И снова об импортозамещении

Анатолий РОМАШЕВ,
начальник отдела безопасности прикладных систем, «Информзащита»

Еще несколько лет назад фраза «отечественные средства защиты информации» вызывала улыбку у специалистов в области информационной безопасности. Причиной приобретения и использования такого рода программного обеспечения или аппаратных комплексов считался не функционал, а требования регуляторов, обязывающих их применять.

Такой подход создавал довольно курьезные ситуации. К примеру, система межсетевого экранирования работает на базе западной продукции, но, для соответствия требованиям регуляторов, перед зарубежным межсетевым экраном в режиме «any-any» физически стоит отечественный аналог. Похожие ситуации встречались повсеместно.

Мнение рынка было таково, что кроме антивирусных средств защиты российские производители средств ИБ предложить для real security больше ничего не могли. Прошло время, и ситуация начала меняться. У отечественных разработчиков средств защиты информации появляются решения, призванные обеспечить защиту от современных типов угроз, и некоторые компании пока очень осторожно, но выходят на западный высококонкурентный рынок со своими продуктами (например, Wallarm и Positive Technologies). Впрочем, таких решений пока не очень много, и доля зарубежных несертифицированных продуктов в составе систем защиты информации заказчиков по-прежнему остается довольно большой, на что в сегодняшних условиях необходимо обратить особое внимание.

Проблематика использования несертифицированных зарубежных средств защиты информации актуальна как в госсекторе (особенно в оборонной промышленности), так и в коммерческих структурах.

Кибервойну прогнозируют многие авторитетные аналитики. В такой ситуации использовать в критических инфраструктурах ПО, произведенное потенциальным «противником», неразумно. При этом повсеместное импортозамещение не должно нарушить отлаженные бизнес-процессы, ведь коммерческим структурам важно, чтобы их инфраструктура и данные были защищены одинаково качественно каждый день.

Современный рынок отечественных ИБ-продуктов может предложить решения, позволяющие обеспечить защиту государственных интересов и обезопасить бизнес коммерческих компаний. Раньше заказчики с высоким уровнем зрелости служб ИТ/ИБ российских вендоров не рассматривали в принципе, сейчас они все чаще соглашаются протестировать отечественные решения, и нередко в конечном итоге выбор падает на них.

Если попытаться разобраться в причинах появления на рынке эффективных средств защиты информации российских производителей, то тезисно можно выделить следующее:

- высокая экспертиза разработчиков;
- мировая тенденция динамичного роста рынка ИБ;
- в некоторых направлениях зарубежным лидерам рынка ИБ российские компании начинают создавать реальную конкуренцию;
- государственное регулирование информационной безопасности.

Разумеется, есть еще ряд факторов (например, господдержка ИТ-отрасли, появление российских ИТ-инвестфондов, изначальная ориентация разработчиков на зарубежный рынок), но оценить, какой вклад они внесли в укрупнение отечественного рынка производителей средств ИБ, – тема для отдельного разговора.

Талантливые программисты в России были всегда, но раньше они уходили либо в лаборатории западных компаний, которые зачастую открывались непосредственно при вузах (Intel тому пример), либо в НИИ, а оттуда в эмиграцию. Причины этого явления носят экономический характер и относятся к периоду 1990-х гг.

С появлением свободного капитала у некоторых отечественных компаний и доступа к инвестициям у других ситуация стала меняться. Эмиграция не уменьшилась, даже, по данным «Росстата», увеличилась, но специалисты сферы ИБ стали все чаще работать на родине. Логика проста: зачем куда-то ехать, если и в России появилась возможность решать не менее

интересные задачи за сопоставимое вознаграждение. Надо отдать должное российским компаниям – производителям средств защиты, которые стали гораздо плотнее и эффективнее работать с университетами и школами, что на Западе практикуется уже не один десяток лет: дни открытых дверей, конкурсы программирования, преподавательская деятельность специалистов ИБ и т. д. Довольно часто студенты 3–4 курсов уже являются штатными сотрудниками российских компаний – разработчиков коммерческого ПО, причем решаемые ими задачи не ограничиваются тестированием программного обеспечения или первой линией технической поддержки.

