«ЕСЛИ ДОВЕРИЯ НЕ БУДЕТ, „ОБЛАЧНАЯ“ ТЕХНОЛОГИЯ ПРОСТО ИСЧЕЗНЕТ»

ПРИЧИНЫ ДЛЯ ПЕРЕХОДА НА «ОБЛАЧНЫЕ» ТЕХНОЛОГИИ И ГИБРИДНЫЕ РЕШЕНИЯ ОЧЕВИДНЫ И ХОРОШО РАЗРЕКЛАМИРОВАНЫ. НО ПОТЕНЦИАЛЬНЫЕ КЛИЕНТЫ СОМНЕВАЮТСЯ В БЕЗОПАСНОСТИ ПОДОБНЫХ СИСТЕМ. МИФЫ О ПОТЕРЕ КОНТРОЛЯ НАД СОБСТВЕННЫМИ ИНФОРМАЦИОННЫМИ СИСТЕМАМИ В БЕСЕДЕ С ГЛАВНЫМ АНТИВИРУСНЫМ ЭКСПЕРТОМ «ЛАБОРАТОРИИ КАСПЕРСКОГО», АЛЕКСАНДРОМ ГОСТЕВЫМ ПОПЫТАЛСЯ РАЗВЕЯТЬ ЕВГЕНИЙ ЧЕРЕШНЕВ.

BUSINESS GUIDE: Чем концептуально отличается формат потребления сервисов, информации и услуг из «облака» по сравнению с традиционными способами с точки зрения безопасности доступа?

АЛЕКСАНДР ГОСТЕВ: Самым принципиальным отличием является местоположение данных и способ доступа к ним. При традиционной организации хранения и предоставления, например в корпоративной сети, есть только два основных места — локальный компьютер и сетевые ресурсы внутри компании. Доступ осуществляется на уровне единой системы безопасности, при этом все находится под универсальным контролем. При размещении данных вовне или использовании внешних сервисов всегда появляются дополнительные звенья — это, как минимум, и сетевой провайдер, и сам провайдер «облачных» услуг. Соответственно, общий уровень защищенности такой системы уже начинает зависеть сразу от нескольких участников, при этом зачастую гарантий бесперебойной или защищенной работы между ними может и не существовать. В итоге вместо системы, в которой необходима только защита периметра организации, возникает система, нуждающаяся в защите внешнего канала и внешнего хранилища. В теории это снижает уровень защиты в целом, но помогает значительно снизить издержки, и в ряде случаев действительно оправдан именно такой вариант организации работы. Ситуация, при которой данные, хранящиеся в «облаке», защищены гораздо лучше, чем если бы они хранились внутри компании, не редкость.

BG: Публичное облако — iCloud, Google — выглядит красиво: почта, возможность обмена документами, в случае Apple — привязка кредитки. Каковы подводные камни?

А. Г.: Подводные камни подобных сервисов достаточно очевидны, и их весьма много. Это и риск доступа к этим данным со стороны иностранных ведомств (поскольку они расположены в США и принадлежат американским компаниям, то руководствуются законами этой страны и обязаны выполнять решения местных судов и регулирующих органов). Это и риск неработоспособности сервиса по техническим причинам (например, в результате хакерской атаки или банального отключения электричества) или по причинам ограничения доступа к нему на национальном уровне (например, Китай ограничивает доступ к ряду ресурсов Google). Не стоит забывать и о прямых атаках: если злоумышленник имеет доступ к вашему компьютеру, он имеет доступ к вашим данным в «облаке». Более того, кроме атак на самих пользователей у злоумышленников появляется новый объект для атак — само «облако». И если в системе безопасности этого «облака» будут бреши, могут быть украдены данные всех пользователей. Показательным примером является взлом компании HBGary в феврале. Хакерам не удалось проникнуть в локальную сеть компании, но им удалось получить доступ к корпоративной почте компании, базирующейся на сервисе Google Apps for Business. В результате весь архив почты был украден и оказался в публичном доступе.

