть деньги и вы их не защищаете, то у вас их заберут»,— резюмирует Александр Лямин.

Однако в отдельных направлениях рынка ИБ эксперты отмечают устойчивый рост. Иван Новиков, глава Wallarm, выделяет один из таких сегментов — защиту от ботов: «Задача определения нечеловека очень остро стоит в таких областях бизнеса, как электронная коммерция, платежи, платные информационные услуги. Решить такую задачу в общем виде невозможно без изучения бизнес-логики веб-приложений. Современные решения могут делать это автоматически, менее продвинутые требуют ручной настройки».

Рустэм Хайретдинов отмечает рост популярности корпоративных мобильных и веб-приложений во время кризиса: стоимость трансакции в сети дешевле, и большинство B2C-компаний (торговых компаний, телекомов, агентств недвижимости, банков и даже государственных организаций) переводят клиентов на обслуживание в личные кабинеты, сокращая количество офисов. «Поэтому растет и спрос на защиту интернет-приложений от хакерских и DDoS-атак. Также растет сегмент систем информационной безопасности, которые защищают ключевые активы компании и помогают экономить деньги: системы противодействия мошенничеству (anti-fraud), системы противодействия утечкам информации (DLP)»,— объясняет Рустэм Хайретдинов. Его слова подтверждает Александр Лямин: «В 2014 году мы выросли на 120%, в прошлом — на 80%, хотя и ожидали, что вырастем на 160% — экономический кризис дает о себе знать». Андрей Заикин, руководитель направления ИБ компании КРОК считает, что DDoS-атаки нередко используются для того, чтобы отвлечь внимание от ключевой задачи злоумышленника.

В системном интеграторе КРОК выручка по направлению информационной безопасности тоже выросла — более чем на 22%. «Официальных данных аналитических агентств по рынку мы пока не видели, складывается ощущение, что он вырос в национальной валюте. Это обусловлено тем, что количество и актуальность угроз информационной безопасности растут во всем мире. Непростая экономическая ситуация в России этот тренд только поддерживает и усиливает»,— отмечает Андрей Заикин.

По мнению Алексея Гришина, директора Центра информационной безопасности компании «Инфосистемы Джет», среди направлений ИБ, растущих в результате импортозамещения, существенно выделяется разработка новых российских продуктов.

Сергей Карпов, генеральный директор «ЕМС Россия и СНГ», также отмечает, что за последний год был анонсирован ряд продуктов по ИБ отечественного производства, но не все они однозначны. «В некоторых случаях это анонсы от известных российских компаний, хорошо зарекомендовавших себя на рынке ИБ, но некоторые решения были созданы в ускоренном режиме компаниями, которые только пришли на рынок информационной безопасности. Это привело к тому, что часть решений оказалась закуплена заказчиками еще в стадии разработки под гарантии разработчиков о бесплатной модернизации до „промышленной“ версии, когда она будет готова»,— рассказывает господин Карпов. Такие «суррогатные» решения приводят к снижению общего уровня ИБ в компаниях, что негативно сказывается на общем уровне доверия к ИБ в целом.

«Также на волне развития интернет-бизнеса значительно вырос спрос на решения по обеспечению безопасности вэб-сервисов. Для многих компаний, в особенности банковского сектора, стали актуальны задачи по выстраиванию процессов вокруг ранее внедренных средств безопасности. Связано это с тем, что выстраивание таких процессов позволяет без серьезных инвестиций существенно повысить уровень защищенности»,— объясняет Алексей Гришин. По его словам, наметилось активное движение в сторону облачных технологий — от обновления баз угроз и уязвимостей до предоставления облачных сервисов безопасности. Юрий Маслов, руководитель направления «Информационная безопасность» компании «АйТи», добавляет, что уже несколько лет растет и в ближайшее время не прекратится спрос сопровождение ИБ-инфраструктуры клиентов.

Сегодня во всем мире в топ-3 ключевых направлений развития рынка ИБ входят сетевая безопасность, облачная безопасность и аналитика безопасности, утверждает Алексей Лукацкий, бизнес-консультант по безопасности Cisco Systems. «Это объясняется достаточно просто: как бы ни была построена система предприятия, все общаются по сети, и туда же направлены и действия хакеров. Поэтому рынок сетевой безопасности находится на первом месте уже многие годы. Лидерство облачной ИБ тоже объясняется просто: в условиях размытого периметра, нехватки средств на закупку «железа» желание отдать непрофильные сервисы вовне облака являются тем, что позволяет все это реализовать»,— говорит Алексей Лукацкий. Замыкают десятку управление угрозами, анализ угроз и хакерских кампаний, защита конечных устройств, управление рисками и решения GRC (Governance, Risk and Compliance), а также безопасность мобильных устройств и управление инцидентами.

