Облака и BYOD: обеспечение безопасности

Алексей КОМАРОВ,
директор по маркетингу и продуктовому управлению, NGS Distribution

Обратная сторона технологии BYOD в контексте облаков – возникновение дополнительных рисков и общее снижение уровня обеспечиваемой безопасности. Рассмотрим основные причины этого явления, а также варианты снижения данных рисков.

Мир без периметра

Исторически компании защищали свой периметр межсетевыми экранами (FW) и системами предотвращения вторжений (IPS – Intrusion Prevention System) от внешних нарушителей, а системами защиты от несанкционированного доступа (НСД) и предотвращения утечек (DLP – Data Loss Prevantion) – от нарушителей внутренних. Такой подход на раннем этапе был вполне оправдан, поскольку данные устройства и пользователи были сконцентрированы в одном месте.

С появлением ноутбуков периметр модифицировался, пользователи стали подключаться к сети Интернет вне контролируемого пространства и по неконтролируемым каналам, однако сам принцип именно периметровой защиты не поменялся, просто удаленные пользователи стали подключаться с помощью технологий VPN, все равно оказываясь внутри контролируемой зоны. За защиту непосредственно периметра, если так можно выразиться, самого ноутбука отвечал набор средств из антивируса (AV – antivirus), локальной системы предотвращения вторжений (HIPS – Hosted IPS) и агента системы DLP.

Затем наступила эра наращивания мощности телефонов, постепенно превратившихся в многофункциональные устройства с мощными вычислительными и коммуникационными возможностями. Вполне естественно, что постепенно они стали использоваться не только для развлечения, но и для работы. Просто потому, что это удобно – просмотреть почту на телефоне или планшете, не доставая из сумки ноутбук.

Распространить на новый тип устройств прежний периметральный подход оказалось не так просто. Среди препятствующих причин – слишком большое разнообразие и слишком частая смена платформ и операционных систем, затрудняющие разработку универсальных средств защиты, а также хотя и существенные, но тем не менее ограниченные вычислительные мощности, не позволяющие установить полноценные средства защиты без снижения производительности. Закрытость архитектуры и ограниченные возможности для разработчиков запускать свои приложения с административными правами у отдельных платформ также не способствовали применению традиционных подходов. Наконец, пользователи стали активно использовать для доступа к корпоративным ресурсам свои собственные устройства, породив тот самый Bring Your Own Device (BYOD), в связи с которым для установки средств защиты и контроля на устройства пользователей возникло препятствие теперь и этического характера.

Таким образом, мобильные устройства со временем вышли за пределы контролируемой зоны, и стало очевидно, что нужны новые подходы.

Еще одним важным фактором последних лет стало массовое распространение облачных технологий, выводящих за рамки корпоративного периметра теперь уже и сами данные, доступ к которым необходимо контролировать и ограничивать. Чужие серверы, чужие каналы связи и чужой обслуживающий персонал – все это не способствует снижению рисков, несмотря на договоры и гарантии от облачного провайдера.

Совмещение облачных технологий и BYOD и вовсе породило чудовище, напрочь лишившее безопасников спокойствия. Сотрудник теперь со своего собственного устройства обращается к корпоративным данным, находящимся на сторонней площадке. Строго говоря, без принятия специальных мер в этом случае не контролируется практически ничего: ни устройство доступа, ни канал, ни сами данные.

Я подумаю об этом завтра...

Массовому распространению BYOD и облачных технологий можно сопротивляться сколь угодно долго, но де-факто их приход в корпоративный сегмент уже состоялся.

Скажем, отдел маркетинга выбирает площадку для проведения вебинаров. Решения для развертывания подобного сервиса на собственных мощностях, конечно, есть, но специализированные онлайн-сервисы гораздо удобней и функциональней. Выбор будет определяться в первую очередь соотношением цена/качество, об уровне безопасности вряд ли кто-то задумается. Привлекать к этому выбору службу безопасности с огромной долей вероятности никто не будет вовсе. Аналогичная ситуация вполне может сложиться и при подборе, например, сервисов почтовой рассылки или даже системы управления взаимоотношениями с клиентами (CRM – Customer Relationship Management).

