

В расчете на простоту и эффективность

Специалисты компании SafenSoft предлагают свои решения для защиты информационных систем

Константин Герашенко

Специалисты компаний, работающих в области информационной безопасности, отмечают не только постоянное увеличение количества угроз, но и расширение сферы деятельности киберпреступников.

Появилось множество новых платформ, в том числе на базе открытых программных продуктов, быстро развивается сегмент мобильных устройств, огромное число платежей и других денежных транзакций осуществляется через банкоматы и Интернет. Все это способствует увеличению активности злоумышленников, основные цели которых — кража денег и информации.

По этой причине спрос на решения в сфере информационной безопасности остается стабильно высоким, а темпы роста данного сегмента превосходят темпы роста ИТ-рынка в целом.

Однако надо отметить, что традиционным антивирусным комплексам становится все труднее быстро реагировать на ежедневно появляющиеся новые угрозы. Дело в том, что в основе почти всех антивирусных систем лежит технология сигнатурного сравнения. Это означает, что антивирус сравнивает фрагменты кода с уже известным вредоносным программным обеспечением. Понятно, что при таком подходе антивирусные решения всегда будут с запозданием реагировать на появление новых вредоносных программ, и, кроме того, есть вероятность, что какие-то особо изощренные и узкоспециализированные вирусы не попадут в поле зрения специалистов.

Вот почему многие ведущие игроки рынка информационной безопасности уделяют внимание другим способам борьбы с вредоносными программными продуктами, в частности развивают технологии эвристического и поведенческого анализов. Но и в этом случае нет гарантии полной безопасности.

Эффективное решение нашли специалисты компании SafenSoft. Они предложили взглянуть на проблему защиты информационных систем не с позиций обнаружения вредоносных программ, а с точки зрения обеспечения безопасной работы самой системы. При таком подходе меняется постановка задачи. Систему больше не нужно защищать от огромного количества постоянно мутирующих вредоносных программ — необходимо обеспечить безопасную работу самой системы. Другими словами, должны работать только те процессы, без которых невозможно выполнение текущей задачи, а вся другая активность считается небезопасной.



Михаил Калиниченко: «Спрос на решения SafenSoft растет. В прошлом году наш оборот увеличился на 40%».

Как отмечает **Денис Гасилин**, директор по маркетингу и PR компании SafenSoft, в прошлом году наметился тренд к переходу от пассивного противодействия киберпреступности и халатности персонала к более активным действиям. У системных интеграторов и конечных заказчиков появился интерес к новым, ранее не использовавшимся технологиям защиты информации.

«Продукты и технологии нашей компании пользуются

все большим спросом, — подчеркнул Денис Гасилин. — При обеспечении защиты корпоративных сетей, мобильных устройств, ноутбуков, удаленных точек — классические подходы к обеспечению информационной безопасности уже истощены, требуются новые, эффективные системы».

По словам **Михаила Калиниченко**, генерального директора SafenSoft, заказчики начинают переходить от «лоскутных» решений разных вендоров к комплексной системе безопасности одного вендора, которая «закрывает» бы все возможные уязвимости — от кражи информации собственными сотрудниками по e-mail или с помощью неразрешенного программного обеспечения до таргетированных хакерских атак. Говоря о результатах работы в 2012 г., Михаил Калиниченко сообщил, что оборот SafenSoft увеличился примерно на 40%, компания получила хорошую прибыль. Появилось несколько крупных заказчиков из числа финансовых компаний и государственных предприятий. Расширяется и региональное присутствие: SafenSoft вышла на рынки СНГ и уже работает в Белоруссии, на Украине, в Казахстане и Грузии. Всего же дистрибьюторская сеть SafenSoft охватывает 16 стран мира.

Канал сбыта представляет цепочку «вендор-партнер-конечный заказчик». «Мы достигли соглашения о сотрудничестве с такими крупными системными интеграторами, как „Абак“ (Казань), ГК „Юнит“ (Екатеринбург) и рядом более мелких фирм, — говорит Михаил Калиниченко. — В настоящий момент готовится соглашение с компанией КРОК. Дистрибуцией наших продуктов занимаются „Софтлайн“, „Софтлоджистик“, „Киви“, БУКА. В целом число партнеров исчисляется десятками и неуклонно растет. Среди крупных заказчиков можно назвать МВД Татарстана, Управление МВД по Челябинской области, КНААПО,

ООО „Заполяргражданстрой“ (Новый Уренгой), департамент Смоленской области по образованию, науке и делам молодежи, администрацию Магнитогорска, Брянскую областную думу и администрацию области, Брянский государственный сельскохозяйственный университет и др.».

