Вячеслав Медведев
старший аналитик отдела развития

Внедрение высокотехнологичных продуктов: мечты и российская действительность

В последнее время многие государственные и частные инициативы направлены на внедрение высоких технологий. Инноградов, технопарки, поиск инноваций в стране и за рубежом, декларации о снижении налогового бремени... Список можно продолжить. В СМИ время от времени появляются сообщения об отечественных разработках мирового уровня. Но почему за редчайшим исключением предлагаемое на рынке программное и аппаратное обеспечение заграничное?

Первая проблема — производство. Современная экономика, декларирующая отсутствие препятствий для бизнеса иных стран на своей территории, автоматически способствует тому, что становится невыгодно выпускать нечто массовое где-либо, кроме государств, где уровень заработной платы невелик. Все иные страны могут сосредоточиться на создании опытных образцов, технологий, управлении бизнесом… Нередки случаи, когда российские специалисты проектируют системы, а их изготовлением занимаются страны Юго-Восточной Азии. И это отнюдь не только бытовая техника, но и отечественные электронные компоненты, серверные системы… Почему же мы не видим всего этого в реальной жизни?

Если разобраться в этом вопросе, увы, окажется, что базовые компоненты — чипсеты и процессоры — все равно зарубежные. Дело в том, что для их производства требуются годы разработок и весьма объемное финансирование. На пустом месте можно только скопировать чужое решение, но это путь, ведущий в никуда. Кто может инвестировать огромные средства в создание продуктов, нужных для технологического рывка?

Казалось бы, бизнес. Получить в свои руки уникальные технологии и взять рынок под свой контроль — что может быть привлекательнее?

Но бизнес — это искусство извлечения прибыли, и он выбирает иной путь. Для разработки инноваций необходимо время. Это высокорисковый бизнес, не приносящий немедленного дохода. Далеко не все компании становятся здесь фаворитами, многие вообще остаются ни с чем. Зачем вкладывать миллионы в то, что может (без гарантии) окупиться только через 5—10 лет, когда сейчас можно взять кредит, приобрести товар и сразу получить деньги?

Выходит, что в случае аппаратных комплектующих помочь могут только долговременная политика государства — наличие преференций для отечественных производителей (скандалы с аппаратными закладка-

ми возникают постоянно) или целевое финансирование.

Как это ни странно, но с аппаратной частью все просто: необходимо «железо», аналогичное уже имеющемуся, но стандартизированное и без каких-либо закладок, — были бы деньги и желание. Гораздо хуже ситуация с программным обеспечением и совсем плохая — с ПО, ответственным за безопасность.

С одной стороны, за последнее время появилось множество достаточно конструктивных документов регуляторов, и это несомненный шаг вперед, но вот обеспечить безопасность с их помощью никак нельзя. Эти решения, по сути, являются показателем разрыва между реальными «способностями» средства защиты и тем, что пользователи «думают» о его функциональных возможностях.

Для примера рассмотрим защиту от вредоносных программ. Практически у всех на рабочих машинах стоит антивирус, но детский вопрос, зачем он нужен, большинство людей вгоняет в ступор. Отбрасывая варианты «потому что все используют» и «регуляторы требуют», добираемся до следующего: «антивирус должен ловить вирусы». Предположим, мы пропустили уточнение, что вирусов (вредоносных программ, способных к саморазмножению) как таковых сейчас практически не существует — бал правят совсем иные типы вредоносных программ, в основном троянских. А в какой же момент антивирус должен уничтожать вредоносные файлы? Ответ с точки зрения реальности поражает: в момент проникновения!

Для большинства системных администраторов и специалистов по безопасности очевидно: антивирус, который пропустил вирус, подлежит замене. Антивирус должен ловить все, выбор антивируса должен осуществляться на основе тестов — таковы обычные заблуждения в области ИБ. И, к сожалению, именно эту точку зрения косвенно подтверждают документы регуляторов. Плюс дань моде: антивирус должен иметь облачные технологии… Зачастую специалисты по безопасности используют модные решения, потому что об их важности заявлено в пресс-релизах, и не задумываются о том, действительно ли это целесообразно и безопасно.

Но современные вредоносные программы создают вовсе не одиночки, сидящие в темных подвалах. Это бизнес, желающий иметь доступ к огромным деньгам и получающий его благодаря незнанию пользователей об уровне угроз. Разработка вредоносных файлов поставлена на поток. И частью этой процедуры является их тестирование на необнаружение актуальными версиями антивирусных программ. Пока антивирус распознает вредоносный файл, тот в живую среду не выпускается.

Зачастую специалисты по безопасности используют модные решения, потому что об их важности заявлено в пресс-релизах, и не задумываются о том, действительно ли это целесообразно и безопасно.

Антивирус, возможно, и перехватывает вредоносные файлы в момент проникновения, но только те, модель поведения которых в нем заложена. Да, есть обнаружение известных вредоносных файлов, скрытых под упаковщиками с незнакомым форматом, есть и технология структурной энтропии для выявления неизвестных угроз по особенностям расположения участков кода в защищенных криптоупаковщиками проверяемых объектах, есть поведенческий анализатор, «изучающий» поведение запущенных вирусов на соответствие алгоритму действия известных типов вредоносных программ. И это, естественно, далеко не полный список — антивирусное ядро постоянно развивается. Все это повышает вероятность обнаружения неизвестной угрозы. Но… Пока антивирус распознает вредоносный файл, последний в живую среду не выпускается.