Получается, что критичная для многих компаний информация о клиентах, партнерах и пр. оказывается вне пределов области контроля сотрудников службы безопасности, которые зачастую могут даже не знать, что соседние подразделения используют какие-то сторонние сервисы.

Похожая история и с мобильными устройствами. Удаленный доступ к корпоративным ресурсам в том или ином варианте есть у многих компаний. Для этого все чаще применяются не VPN-технологии, а веб-доступ (хорошо еще, если по протоколу SSL), причем использоваться может любое устройство с веб-браузером, тем более если в качестве метода аутентификации применяется лишь пара логин – пароль. С высокой долей вероятности данные для входа пользователь сохранит в памяти самого устройства (ведь так действительно гораздо удобнее), и тогда постороннего, так или иначе получившего телефон сотрудника, от доступа к критическим корпоративным данным будут отделять лишь четыре цифры ПИН-кода или, если пользователь беспечен, вообще ничего. При этом, с точки зрения службы безопасности, вроде бы все хорошо: пароли используются надежные, а любые попытки их подбора тут же блокируются.

Наконец, практически всегда есть некая привилегированная группа пользователей (скажем, топ-менеджмент), которая часто считает возможным ставить себя выше корпоративных правил и стандартов, банально нарушая их или требуя этого от ИТ-персонала, с тем чтобы для собственного удобства использовать любые устройства и облачные сервисы по своему усмотрению. Знает ли о таких вольностях служба безопасности – большой вопрос.

Активное использование собственных устройств и внешних облачных сервисов стало повсеместным, хотя, конечно, нельзя отрицать тот факт, что все еще встречаются «заповедные» территории компаний, где действует тотальный и строго контролируемый запрет на любые попытки нарушить периметр какими-либо современными технологиями.

Не можешь предотвратить – возглавь

В свете всего вышесказанного самым разумным представляется признание факта существования и активного применения в компании облачных сервисов и собственных мобильных устройств сотрудников и внедрение регламентов, процедур и специальных средств защиты для снижения возникающих дополнительных рисков.

В рассмотренном примере с онлайн-сервисами, которые выбирают различные подразделения компании, задачи службы безопасности можно сформулировать следующим образом:

- активное участие в выборе сервисов, чтобы экспертная оценка обеспечиваемого уровня безопасности учитывалась при финальном выборе;
- контроль и управление имеющимися учетными записями во всех используемых сервисах;
- сведение к минимуму ситуаций применения единой учетной записи от какого-либо сервиса одновременно группой сотрудников в целях сохранения возможности определить конкретных ответственных за то или иное действие;
- выявление фактов использования неодобренных сервисов (облачные файловые хранилища, онлайн-почта и пр.).

Для мобильных устройств сотрудников необходимо разработать правила по их использованию для доступа к информационным ресурсам компании для различных групп пользователей, найти компромисс между желаниями и потребностями бизнес-подразделений и топ-менеджеров и уровнем безопасности, который при этом может быть обеспечен. Кроме того, следует регулярно проводить обучение сотрудников для повышения их осведомленности: сотрудники должны понимать важность установки паролей на телефон, осознавать опасность, которая может исходить от устанавливаемых из недоверенных источников приложений, и т. д.

Приведенные организационные варианты позволят «обуздать» бесконтрольность облаков и BYOD в компании, но желательно дополнить их внедрением специализированных технических средств и решений.

Системы управления мобильными устройствами

Производители систем управления мобильными устройствами (MDM – Mobile Device Management) в рекламных материалах обычно обещают «серебряную пулю», но на практике эти решения эффективны только в случаях запрета BYOD и раздачи мобильным сотрудникам стандартизированных корпоративных устройств. MDM-системы, которая

была бы одинаково эффективна для всех современных типов устройств, просто не существует, а надеяться, что все сотрудники приобретут однотипные телефоны и планшеты, понятное дело, наивно.