По словам Дениса Гасилина, установившиеся в этом году партнерские отношения с крупнейшими компаниями-интеграторами будут способствовать более предметному и тесному взаимодействию с конечными заказчиками. Кроме того, вендор обещает проводить гибкую политику ценообразования, что сделает сотрудничество с SafenSoft выгодным для партнеров.

Михаил Калиниченко отметил, что продуктовая линейка компании включает решения для защиты банкоматов и платежных терминалов, конечных точек корпоративной сети, а также домашних компьютеров. «Взрывной рост количества банкоматов, новые требования Центробанка, законы, обязывающие организации защищать персональные данные своих сотрудников и клиентов, — все это идет на пользу нашему бизнесу, ведь продукты SafenSoft специально разрабатываются и развиваются так, чтобы соответствовать текущим и будущим потребностям рынка в области информационной безопасности, а также требованиям регуляторов, — заявил генеральный директор SafenSoft. — В разных рыночных нишах мы позиционируем себя по-разному. Например, на рынке защиты персональных компьютеров мы говорим о себе как о поставщике принципиально другого средства защиты, нежели антивирус.

В нише защиты ПО банкоматов и устройств самообслуживания мы занимаем лидирующие позиции и предлагаем решение, разработанное специально для таких устройств. На рынке средств защиты корпоративных систем мы исповедуем не классические догматы, а придерживаемся инновационного подхода. Здесь наши продукты полностью отвечают современным запросам заказчиков к системам информбезопасности, обеспечивая централизованную защиту и контроль целостности ПО клиента, и одновременно

«Прогноз» строит партнерскую сеть

Ольга Мельник

Разработчик BI-платформы фирма «Прогноз» была создана в Перми, там же до сих пор трудится основная команда разработчиков, более тысячи человек. Основой продуктов «Прогноза» стали научные разработки кафедры экономической кибернетики Пермского университета и Института экономики Уральского отделения Российской академии наук. За двадцать лет выполнено более полутора тысяч проектов в 35 странах, офисы и представительства компании открыты в 10 государствах. По предварительным данным, консолидированная выручка по МСФО ГК «Прогноз» в 2012 г. достигла 125 млн. долл., по сравнению с 2011 г. (81 млн. долл.) рост составил 55%. Львиная доля оборота по-прежнему приходится на Россию, несмотря на быстрый рост продаж за рубежом. «Прогноз» остается частной фирмой, IPO в планах есть, но не на текущий год.

Пока компания выполняла проекты для администрации президента РФ, «Газпрома» и органов власти разных уровней, ее успехи можно было приписывать внерыночным факторам. Но контракты с Coca-Cola и Международным валютным фондом показали, что продукты российского вендора конкурентоспособны на мировом рынке: год назад его платформа впервые была включена в «Магический квадрант» Gartner. В этом году продукт Prognoz Platform упрочил свои позиции: аналитики Gartner оценили его выше,

чем в прошлом, но по-прежнему отнесли к «нишевым».

По словам **Ильи Юта**, заместителя руководителя центра проектирования системного программного обеспечения, цель «Прогноза» — попасть в «лидеры» «Магического квадранта». Судя по отчетам Gartner прошлых лет, в сегменте «BI и аналитические платформы» развитие идет стремительно. Есть квадранты Gartner, где число, состав и даже позиции участников почти не меняются даже за пятилетку. Здесь же видна картина напряженной борьбы: одни фирмы появляются, другие исчезают, позиции меняются за год очень значительно, так что амбиции «Прогноза» вполне оправданны.

В состав Prognoz Platform (PP) входят традиционные BI-инструменты для разработки отчетов и дашбордов, а также инструменты для статистического анализа временных рядов, моделирования и прогнозирования. Так обеспечивается интеграция средств описательной (descriptive) и предсказательной (predictive) аналитики.