ЛОКАЛЬНЫЕ ПРОАКТИВНЫЕ ПРОГРАММЫ ВЫПОЛНЯЮТ НЕ МЕНЕЕ ВАЖНУЮ ФУНКЦИЮ, ЧЕМ «ОБЛАКО»

ЮРИЙ МАРТЬЯНОВ

«ОБЛАЧНЫЕ» ТЕХНОЛОГИИ ИЗНАЧАЛЬНО НЕ ЗАДУМЫВАЛИСЬ КАК СРЕДСТВО РЕШЕНИЯ ПРОБЛЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

BG: Когда компания отказывается от хранения части данных (или абсолютно всех) на офисных серверах и отдает все на аутсорсинг, она сталкивается с вышеописанными рисками. А есть ли плюсы?

А. Г.: Что касается плюсов, то они, конечно же, есть, и именно они делают «облачные» технологии столь привлекательными и обеспечивают им стремительное развитие. Основным преимуществом является возможность снизить затраты на создание и поддержание собственных систем хранения и обработки данных, электронного документооборота. Стоимость серверов, оплаты труда администраторов, расходов на электроэнергию и многое другое перекладывается с компании на провайдера облачных услуг. Система организации доступа к этим ресурсам также позволяет значительно расширить возможности, например для мобильных пользователей, снимая массу ограничений при удаленной работе или использовании альтернативных операционных систем.

BG: Вспомним о человеческом факторе. Известно, что Кевин Митник не взламывал сети сам — он находил общий язык с не самыми квалифицированными в IT сотрудниками корпораций, и они делали работу за него. Что с «облаком»? Конечно, риск шантажа меньше, но и цена ошибки в случае вербовки сотрудника дата-центра в теории выше или нет?

А. Г.: Конечно, проблема инсайдерских атак стояла и будет стоять всегда независимо от того, использует компания «облака» или нет. С одной стороны, в ситуации с дата-центрами ответственность за подобные инциденты целиком лежит на владельце сервиса, однако в настоящее время практически отсутствует практика страхования подобных рисков и четкого разграничения ответственности. Грубо говоря, если ваши данные будут украдены в ходе инсайдерской атаки в дата-центре, вы вряд ли сможете получить компенсацию, покрывающую нанесенный ущерб. С другой стороны, защита собственных данных в «облаке» — общая задача клиента и владельца сервиса. Клиент должен использовать дополнительные меры, которые помогут избежать проблем даже в случае действий «облачного» инсайдера. Наиболее очевидный пример — дополнительное собственное шифрование данных. Не стоит думать, что все, что попадает в «облако», тут же станет доступным кому-то еще. Именно на доверии пользователя к «облакам» и строится их существование. Если доверия не будет, технология просто исчезнет. Пока это доверие есть, но относительно слабое. Будущее развитие покажет, будет оно крепнуть или наоборот.

BG: Какими программными продуктами защищаются информация и сервисы в «облаке»? Правильно ли я понимаю, что поставщики оборудования, в частности HP, могут выбирать партнеров и, по сути, происходит модификация уже существующих корпоративных систем защиты, в том числе от «Лаборатории Касперского»?

А. Г.: Поставщики оборудования, конечно, могут выбирать партнеров, но сложившаяся практика показывает, что выбор программных средств защиты делается исключительно «облачным» провайдером, при этом он совершенно не зависит от производителя используемого оборудования. Основным ПО для защиты данных в облаках являются системы шифрования, бэкапирования, контроля целостности и разграничения доступа. Антивирусная защита пока еще не стала стандартом де-факто для подобных систем, и это вызвано крайне широким спектром используемых «облачными» провайдерами платформ и отсутствием стандартов. Антивирусная индустрия находится только в самом начале процесса, но очевидно, что существующие корпоративные системы защиты не могут быть модифицированы для решения подобных задач. «Облачные» технологии изначально не задумывались как средство решения проблем информационной безопасности, и суть их технологии совсем в других преимуществах.

BG: Очень многие дата-центры расположены не в России. Даже так — почти 100% данных российских компаний будет храниться за рубежом, на серверах Европы и США. Это достоинство, недостаток или не имеет никакого значения?

