информационные технологии

Безопасный интеллект

В период экономического спада желающих поживиться чужим добром становится все больше. Киберпреступность набирает обороты и самоорганизуется в эффективные структуры. Поставщики аппаратных и программных средств противопоставляют интеллектуальные средства защиты, обеспечивающие непрерывность бизнес-процессов. Сегмент информационной безопасности (ИБ) сохраняет рост на фоне общего спада в ИТ-отрасли.

ЕВГЕНИЙ ПАВЛЕНКО

Вопросы информационной безопасности становятся только острее

— сектор рынка —

На прошедшей в феврале в Сан-Франциско конференции по ИБ RSA Security Conference-2014 чаще всего можно было видеть на вывесках и слышать на выступлениях слово «intelligent» («умный, интеллектуальный») по отношению к средствам информационной безопасности.

Это отражает некий продуктовый тренд, которому пытаются следовать маркетологи компаний, выпускающих соответствующие программные и аппаратные средства. Владимир Гайкович, глава компании «Андэк», рассказывает, что атаки киберпреступников стали целенаправленными, распределенными во времени и использующими разноплановые методы для преодоления защиты.

Целью этих атак, как правило, является кража денег. Охота за одной жертвой может продолжаться месяцами, за это время хакер пытается нащупать дыры в защите и пробует различные способы взлома системы безопасности, а после проникновения в систему ведет себя осторожно, ожидая момента для совершения хищения.

По мнению аналитиков, надежно защититься от таких нападений с помощью межсетевых экранов, систем обнаружения атак, антивирусов и других стандартных средств невозможно. Современная система защиты должна непрерывно контролировать действия пользователей и программ, сигнализируя администраторам о подозрительных ситуациях.

По мнению поставщиков, интеллектуальность средств защиты как раз и заключается в том, чтобы на основе данных от разнородных средств защиты строить модели поведения пользователей и программ и на основании отклонений от них судить о наличии той или иной проблемы.

Антон Чувакин, директор по исследованиям в области ИБ американской компании Gartner, говорит, что инновации, которые показывают на конференции RSA, как правило, начинают появляться у корпоративных пользователей спустя два-три года после анонса. По опыту прошедших лет в России первые внедрения новых технологий случаются еще спустя два-три года. То есть пока нет речи о массовом внедрении комплексных интеллектуальных систем защиты в российских компаниях.

При этом киберпреступники сегодня как никогда организованны и технологически подкованы. Питер Анаман, глава отдела по онлайновому пиратству Microsoft Cybercrime Center, во время конференции Play It Safe Day рассказал о ботнете Citadel, который был организован как хороший бизнес. Хакер, который проживает предположительно на территории РФ или Украины, по прозвищу AquaBox организовал веб-сервис, в который были приглашены порядка 90 киберкриминальных групп. Через сайт они получали обновления вредоносного ПО, техническую поддержку, могли купить дополнительные ресурсы для организации атак и т. д. Так, даже неискушенный в технологиях злоумышленник мог с легкостью организовать DDoS-атаку.

По словам Александра Лямина, генерального директора компании Qrator Labs, защищающей от DDoS-атак, сегодня устроить серьезное нападение такого рода можно, используя всего лишь пять-десять серверов. При этом, по словам господина Лямина, 90% сетей операторов в РФ не готовы к подобным вторжениям. Это значит, что при возникновении атаки достаточно высокой скорости, могут отключаться целые сегменты российской части интернета.

Другая угроза, которая приводит к потерям огромных сумм денег — утечки информации. В аналитическом центре Zecurion Analytics посчитали, что по этой причине в 2013 году российские и зарубежные компании потеряли более $25 млрд. Причем в 30% случаев к этому привела деятельность хакеров или внутренних инсайдеров. Общий ущерб от внутренних инцидентов информационной безопасности вырос на 25% по сравнению с 2012 годом и составил чуть более $25 млрд.

Рост объемов ущерба от утечек данных указывает на то, что компании не уделяют защите информации должного внимания, вследствие чего теряют колоссальные деньги. Так, в среднем по миру убыток от одной утечки составил $32 млн, в России размер финансового ущерба несколько меньше, а вот максимальные потери от одного инцидента составили более 4 млрд рублей.

Владимир Ульянов, руководитель аналитического центра Zecurion, говорит, что в 2014–2016 годах стоит готовиться к увеличению краж персональных данных из банков. Мошеннические схемы, связанные с эквайрингом пластиковых карт, становятся все более эффективными и позволяют злоумышленникам быстро монетизировать полученную информацию.

Непрерывный рок-н-рол

На рынке средств информационной защиты существует большое количество продуктов, которые реагируют на какие-то отдельные виды угроз. Такой подход уже устарел, но многие компании продолжают им пользоваться. При этом ситуация постепенно сдвигается, и корпоративные заказчики понемногу начинают понимать преимущества комплексных интеллектуальных систем защиты, обеспечивающих непрерывность бизнес-процессов.

