Безопасный BYOD

Обзор проблем и технологий ИБ при поддержке концепции BYOD в компаниях.

Владимир Бенгин – руководитель направления внедрения решений информационной безопасности, группа "Астерос".

Введение

Концепция BYOD (bring your own device) в настоящее время становится одной из самых популярных в мире. В России это направление также начинает активно продвигаться. Однако весьма часто данное понятие неправомерно используется для описания более узкого круга задач, из чего следуют и неверные выводы о технологиях защиты BYOD. К примеру, BYOD часто понимают как некую технологию использования собственных смартфонов для работы с корпоративной почтой. Но BYOD – это не обязательно смартфон, это может быть и ноутбук, и не обязательно удаленно, может быть и внутри корпоративной сети. Лучшим описанием концепции BYOD является ее девиз: "Сотрудник имеет возможность работать с корпоративными ресурсами вне зависимости от места, времени или устройства, с которого он решил работать". Это может быть как личный смартфон или планшет, так и ноутбук.

Пока не столь популярная в российских компаниях, на Западе концепция полного отказа от стационарного рабочего места – это новый виток в развитии корпоративной культуры, во многом основанной на доверии. В зависимости от должности специалиста работодателем выделяется бюджет, на который тот вправе самостоятельно выбрать подходящий для себя ноутбук, планшет, смартфон. При данном подходе сотрудник сам становится "администратором" своих устройств. Он вправе устанавливать на них собственные приложения, может как принести их в компанию и подключить к локальной корпоративной сети, так и использовать в публичных местах (например, в кафе с открытым Wi-Fi).

Этот подход вызывает много споров из-за корпоративных политик безопасности. Но стоит помнить, что методы и средства защиты активно развиваются, давая возможность реализовать необходимый и адекватный уровень защиты такой "паутины", ничем не уступающей обычным локальным сетям.

Технологии ИБ для поддержки BYOD

Проблемы

Среди основных проблем ИБ, на которые нужно обратить внимание, выделяются следующие.

1. Пользователь использует устройство в сетях открытого доступа. Помимо прямой атаки, это чревато тем, что злоумышленники будут отслеживать весь трафик (или даже видоизменять передающийся поток от пользователя, реализуя одну из наиболее опасных угроз – Man in the Middle).

2. Устройство может быть потеряно или украдено со всей конфиденциальной информацией.

3. Конечный пользователь, являющийся администратором своего устройства, может установить и удалить любое ПО.

4. Концепция BYOD подразумевает наличие целого "парка" устройств под управлением: MAC OS, Windows Vista/7/8, Apple IOS, Android OS, Windows phone и т.д., что значительно усложняет процесс централизованного управления. При этом уровень предоставляемого доступа к ресурсам зависит от большого числа входящих условий: статуса присутствия сотрудника на работе, места, времени и типа устройства, с которого осуществляется доступ.

Методы и способы защиты

Ключ шифрования

Основным методом защиты информации в открытых сетях является шифрование, де-факто ставшее стандартом. Но не каждое шифрование есть панацея. Необходимо обращать внимание на используемые алгоритмы и длину ключей. Генерация первичного ключа только на основе пароля пользователя является небезопасной. Злоумышленник может "представиться" системе дружественным сервером и в итоге вскрыть пользовательский пароль (или необходимый для аутентификации кэш).

Более безопасно использовать сертификаты. На опыте "Астерос" можно утверждать, что решения вендоров, использующие стандартные алгоритмы и протоколы, более надежны, чем собственные разработки компаний-заказчиков. Современные мобильные устройства достаточно производительны, чтобы поддерживать шифрование, к примеру, на основе AES-256 с длиной ключа 1024 и выше.

Однако это не единственное условие подключения пользователей к корпоративным ресурсам из внешней среды. Рабочая станция сотрудника, находясь внутри компании, защищена межсетевыми экранами, системами предотвращения вторжения, сетевыми антивирусами и т.д. Устройство "вне компании" всего этого лишено.

Внедрив вредоносный код, злоумышленник может заменить сертификат сервера доступа и получить логин и пароль пользователя, как только тот попытается подключиться к корпоративной сети. Если в компании развита практика BYOD, стоит подумать о том, какие политики безопасности и средства защиты использовать на устройствах своих сотрудников. И, главное, как, чтобы не нарушать границы "личного пространства". Что касается средств защиты, сегодня все ведущие вендоры уже имеют комплексные решения по защите клиентских станций как для традиционного семейства Windows, так и других ОС мобильных устройств.

Для шифрования данных необходимо специализированное ПО, позволяющее иметь крипто-контейнеры и контролировать другие приложения, осуществляющие доступ к контейнеру. Если планируется использовать крипто-контейнеры, необходимо задуматься о MDM-решениях (MobileDeviceManagement), которые позволяют централизованно управлять мобильными устройствами.

Данные вне поля действия

Чтобы защитить информационные активы при утрате устройства, можно хранить все конфиденциальные данные внутри корпоративной сети. Работу с ними организовать только при включенном удаленном соединении. Таким образом, при потере девайса данные не пострадают. При таком подходе само устройство "выигрывает" в производительности, так как нет необходимости постоянно шифровать хранимую на нем информацию. Но у такого подхода есть и минус: сотрудник не сможет работать в автономном режиме.

