

CeBIT: опасные облака

Безопасность для облаков — одна из самых горячих тем на ИТ-рынке

ЮЛИЯ ДЮКОВА

Computerworld Россия

Разговоры о преимуществах облачных вычислений идут не первый год, но опасения относительно сохранности данных в облаке не убывают. Новая угроза безопасности возникает и со стороны мобильных устройств, которые за несколько лет стали частью повседневной жизни и компаний, и домашних пользователей. На недавней выставке CeBIT поставщики средств информационной безопасности рассказали о том, какой ответ они готовят вызовам времени.

Мобильные платформы и социальные сети

Немецкая компания G Data Software, традиционно ориентирующаяся на малый и средний бизнес, а также на домашних пользователей, привезла на CeBIT 2011 решение MobileSecurity, предназначенное для смартфонов на платформе Android.

«В течение многих лет мы считали, что нет смысла работать с мобильными платформами. Рынок очень разрозненный, на нем много вендоров и вариантов платформ: Apple, BlackBerry, Android, Windows Mobile, Symbian. Тогда нам очень мало встречалось вредоносного кода для мобильных устройств», — прокомментировал появление новинки Дирк Хохштрате, член правления G Data.

Однако, по его словам, ситуация изменилась коренным образом два года назад, когда Google выпустила платформу Android, которая начинает доминировать на рынке (в 2010 году, по оценке Хохштранте, ее рост достиг примерно 900%). На Android обрастили взоры и другие разработчики средств безопасности. Так, компания Eset привезла на CeBIT бета-версию собственного решения для Android.

Наталья Касперская, генеральный директор компании InfoWatch и председатель совета директоров «Лаборатории Касперского», видит в распространении разнообразных мобильных платформ серьезную угрозу безопасности информации, полагая, что их

существование «создает огромную дыру для утечки данных». По ее словам, пока не очень понятно, что делать с этим «зоопарком», как защищать мобильные устройства — и с точки зрения предотвращения утечек данных, и с точки зрения будущих угроз. Она также полагает, что с развитием платформы Android появится достаточное количество вирусов для нее и что защита мобильных устройств будет отдельным большим направлением деятельности.



ДИРК ХОХШТРАТЕ полагает, что будущее — за платформой Android

Что до остальных платформ, то, как считает Хохштранте, они переживают упадок, и поэтому в компании о них думают гораздо меньше. Однако известие о партнерстве Nokia и Microsoft, вследствие которого на смартфонах финской компании будет устанавливаться Windows Mobile 7, по его мнению, говорит о том, что рынок вновь ждет перетасовка.

В G Data также отмечают опасность социальных сетей. В компании полагают, что атаки в социальных сетях очень похожи на распространение червей в электронной почте, но в социальных сетях успешность таких атак возрастает в десять раз из-за человеческого фактора: люди склонны доверять сообщениям, при-

ходящим от их друзей. Для обеспечения безопасности G Data собирает информацию о ресурсах, и если выясняется, что они опасны, то она помещается в облачную базу данных. «В Германии сейчас мы запускаем G Data Cloud Security, это бесплатный плагин для Internet Explorer и Firefox, проверяющий адреса, на которые вы пытаетесь зайти», — заявил Хохштранте.

На российский рынок G Data вышла в конце 2009 года и в ближайшее время планирует открыть в Москве полноценный офис с шестью-восьмью сотрудниками, а также выйти на рынки Украины и Белоруссии. За прошлый год в России компания продала несколько тысяч коробочных продуктов домашним пользователям и сейчас начинает продажи через Интернет. Также у компании более 30 партнеров в регионах в области продаж B2B.

Впереди Европы

Доминирующим направлением в области информационной безопасности, по мнению Касперской, сейчас становится защита данных. В то время как инфраструктура компаний уже более или менее защищена, данные остаются уязвимыми, например потому, что в процессе работы быстро «плодятся» новые документы, часто оцифровываются старые. Другая проблема — возрастает сложность данных, категоризация информации превращается в отдельную задачу, которая пока не получила решения.

При этом она отметила, что российские компании не любят пускать на свою «кухню» чужих. Поэтому, например, у InfoWatch пока нет решений для облаков. Однако со временем появятся центры, которые будут сертифицировать провайдеров услуг на предмет безопасности, договоры, охватывающие весь спектр возможных проблем, и т. д. И преимущества облачных вычислений возьмут верх.

Сейчас InfoWatch планирует развивать продажи на Ближнем и Среднем Востоке.

А вот попытки работать на немецком рынке, по словам Касперской, оказались не очень удачными: местные предприятия опасаются гнева профсоюзов, выступающих против слежения за перепиской сотрудников. «Рынок DLP здесь, как ни странно, меньше развит, чем в России. Германия в этом плане отстает на два шага», — уверяет Касперская. — Но мы не теряем надежды, мы будем развивать рынок. Мы будем защищать не от утечек вообще, а от конкретных типов утечек для конкретных ниш».

Борцы с пиратством отметили десятилетие своей деятельности

НП ППП подвело итоги и обсудило планы на будущее

ТАТЬЯНА ФАРХАТ

Computerworld Россия

Некоммерческое партнерство поставщиков программных продуктов провело юбилейное собрание, посвященное десятилетию со дня образования. НП ППП было создано в 2000 году для борьбы с компьютерным пиратством. В ноябре состоялось первое учредительное собрание, на нем членами Пар-

тиерства стали «1С», АСКОН, «Гарант», «ИнтелГрупп», «Ладомир», «Ламинфо», «Логос-К», «Профит-Центр» и «СибЭксПро». На сегодняшний день в организации состоят 306 компаний; на собрании в ряды НП ППП было принято десять компаний, столько же исключено.

В 2001 году состоялась встреча учредителей организации с Владимиром Путиным, занимавшим тогда пост президента России. Результатом этой встречи стал федеральный закон «О внесении изменений и дополнений в статью 146 Уголовного кодекса Российской Федерации». Наконец, была введена ответственность за приобретение, хранение,

перевозку контрафактных носителей, если таковое осуществляется с целью сбыта, а также уточнены количественные критерии общественной опасности деяния [крупный размер — 100 МРОТ; особо крупный размер — 500 МРОТ]. Ранее четкие показатели величины ущерба отсутствовали.

Сегодня НП ППП активно сотрудничает с правоохранительными органами, причем в двух случаях из трех инициируют взаимодействие именно сотрудники МВД.

Одной из главных составляющих сотрудничества с правоохранительной и судебной системами являются

разработка и рекомендации для издания «Компьютерное пиратство: методы и средства борьбы», а также выпуск специализированных методических материалов. Постоянно проводятся семинары для работников правоохранительных органов при поддержке Еврокомиссии.

Важным событием, по мнению НП ППП, стало принятие Верховным судом постановления от 21 декабря 2010 года № 28 «О судебной экспертизе по уголовным делам». В нем, в частности, сказано, что наряду с государственными судебно-экспертными учреждениями экспертную деятельность осуществляют и негосударственные — представители некоммерческих организаций и даже частные лица. Эта новация, по мнению НП ППП, может быть на руку нечестным компаниям. В прошлом году началась также работа по внесению очередных изменений в четвертую часть ГК.