Аркадий Прокудин, заместитель руководителя Центра компетенции информационной безопасности компании «АйТи», говорит, что сегодня передовой подход в области ИБ, когда человек создает процессы, а защиту осуществляют системы в автоматическом режиме. То есть создается самозащищающаяся инфраструктура, так как человек не в состоянии успеть на все среагировать в реальном времени.

И, конечно, при построении таких систем на первое место выходят интеллектуальные системы защиты. «Современный крупный клиент понимает, что, поставив межсетевой экран и антивирус, защиты организации не добьешься. Необходимо подходить комплексно к проблеме. Сегодня уже недостаточно системы, которая автоматизирует выполнение рядовых функций защиты. Настало время решений, автоматизирующих целые процессы»,— говорит господин Прокудин.

Михаил Башлыков, руководитель направления информационной безопасности компании КРОК, отмечает, что уровень зрелости и заказчиков, и поставщиков растет. Помимо базовых средств информационной безопасности компании внедряют сложные системы защиты, которые должны учитывать особенности бизнес-процессов и бизнес-систем. «Управление ИБ — это процесс. И его нужно строить по общепризнанным стандартам (ISO-27001, ГОСТ) с учетом специфики организации. При оценке эффективности этого процесса также часто учитываются вопросы непрерывности бизнес-деятельности»,— сказал он

Дмитрий Титков, менеджер по работе с финансовым сектором компании Check Point Software Technologies, говорит, что компании ищут способы более эффективной защиты, стремясь при этом к удобству управления и простоте использования. «Сегодня нужно воспринимать комплексный подход к ИБ как некоторую философию системы, которая бы была интеллектуальной и гибкой, при этом сохраняя непрерывными бизнес-процессы. Именно такой подход был применен в этом году компанией Check Point в концепции Software-Defined Protection — новой архитектуре безопасности, которая помогает соответствовать одновременно и размытым границам корпоративного периметра, и динамике эволюции угроз»,— продолжает господин Титков.

Сегодня стало понятно, что любая защита данных или инфраструктуры — это постоянный процесс, который меняется и совершенствуется во времени (как у заказчика, так и у производителей средств безопасности). Если этого не происходит, появляются дыры в защите.

Аркадий Прокудин рассказывает, что раньше заказчики хотели от систем управления ИБ, чтобы она помогала управлять настройками оборудования из одной точки. Но сегодня задачи куда шире. Современный заказчик не просит, а требует выстроить у него информационную безопасность как процесс и автоматизировать его. А это сделать непросто, потому что в процесс управления ИБ включены и управление активами организации, и управление рисками и множество других подпроцессов.

По мнению Сергея Земкова, управляющего директора «Лаборатории Касперского» в России, странах Закавказья и Средней Азии в настоящее время основа роста рынка ИБ — это комплексные продукты, которые обеспечивают безопасность данных компании во всех аспектах деятельности, имеют централизованное управление, удобны и экономичны.

По его словам, набирают популярность системы Security Intellegence, причем в первую очередь так называемые Security Cloud — защитные решения, находящиеся в «облаке» и доступные заказчикам через интернет. Такие системы, как, Kaspersky Security Network, наделены большим количеством «интеллекта», а их перенос в «облако» позволяет системе оперировать большими объемами данных и получать доступ к большим вычислительным мощностям и, таким образом, быстрее реагировать на самые актуальные угрозы и атаки в киберпространстве. По словам господина Земкова, сегодня уже многие крупные компании принимают решение об использовании подобных интеллектуальных систем внутри собственной IT-инфраструктуры.

Ищи ветра в поле

Вопросы безопасности становятся все острее не только из-за роста активности и организованности киберкриминала. Влияют и другие факторы, о которых рассказал на IDC IT-Security RoadShow в Москве главный исследователь-аналитик IDC Михаил Попов. Среди них: усиливающийся тренд Bring Your Own Device и мобильность, распространение «облаков», повышение активности компаний в социальных сетях. Именно в этих областях, а также в сфере инструментов работы с Big Data аналитик IDC видит поле для деятельности разработчиков средств защиты. Это сегменты, за счет которых рынок ИБ в России и мире будет развиваться в ближайшие годы.

Конфиденциальные данные организаций, которые хранятся на персональных мобильных устройствах, находятся вне контроля ИТ-отделов и остаются крайне уязвимыми. Согласно исследованию Check Point «Влияние мобильных устройств на безопасность информации», каждая шестая компания в мире потеряла в 2012 году от утечек через мобильные устройства более $0,5 млн, а в 42% организаций ущерб превысил $100 тыс.

Драйверами рынка ИБ выступают сегодня решения по защите «облачных» инфраструктур, виртуальных сред, а также мобильных технологий, получающих все большее распространение. Он ожидает, что сохранят свою популярность решения, защищающие от утечки конфиденциальной информации, мошенничества, направленных атак на информационные системы. «Обычно подобные риски возрастают в кризисное время, когда увеличивается конкуренция, происходят слияния и поглощения,— объясняет господин Башлыков.— Также на популярность средств информационной безопасности большое влияние оказывают новостные поводы, появляющиеся периодически в СМИ. Стоит в информационном поле появиться новости о DDoS-атаке или новом вирусе, как заказчики начинают интересоваться техническими средствами, которые уменьшают негативные последствия от действий злоумышленников». На фоне публикаций об отказах в обслуживании сайтов госструктур и телеканалов можно ожидать, что в этом году на соответствующие средства защиты будет ажиотажный спрос. В Национальной ассоциации инноваций и развития информационных технологий (НАИРИТ) подсчитали, что за прошлый год количество DDoS-атак на государственные и коммерческие инфраструктурные институты выросло на 178%, тогда как в предыдущие годы эта цифра сохранялась на уровне 20–30%.