А как же тесты? «Лучший антивирус по количеству найденных угроз», «Лучший антивирус по скорости проверки», «Лучший антивирус на тесте эвристиков»…

Но результаты испытаний говорят лишь о том, насколько успешно тот или иной антивирус подавляет известные угрозы, в то время как на самом деле более опасны неизвестные вредоносные программы, которые он пропустил ранее (те самые, которые тестируются злоумышленниками на необнаружение). Вопрос в том, как антивирус справляется с ними. И следующий из него: какими должны быть требования к антивирусной системе защиты, когда реальность обхода антивируса в любой момент — факт, не подлежащий сомнению?

В условиях, когда в любой момент локальная сеть компании может быть скомпрометирована, системный администратор должен заранее принять меры на случай проникновения или самовольных действий сотрудников. По сути, он должен обеспечить доверенную среду при использовании программ, каждая из которых не может считаться доверенной (в силу уязвимости или неверной настройки).

В этом случае установленный антивирус должен не просто не пускать в сеть вредоносные программы, он должен уметь лечить активные заражения, не опознанные на момент проникновения угрозы. Антивирус обязан полностью находиться под контролем самозащиты — неизвестная вредоносная про-

грамма, обойдя защиту, первым делом попытается заблокировать получение обновлений. К управлению антивирусом нельзя подключать внешнюю систему управления, которая не находится под контролем самозащиты антивируса. В системе антивирусной безопасности должен быть «Офисный контроль», ограничивающий права доступа пользователей и потенциально опасных программ.

Но знают ли специалисты по безопасности о возможностях систем защиты, предлагаемых вендорами (не говоря уже об их лицензировании)? Увы, нет. Так, фактическим стандартом экстренного лечения является утилита *Dr.Web CureIt!,* но многие ли знают о том, что уже давно существует ее аналог с опцией лечения по сети, не требующий личного присутствия у зараженного компьютера, — *Dr.Web CureNet!?*

К сожалению, при создании систем защиты акцент делается на безопасности компьютеров. «Что вы защищаете?» — «Рабочие станции». Но вирус не украдет вашу машину, а вредоносные программы, уничтожающие мониторы или жесткие диски, уже стали легендой: зачем губить монитор, если нужно вывести требование о выкупе?

Необходимо защищать информацию. Типичной ошибкой современного подхода к этой проблеме является обоснование отказа от защиты почты на уровне почтовых серверов или интернет-трафика на уровне шлюзов. Можно сравнить подходы стандарта *PCI-DSS,* пропи-

Естественным препятствием для применения современных средств защиты является финансовый вопрос — мелким или имеющим множество филиалов компаниям просто негде найти необходимое количество квалифицированных специалистов по безопасности.

савшего, что антивирус должен защищать от известных вредоносных файлов, и наших стандартов, требующих при наличии технической возможности установки антивируса на все объекты, которые могут быть заражены.

Какой бы ни использовался почтовый сервер — *MS Exchange, Lotus, Kerio, — у Dr.Web* есть решение для их защиты. Но… «Мы не защищаем почту на серверах, т.к. у нас есть антивирус и антиспам на рабочих станциях.» Конечно, есть, но повторим еще раз: пока антивирус обнаруживает вредоносный файл, тот в живую среду не выпускается. Неизвестные на момент проникновения вредоносные программы скапливаются в почтовых ящиках и дожидаются момента, когда пользователь отключит защиту или зайдет в почту с традиционно незащищенного мобильного либо домашнего устройства. И хорошо, если он заразит только свою машину, а если вирус уйдет к партнерам? Только антивирус на уровне почтового сервиса может пролечить почтовые ящики — за него этого не сделает никто.

Но нужно ли всегда выбирать защиту на уровне действующего почтового сервера компании? Далеко не факт. Антивирусы для почтовых серверов всегда ограничиваются интерфейсом, предоставляемым их разработчиками. И если компании нужен действительно мощный продукт, надо смотреть в сторону почтового шлюза, такого как дополнительный компонент *SMTP-proxy* в составе *Dr.Web Mail Security Suite*. В отличие от наиболее часто применяемых решений для защиты почтовых серверов он позволяет обеспечить более высокое качество фильтрации трафика не только с помощью антивируса и антиспама, но и за счет проверки правильности построения почтовых сообщений, соответствия отправителя используемому адресу, репутационных технологий…

Совершенно иную цель преследует защита периметра. В любой локальной сети работают компьютеры и устройства (временно или постоянно), установка антивируса для которых невозможна в силу особенностей выполняемых задач, слабости аппаратной части или по иным причинам. А вот попасть туда вирусу не мешает никто. За исключением особо одиозных представителей «темной стороны», большинство вредоносных программ не требует для своего запуска особых ресурсов или установки неких приложений. Казалось бы, заражения принтеров или устройств для чтения электронных книг — это такая же экзотика, как и заражение атомной станции. Однако последствия таких «манипуляций» могут быть масштабными. Пресечь проникновение способны только антивирусы на уровне шлюза.

Естественным препятствием для применения современных средств защиты является финансовый вопрос — мелким или имеющим множество филиалов компаниям просто негде найти необходимое количество квалифицированных специалистов по безопасности. В этом случае выходом может стать покупка программно-аппаратного комплекса, построенного в расчете на использование персоналом с минимальными знаниями по безопасности. Например, *Dr.Web Office Shield*.

Факт заражения может гарантированно подтвердить только «патологоанатом» — специалист по экспертизе инцидентов безопасности (например, из «Доктор Веб»), но стоит ли доводить дело до его визита? Не лучше ли подумать о защите заранее? эр