На уровнях средств разработки и BI-инфраструктуры в PP имеются механизмы для организации репозитория с многомерными источниками данных, ведением НСИ, ETL, настройками безопасности, доступом к реляционным БД и многомерным кубам. Предоставляются средства для кастомизации и разработки приложений (среда разработки, компоненты, SDK,



язык **Fore**, веб-сервисы). Реализована технология in-memory для многомерных кубов. Пользовательские инструменты и приложения доступны через веб-интерфейс в виде настольных и мобильных приложений. Инструменты платформы интегрированы с MS Office, порталами.

Для российского рынка все оценки Gartner имели бы в основном академический интерес, но с конца 2012 г. вендор начал создавать партнерскую сеть. Раньше «Прогноз» продавал и внедрял свои разработки самостоятельно, хотя действовали технологические партнеры и некоторые партнеры-внедренцы. **Артем Гришковский**, советник генерального директора компании, считает, что построение полноценной партнерской сети займет минимум 2–3 года.

В мире у «Прогноза» уже более 50 партнеров, в России — всего несколько, в том числе «Софтлайн», AT Consulting, «Барс» (Казань), «Профи» (Липецк), «Омега» (Санкт-Петербург). Гришковский отмечает, что в прошлом году руководству «Прогноза» стало ясно, что без развития партнерской сети невозможен ни дальнейший рост, ни упрочение положения на рынке, ни значимое расширение клиентской базы. Активное открытие в России представительств Microstrategy, энергичные действия SAP по продвижению своих BI-продуктов, тоже сыграла роль. Будущее вендор видит в партнерстве с консалтинговыми и интеграторскими фирмами, причем считает необходимым индивидуальную работу с каждым партнером. «Прогноз» контролирует каждое партнерское внедрение: как замечает Гришковский, «не все партнеры к этому готовы». С другой стороны, возможны ситуации, когда партнер еще не имеет квалификации, но у него уже есть клиент.

В этом случае «Прогноз» может провести внедрение своими силами при условии, что сотрудники партнерской фирмы тоже примут участие и будут изучать продукт и методологию внедрения, а на следующий год уже примут на себя определенные обязательства.

«Прогноз» делает и шаг в необычную для софтверного вендора сторону — открыт онлайн-сервис PROGNOSZ. Data Portal. Он дает доступ к обширному комплексу данных национальной и мировой экономики, структурированному по отраслям и рынкам. Сервис содержит постоянно обновляемую информацию из более чем двухсот авторитетных российских и международных источников. Ранее Data Portal служил только внутренним нуждам фирмы, но недавно было решено сделать его коммерческим. Предусмотрен период бесплатного ознакомления. Полная годовая подписка составляет 400 тыс. руб., но можно заказывать любой желаемый набор или использовать какие-то из готовых наборов с пропорциональным снижением цены. В качестве потенциальных потребителей создатели сервиса рассматривают все компании, имеющие аналитический отдел. Одним из основных конкурентов этому сервису руководители «Прогноза» называют агентство «Блумберг», а своими преимуществами считают инструментарий поиска, анализа и визуализации данных. Примечательно, что на основе портала корпоративные клиенты могут создавать гибридные решения: использовать данные и аналитические инструменты внутри фирмы, объединяя внешнюю информацию и собственные данные. Для таких проектов потребуется привлечь специалистов «Прогноза» или компании-партнера.

» обладают функциональными возможностями DLP-систем. Кроме того, наши решения не требуют ежедневных обновлений, не нуждаются в постоянном подключении к Интернету, менее требовательны к ресурсам системы и эффективнее противостоят целенаправленным атакам.

Все больше заказчиков выбирают инновационный проактивный подход к защите. Решение SafenSoft Enterprise Suite, предназначенное для защиты рабочих станций и серверов корпоративной сети, используется уже более чем в 400 финансовых, коммерческих и государственных структурах».

Представители компании также сообщили, что число

инсталляций системы SafenSoft TPSecure, «обороняющей» устройства самообслуживания, выросло в России до 70 тыс., завершено тестирование на совместимость с банкоматами ведущих производителей. В SafenSoft отмечают, что их продукты хорошо сочетаются и не конфликтуют с решениями других вендоров, в том числе с антивирусными программами.

В частности, в начале этого года стало известно, что система SafenSoft TPSecure для защиты программного обеспечения банкоматов будет продвигаться на рынки Латинской Америки совместно с антивирусом «Лаборатории Касперского».