Датчик движения

На фоне общей стагнации экономики РФ и прогнозов по падению объемов рынка информационных технологий в целом рынок информационной безопасности все еще выглядит перспективным.

Михаил Башлыков говорит, что сегмент ИБ традиционно растет примерно в 1,5–2 раза быстрее, чем другие ИТ-услуги «Поэтому снижение темпов для нас не столь драматично. По итогам 2013 года мы ожидаем, что данное направление в КРОК увеличится примерно на 10%. И тенденция к росту сохранится. Конечно, сложно давать четкие прогнозы, но рост, по нашим предположениям, в ближайшей перспективе составит 15–20%»,— заключает он.

Сергей Земков объясняет, что сегмент ИБ продолжает расти, так как защитные решения по-прежнему входят в базовые ИТ-системы для работы любого предприятия. «Вместе с тем мы наблюдаем влияние кризисных тенденций — в частности, они спровоцировали снижение темпа роста на рынке ИБ во второй половине прошлого года. В целом, по нашим оценкам, в итоге за 2013 год рынок вырос не более чем на 10–12%»,— говорит господин Земков.

Несмотря на замедление экономики, связанное с кризисными тенденциями, крупный бизнес и государство продолжат реализацию проектов в области ИБ в нынешнем году.

«Традиционно основными потребителями услуг информационной безопасности являются финансовые организации, операторы связи, крупные торговые сети, развивающие онлайн-торговлю. Эти компании сильно зависят в целом от ИТ, потому простой систем, вызванный, например, DDoS-атакой, может негативно отразиться на всем бизнесе. Для государственных структур вопрос защиты ресурсов также стоит достаточно остро. Жесткие требования регуляторов обязывают их хранить, обрабатывать и передавать информацию должным образом»,— объясняет господин Башлыков.

Дмитрий Титков напоминает также, что компании телекоммуникационной отрасли в погоне за новыми скоростями передачи данных (3G, LTE и т. д.) требуют от поставщиков ИБ все более и более производительных решений. Кроме того, ведущие предприятия нефтегазового сектора традиционно являются активными потребителями решений по информационной безопасности. В последнее время также всерьез озаботились вопросами ИБ государственные и общественные организации, которые все чаще подвергаются атакам по политическим мотивам (так называемый хактивизм).

Господин Земков отдельно отмечает решения для защиты критических объектов и инфраструктуры (сектора энергетики, предприятия транспорта и т. п.). Защищать и использовать решения по безопасности такие предприятия будут все активнее, потому что угрозы для них становятся все более реальными.

Введение требований по уведомлению об инцидентах может стать драйвером развития рынка ИБ. Это позволит увидеть реальную картину по инцидентам и мошенническим действиям в масштабах страны. Следующим шагом, по мнению господина Прокудина, должно быть требование по уведомлению о таких инцидентах в режиме реального времени.

Также в последнее время законодатели взялись за сектор промышленности и критически важных объектов. В этой области господин Прокудин видит потенциал для роста.

То есть российский рынок ИБ, как и в прежние годы, весьма зависим от требований регуляторов. Это означает, что компаниям приходится следовать требованиям ФСТЭК, ФСБ и Банка России. Но выполнения этих требований, как правило, недостаточно для обеспечения реальной безопасности, которая необходима для ведения бизнеса сегодня. Количество угроз растет, но компании стремятся обеспечить защиту, не раздувая штат сотрудников. Поэтому все больше российских заказчиков обращаются за соответствующими решениями к мировым лидерам, которые, в свою очередь, уделяют достаточное внимание вопросам локальной сертификации продуктов.

Аркадий Прокудин рассказывает, что, как правило, развертывание современной системы ИБ происходит в два этапа. Для начала внедряются системы управления логами и системы управления событиями/инцидентами. В этом направлении господин Прокудин обозначает следующих лидеров: IBM QRadar, HP ArcSight и McAfee SIEM. Эти приложения позволяют собирать информацию о состоянии всех информационных систем и систем безопасности в едином месте. Такой подход позволяет видеть полную картину организации, не упуская даже мельчайших моментов. Внедрение систем SIEM позволяет руководителю ИБ и ИТ принимать решения при возникающих инцидентах в кратчайшее время, опираясь на полную информацию.

Вторым этапом внедряются решения следующего интеллектуального уровня — системы автоматизации процессов ИБ и построения систем управления информационной безопасностью. Такие комплексы базируются на решениях Security Information and Event Management (управление событиями и информацией о безопасности) и включают в себя управление рисками и активами, а также отчетностью и инцидентами.

Светлана Рагимова