Из трех классических драйверов развития ИБ в мире и России — страх, законодательство, экономика — второй сейчас является одним из основных, говорит Алексей Лукацкий. «В России 16 регуляторов по информационной безопасности, которые за последние 4 года выпустили нормативных документов больше, чем за предыдущие 25 лет. И это не только традиционные регуляторы — ФСТЭК, ФСБ, Банк России, Минобороны, но и новые, занявшиеся данной темой относительно недавно,— Роскомнадзор, Минкомсвязь, Минэкономики и т. д. Зачастую новые обязательные требования регуляторов заставляют компании бизнеса хоть что-то делать в области безопасности. К сожалению, строгость законов у нас компенсируется необязательностью их исполнения, слабой правоприменительной практикой и низкой квалификацией проверяющих. Все это часто приводит к тому, что заказчики выполняют требования поверхностно либо игнорируют их, рассчитывая на невнимательность и забывчивость регулирующих органов»,— сетует господин Лукацкий. Тем не менее, по мнению Александра Гришина, влияние регулятора на рынок ИБ сегодня снизилось по сравнению с прошлыми годами: заказчики перестали осуществлять проекты лишь ради соответствия требованиям. «Сами регуляторы начали создавать центры по противодействию киберугрозам, например FinCert и ГосСОПКА, целью которых является предоставление сервисов для организаций разных отраслей. Создается правовая база, позволяющая обеспечить противодействие киберпреступности. И все это положительно сказывается на рынке»,— уверен Александр Гришин.

Скрытая угроза

Если ознакомиться с публикациями и выступлениями экспертов на тему главных угроз в области ИБ за последние 10 и даже 15 лет, то становится ясно, что одна угроза остается неизменной — человеческий фактор. Алексей Лукацкий называет две основные угрозы — это невысокая компетенция пользователей и низкое качество программного обеспечения. «Именно они приводят к тому, что злоумышленники могут осуществлять хитрые и не очень атаки на разные отрасли и объекты. Например, именно по этим двум причинам клиенты банков страдают от хищения средств: они не умеют распознавать действия мошенников и хакеров, а разработчики банковского ПО сами не до конца понимают, как создавать безопасный софт»,— утверждает Алексей Лукацкий. А вот Андрей Заикин уверен, что больше половины инцидентов происходит по вине обычных пользователей. В некоторых случаях по незнанию, в других — по предварительному сговору с мошенниками, что наиболее часто происходит в банковской сфере.

Александр Гришин считает, что важность человеческого фактора как одной из основных угроз стремительно растет. «Темпы развития таких технологий, как мобильные устройства, вэб-сервисы (интернет-торговля и интернет-банки), интернет вещей, значительно опережают развитие средств защиты. А следом за технологиями развивается киберпреступность. Для противодействия угрозам необходимо в первую очередь повышать осведомленность пользователей»,— предупреждает Александр Гришин.

На уровне государства имеются и другие угрозы — иностранные спецслужбы и кибертеррористы, которые уже угрожают его безопасности, либо будут это делать в самом ближайшем будущем, уверен Алексей Лукацкий.

Александр Лямин утверждает, что количество DDoS-атак в России растет на 50% ежегодно — темпами, вдвое превышающими мировые. «Когда DDoS-атаки только появились, основная точка их нейтрализации располагалась на территории заказчика — в его датацентре и на его оборудовании. Но потом даже крупный enterprise перестал справляться с DDoS-атаками. И в 2010 году точка решения проблемы переместилась к операторам связи. Но уже в 2014 году, с появлением атак класса amplification, даже крупнейшие операторы связи были не в состоянии справиться со злоумышленниками. Начинается эра облачных решений в ИБ, когда эффективный ответ распределенной угрозе может быть только распределенным»,— говорит он. Уже в ближайшие два-три года ландшафт рынка ИБ должен кардинально измениться. Александр Лямин объясняет: «Сейчас уже появилось два новых вектора атаки: инфраструктура сети и TCP-стек. Для ИБ-индустрии это вызов на ближайшие год-полтора». Однако в будущем, говорит господин Лямин, грядет «троица апокалипсиса»: интернет-вещей, IPv6 (шестая версия интернет-протокола.— **„Ъ“**) и эволюция мобильных сетей передачи данных. «Девайсы IoT (Internet of Things — интернет вещей.— **„Ъ“**) еще на выходе с завода содержат в себе уязвимости, которые никогда не патчатся (не устраняются за счет обновления установленной на устройстве программы.— **„Ъ“**). Это благодатное поле для хакеров, которые легко получат доступ в каждый дом. Так что ландшафт ИБ будет меняться радикально, если раньше от DDoS-атак страдали компании, то скоро будут страдать обычные люди»,— констатирует Александр Лямин.