А. Г.: Каждая компания решает это для себя сама. В целом сложившаяся ситуация обусловлена наличием на Западе большого количества подобных сервисов, обладающих значительным опытом, предлагающих весьма существенную финансовую экономию и развитую технологическую базу как в плане каналов связи, так и используемого оборудования. Это достоинства. К недостаткам можно отнести так называемые трансграничные проблемы, когда возникают вопросы юридического характера к хранящимся там данным.

BG: Новый продукт «Лаборатории Касперского» Kaspersky Internet Security 2012 сочетает в себе классическую защиту и облачные технологии — о чем речь?

А. Г.: Сегодня новые вредоносные программы появляются с огромной скоростью — примерно 35 тыс. каждый день. При этом компьютер может использоваться в разных условиях: иногда он подключен к интернету и активно применяется для всевозможных онлайн-действий (шопинг, интернет-банкинг, общение в социальных сетях, игры), поэтому должен быть надежно защищен от интернет-угроз различных типов. В других же ситуациях соединение с интернетом отсутствует и компьютер является уязвимым для вредоносных программ, распространяющихся, например, через USB-флешки. Именно поэтому решение для защиты пользователей от всех типов современных интернет-угроз должно сочетать традиционные антивирусные методы и новейшие «облачные» технологии, то есть быть гибридным.

В продуктах «Лаборатории Касперского» «облачная» защита реализована в Kaspersky Security Network, специальной сети, мгновенно доставляющей на централизованные серверы информацию обо всех попытках заражения и подозрительного поведения на миллионах пользовательских машин. Стоит новой вредоносной программе попытаться заразить хотя бы один компьютер, защищенный продуктами «Лаборатории Касперского», как информация о ней и ее действиях поступает в исследовательский центр. Система немедленно вырабатывает соответствующие средства защиты (сигнатуры, шаблоны нежелательного поведения, списки адресов вредоносных сайтов) и через KSN доставляет их на компьютеры остальных пользователей, избавляя от необходимости проводить ресурсоемкий анализ, минимизируя ложные срабатывания и защищая от самых последних угроз еще до выхода соответствующих сигнатур. Однако компьютер защищен даже в том случае, если доступ к интернету, а значит, и связь с «облаком» отсутствуют. Это обеспечивается традиционными антивирусными технологиями. Локальные проактивные программы выполняют не менее важную функцию, чем «облако»: они отслеживают и анализируют все системные события, блокируют вредоносное ПО и предохраняют компьютер от угроз, приходящих не из интернета. Кроме того, именно они собирают и обрабатывают информацию о работе программ, которую затем передают в «облако», и защищают компьютер, когда интернет-соединение отсутствует. Таким образом, именно сочетание локальных и «облачных» технологий позволяет антивирусному продукту работать быстро и эффективно, обеспечивая высочайший уровень безопасности. Благодаря свойствам гибридной защиты время обнаружения и ликвидации угроз снижено до 40 секунд, а скорость выполнения некоторых операций возросла на 50% по сравнению с предыдущими версиями.

BG: Многие компании боятся того, что облачные технологии — это наркотик: однажды подсев на технологии определенного поставщика, будет практически нереально с этой иглы слезть. Это так или нет?

А. Г.: Я бы не был так категоричен. Более того, ситуация часто бывает совершенно противоположная: начав использовать «облачные» технологии, компании получают невиданную ранее свободу выбора. Смена «облачного» провайдера — это процесс гораздо более легкий, чем существующая жесткая привязка к уже построенным внутри компании системам. Перенос данных может быть осуществлен в весьма короткие сроки. Что касается «облачных» средств защиты, таких как SaaS-сервисы электронной почты или веб-фильтрации, то их смена также не требует особых затрат и времени. В области защиты «облачных» провайдеров мы будем концентрироваться на разработке систем защиты виртуальных машин в области хостинга приложений и баз данных. Крайне важным для нас является участие в разработке стандартов. Совместно с разработчиками виртуальных систем ведется работа по реализации программных средств и технологий, призванных обеспечить полноценное функционирование антивирусных систем в связке с виртуальными машинами. ■