Большой толчок развитию разработки ИБ-продуктов в России, несомненно, дал общемировой тренд развития ИТ. Появились ниши, где либо конкуренция не очень высокая, либо есть возможность предложить что-нибудь более функциональное. Так, российские компании стали выходить на рынок EndPoint Security, анти-DDoS, DLP, MDM, защиты SCADA-систем, анти-APT, анти-Fraud решений, WAF, SIEM. Отчасти по этой причине некоторые компании, работавшие раньше в основном с госзаказами, переориентировались на коммерческий сектор (яркий пример – МФИ Софт, производивший оборудование и ПО для СОРМ, в настоящее время реализующий высокопроизводительные решения по защите БД, DLP с учетом своих наработок в части СОРМ). Предлагаемые отечественные решения перестали уступать по функционалу и уровню сервиса зарубежным аналогам и в сочетании с рублевым прайс-листом выглядят заманчиво для российских заказчиков.

Еще одно преимущество отечественных решений – они создаются с учетом российской специфики. Зарубежные производители прекрасно знают, как должен выглядеть PAN, email или номер социального страхования гражданина США, но объяснить им, что такое российские персональные данные (например, СНИЛС) порой проблематично. Также стоит учитывать разницу в количестве клиентов у зарубежных и отечественных вендоров. Опыт «Информзащиты» по работе с зарубежными и отечественными производителями средств ИБ показывает, что реализация запросов на доработку функционала, время реакции и отработки инцидентов у отечественных производителей быстрее, а уровень pre-sale и post-sale поддержки – выше.

В то же время необходимо отметить, что есть направления, в которых аналогов зарубежным продуктам у отечественных производителей пока нет либо они в чем-то уступают. Наиболее конкурентоспособны решения отечественных производителей в части антивирусной защиты (AV), защиты веб-приложений (WAF), защиты от утечек конфиденциальной информации (DLP), защиты SCADA-систем. Рынок SIEM-систем, межсетевых экранов, систем обнаружения/предотвращения вторжений (IPS/IDS), систем управления учетными данными (IDM), систем управления мобильностью предприятия (EMM), защиты от целенаправленных атак, систем контроля привилегированных пользователей (PAM) и некоторых других систем остается за зарубежными производителями, но доля отечественных решений неуклонно растет. А вот, скажем, решений по анализу поведения пользователей (User Behavior Analytics), защите облачных технологий (Cloud Security, например Cloud Access Security Brokers), решений класса GRC среди отечественных производителей средств защиты информации либо нет, либо рассматривать их как серьезных конкурентов зарубежным производителям пока рано. Так что простор для творчества у отечественных производителей есть, и при наличии спроса можно ожидать и предложения.

Решения от зарубежных производителей, как правило, представлены на рынке давно. В 2000-х они действительно были визионерами, делали эффективные и функциональные решения класса МЭ, IPS/IDS, WAF, DLP и т. д., но в 2017 г. использовать в своих продуктах реляционную базу данных, «толстых клиентов» в качестве консолей управления, мегабайты сигнатур – это, как минимум, несоответствие современным стандартам. С момента создания архитектура продуктов не менялась, просто добавлялся тот или иной функционал, увеличивался номер версии продукта и т. д. Полностью переделать продукт, его архитектуру и принципы работы никто не решается по вполне объективным причинам: переработка продукта требует довольно серьезных затрат (по сути, это разработка нового продукта с реализацией обратной совместимости, включающая еще и поддержку двух веток одного и того же продукта). В этом еще одно преимущество компаний, которые только начинают разработку: они уже на старте могут включить в дизайн современные технологии и подходы, что, собственно, и делают.

Анализируя отечественный рынок средств ИБ, нельзя не сказать о государственном регулировании ИТ- и ИБ-отрасли. Исторически наше законодательство (объективности ради – не только российское), регламентирующее вопросы ИБ, немного отстает от реактивно развивающихся зарубежных технологий. Поэтому утверждать, что государственное регулирование дает толчок развитию ИБ отрасли, нельзя. Но именно такое регулирование позволило в свое время российским компаниям, продающим сертифицированные средства защиты информации, направить часть выручки на развитие новых направлений и решений. Как результат – появление довольно интересных продуктов, которые нацелены на защиту от сложных угроз в области ИБ и позволяют составить конкуренцию зарубежным аналогам.

Сегодня позитивной тенденцией является тот факт, что регуляторы наконец обратили свое внимание на современное положение дел в мире ИБ. Новые требования теперь проходят этап обсуждения экспертным сообществом. Реализация этих требований к защите информации, несомненно, должна положительно сказаться на общем уровне защищенности как государственных информационных систем и критически важных инфраструктур, так и коммерческого сектора. ■