Тем не менее рынок подобных решений сейчас достаточно насыщен и вполне возможно найти продукт, максимально помогающий в решении основных проблем с мобильными устройствами, хотя, конечно, в каждом конкретном случае он, скорее всего, будет свой.

VPN и проксирование

Разумным подходом с точки зрения повышения безопасности представляется организация доступа мобильных устройств в сеть Интернет через шлюз, так называемое проксирование, когда устройство подключается к серверу компании и уже через него «общается» с внешним миром. Таким образом, на устройство будет поступать только безопасный трафик, а все отправляемое с него вовне тоже проходить инспектирование. При этом возможно использование технологии VPN, чтобы канал между самим устройством и сетью компании был дополнительно зашифрован.

Основная проблема при таком подходе заключается в том, что и личный трафик с устройства пользователя будет проходить инспектирование, что сложно назвать корректным и этичным. Предоставляя пользователю возможность самостоятельно отключать проксирование, компания рискует тем, что в какой-то момент он забудет включить его снова.

Частными случаями подобного подхода являются облачный антивирус и облачная DLP, когда проксирование осуществляется не на серверы компании, а на серверы сторонних провайдеров услуг, что далеко не все компании готовы принять: не только данные передать в облака, но и саму функцию их защиты доверить посторонним организациям – такой шаг должен быть тщательно взвешен.

Классические решения

Такие приложения, как мобильные антивирусы, средства создания шифрованного контейнера и другие классические, привычные для пользователей компьютеров, средства защиты, конечно, существуют, однако их качество требует скрупулезной проверки и тестирования до принятия решения в эксплуатацию. Сложности с такими решениями уже упоминались – это недостаточная кроссплатформенность, высокая требовательность к вычислительным ресурсам и низкая функциональность для закрытых платформ. Дополнительно можно отметить трудности с централизованным управлением этими приложениями при отсутствии интеграции с MDM.

Единая платформа аутентификации

На рынке доступны решения, позволяющие централизованно осуществлять аутентификацию пользователей при их доступе к самым разным ресурсам и сервисам, а также с произвольных видов устройств. Проще говоря, сервер аутентификации располагается внутри компании, и все попытки получить доступ к тому же облачному сервису перенаправляются к этому серверу аутентификации. Таким образом, компания получает возможность контролировать доступ сотрудников к облачным сервисам, вести логирование этих событий и передавать в систему сбора и корреляций событий, в итоге повышая общую безопасность доступа к облачным приложениям.

Такие платформы, как правило, поддерживают широкий круг методов аутентификаций (от генераторов одноразовых паролей и SMS до бестокенных технологий и голосовой телефонии), что позволяет для каждого сервиса и ресурса в зависимости от степени его критичности выбрать оптимальный.

Порталы удаленного доступа

Один из подходов повышения уровня безопасности при доступе сотрудников с мобильных устройств к ресурсам компании – использование специализированных порталов, на которых осуществляется публикация внутренних ресурсов или веб-интерфейсов тех же облачных сервисов. Для доступа к любому ресурсу пользователю требуется только наличие браузера. При таком подходе к ресурсам и сервисам прямой доступ извне закрыт, а применение технологии однократного входа (SSO – Single Sign-On) позволяет администратору, например, не сообщать сотруднику реальный пароль от какого-либо облачного сервиса – для пользователя аутентификация будет осуществляться только один раз.

Упомянутая единая платформа аутентификации может использоваться для аутентификации пользователей на таком портале удаленного доступа при доступе с любого устройства тем способом, который в каждом конкретном случае будет оптимален с точки зрения соотношения удобства применения и безопасности.

Заключение

Очевидно, что облачные и мобильные технологии пришли «всерьез и надолго». Прогресс не остановить, поэтому задумываться о безопасном использовании этих технологий нужно уже сейчас, несмотря на то что большая часть имеющихся на рынке решений, конечно, далеко не совершенна. Вместе с тем, компании, предпочитающие подождать, пока рынок «перебурлит» и из пены появится сверкающий в лучах солнца корабль идеального решения, рискуют просто не дожить до этого светлого дня, пострадав от серьезной утечки или взлома либо их череды и сочетаний. ■