Алексей Упатов

«Организации стали более серьезно относиться к мобильным угрозам»

— эксперт —

На конференции MWC-2016 в Барселоне Евгений Касперский сказал, что кибербезопасность строится на знании людей и компаний об угрозах, использовании правильных продуктов для защиты и некоторой доли паранойи. СЕРГЕЙ ЗЕМКОВ, управляющий директор «Лаборатории Касперского» в России, странах Закавказья и Средней Азии, рассказывает, следуют ли этим принципам клиенты в реальности.

ПРЕСС-СЛУЖБА «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

— Какие тенденции в сфере ИБ сегодня наблюдаете?

— Традиционно востребованы те решения, которые помогают компаниям либо сохранить деньги (данные, информацию, соответствие требованиям законодательства), либо заработать. Достаточно неплохо продолжают расти продажи комплексных решений в области защиты от внешних и внутренних угроз, решения по борьбе с таргетированными атаками, активно развиваются продажи различных сервисов по безопасности (защита от DDoS-атак, расследование компьютерных инцидентов, и другие), а также предоставление подобных сервисов из облаков различных провайдеров телеком-услуг.

У нас все чаще в качестве решения рассматриваются именно продукты российских компаний. Обусловлено это, конечно, прежде всего экономическими проблемами (рост курса доллара и евро, режим максимальной экономии и эффективности) и внешне- и внутриполитической ситуацией (санкции, контрсанкции, импортозамещение и др.).

— Как меняются подходы в защите от киберугроз?

— Для больших компаний важны комплексные решения, включающие в себя еще и сервисную составляющую: техподдержку, возможность оказания услуг по расследованию компьютерных инцидентов и так далее. В целом компании все чаще выбирают как раз такие комплексные и специализированные решения. Они постепенно осознают, что традиционного антивируса уже недостаточно: ландшафт угроз и атаки становятся все более сложными. Так, по данным исследования «Лаборатории Касперского», одним из ключевых приоритетов для российского бизнеса становится защита от целевых атак, в 2015 году ее использовали уже 40% организаций.

Поэтому и для «Лаборатории Касперского» главным образом прошлый год был связан с развитием нескольких новых ключевых продуктов и направлений: решения по борьбе с таргетированными атаками, решения по защите критических инфраструктур и АСУ ТП (и развитие в рамках этого направления ряда дополнительных сервисов, таких как penetration testing, тестирование безопасности приложений, реакция на инциденты ИБ и др.), защита виртуализации и решения для ЦОДов. Еще одной востребованной темой оказались сервисы по обучению специалистов и различные программы осведомленности персонала в вопросах ИБ.

Таким образом, мы предложили нашим клиентам классическую модель: от выявления на этапе различных тестов узких мест в ИБ до решения этих проблем с использованием разработанных нами технических средств защиты и программы обучения для специалистов ИТ и ИБ и общего персонала, так как зачастую именно человек является слабым звеном в системе ИБ любой компании. Кроме того, рост таргетированных угроз и целенаправленных атак показывает, что без наличия в штате крупной компании специалиста (-ов), обладающих достаточно глубокими знаниями в области antimalware research, крайне сложно противостоять этим видам атак, технические средства являются лишь инструментом, помогающим сотрудникам ИБ обнаружить подозрительную активность в корпоративной сети.

— Угрозы, которые несет бизнесу стремление сотрудников использовать публичные облачные сервисы и личные устройства уже имеют решения и больше уже не так страшны?

— Мы видим, что организации стали более серьезно относиться к мобильным угрозам: 48% респондентов нашего опроса сообщили, что гораздо более обеспокоены вопросами мобильной безопасности, чем год назад. Это действительно актуальная угроза, ведь сегодня в России, согласно опросу домашних пользователей, проведенному «Лабораторией Касперского» в 2015 году, почти каждый четвертый сотрудник компании использует собственное мобильное устройство для работы и хранит на нем рабочие файлы. Порой в гаджетах пользователей можно обнаружить и более конфиденциальную информацию, например пароли для учетных записей рабочей почты (17%). Следовательно, потеря или кража устройства может иметь серьезные последствия для бизнеса.

Несмотря на это, каждая пятая организация (21%) не принимает вообще никаких мер для защиты смартфонов и планшетов сотрудников, используемых для работы. Наиболее популярный способ защиты — антивирусное решение, но его использует сейчас только 40% компаний, а планирует обратиться в будущем 45%. При этом угроз под мобильные платформы становится все больше: за прошлый год наши эксперты обнаружили в три раза больше новых вредоносных программ, их количество приближается к 1 млн новых программ в год.

Поэтому компаниям необходимо иметь внятные политики безопасности по работе с корпоративными сервисами с мобильного устройства, иметь возможность удаленно управлять устройством, оперативно реагировать на внештатные ситуации, такие как попытка целевой атаки или кража устройства. В обязательном порядке требуется установка защитного ПО.

Интервью взяла Мария Анастасьева