Удобная аутентификация

Возможно и использование методов многофакторной аутентификации, которая значительно повышает безопасность. Однако есть ограничения ее использования в разрезе концепции BOYD. К примеру, один из самых надежных и популярных методов двухфакторной аутентификации – использование пары "пароль и USB-ключ" – нельзя использовать на большинстве планшетов и смартфонов в силу отсутствия USB-разъема. Зато этот факт можно применять в качестве метода разграничения доступа: для ноутбуков предоставлять более высокие права доступа на основе пары "USB-ключ – пароль",

для смартфонов и планшетов, не имеющих возможности использовать токены, применить другие методы двухфакторной аутентификации. Например, биометрические (черты лица, голос и т.д.), одноразовые пароли (брелоки, смарт-карты, специализированное ПО).

При этом важно обратить внимание на сохранение удобства использования мобильного устройства после внедрения на нем всех необходимых средств защиты. В этом разрезе одна из главных проблем – использование на одном устройстве нескольких паролей. Представьте, что сотрудник должен сначала снять блокировку (пароль № 1), затем подключиться к корпоративной сети (пароль № 2), начать использовать необходимый для работы сервис (пароль № 3). Таких сценариев можно придумать множество и все они будут казаться некомфортными для конечного пользователя в силу большого количества рутинных операций. Помочь в этой ситуации может SSO (SingleSign-On, технология единого входа). К примеру, можно отдать на откуп владельцу политику по установке пароля разблокировки устройства. А для использования корпоративных приложений необходимо будет ввести единый пароль, который, впоследствии, система будет использовать для нескольких аутентификаций пользователя в режиме SSO.

Под контролем NAC

Один из важных аспектов безопасности при концепции BYOD – контроль за конфигурацией устройства. Сейчас на рынке представлено большое число программных продуктов, не позволяющих пользователю удалить их даже в том случае, если пользователь имеет права локального администратора. Но эта защита неидеальна: пользователь всегда может отформатировать диск и установить систему снова или сбросить настройки своего мобильного устройства до заводских. После этого он, конечно, не сможет подключиться к корпоративной сети удаленно, но, что если он принесет такое устройство в компанию? Как определить, не удалил ли сотрудник антивирус со своего устройства, считая его наличие необязательным?

Для этих целей идеальна технология NAC (Network Access Control – контроль доступа к сети). Она основана на протоколе 802.1x и поддерживается многими производителями сетевого оборудования. NAC контролирует оконечные подключения к сети компании. Каждый коммутатор компании находится под управлением центрального сервера, и в момент появления активности на одном из портов передает информацию с подключаемого устройства прежде, чем новое подключение получит доступ в сеть. На основе полученных данных центральный сервер принимает решение, может ли устройство получить доступ к сети и к какой именно. Информация, которую отправляет смартфон или планшет, может быть совершенно разной – от аутентификационных данных до отчета об установленном ПО, значения в ветках реестра и актуальности антивирусных баз. Для лучшего понимания, как это работает, приведем несколько примеров настроенной системы NAC.

1. *Подключение к сети принтера или телефона*. Все, что о них можно узнать, – это MAC-адрес. На его основе сервер может определить производителя и тип устройства, и, следовательно, сразу же перевести данный порт в режим работы с принтерами или телефонами, разрешив доступ устройству только для необходимых сервисов.

2. *Подключение к сети рабочей станции пользователя*. После аутентификации пользователя и проверки сертификата хоста система понимает, что это рабочий хост пользователя (работающего по концепции BYOD). Далее сервер запрашивает проверку системы на наличие антивируса и актуальности его вирусных баз, а также наличия всех необходимых программ в соответствии с политикой компании (к примеру, DLP-агент). Только после успешного прохождения такой процедуры пользователь получает полный доступ. Если хотя бы один из параметров не выполняется, устройство может быть переведено в карантинную зону.

3. *Подключение к сети мобильного устройства сотрудника*. После стандартной аутентификации необходимо проверить устройство на соответствие требованиям политики ИБ, так же как и с рабочей машиной. Но здесь серверу NAC придется запросить информацию у MDM-решения и, получив положительный ответ, предоставить доступ в сеть сотруднику.

4. *Подключение к сети гостевого ноутбука*. Wi-Fi-контроллер, как и все проводные коммутаторы, подключен к единому серверу NAC. При подключении к открытой сети, контроллер перенаправляет пользователя на гостевой портал, где после регистрации пользователю сразу предоставляется временный сертификат для защищенного соединения Wi-Fi, либо предлагается пройти проверку хоста.

Необходимо понимать, что внедрение NAC является одной из самых сложных задач. В случае, когда рассматривается использование смартфонов и планшетов вне компании, достаточно MDM-решения, а при необходимости только удаленного подключения мобильных устройств к конкретным ресурсам сети (без хранения конфиденциальной информации) достаточно будет VPN-клиента и хорошего антивируса с МЭ.

Однако, если планируется полноценный переход к концепции BYOD, необходимо использовать все вышеперечисленные технологии совместно с NAC.

Владимир Бенгин,
группа "Астерос".

McAfee: идентификация на основе распознавания речи и черт лица

Май 2013 г. – McAfee представила новую программную разработку McAfee® LiveSafe™ – кроссплатформенный сервис для защиты данных и персональной информации пользователей, а также всех их устройств, разработанный на основе технологии распознавания голоса и черт лица.

Согласно исследованию McAfee, практически 90% пользователей во всем мире используют более одного цифрового устройства, и более 60% пользователей используют три и более устройств. Кроме того, исследование выявило, что более 50% пользователей используют эти устройства для личных целей как минимум 15 часов в неделю, или 2 часа в день. В более чем 40% семей используются пять или более устройств с выходом в интернет, что значительно повышает риск быть подвергнутым онлайн-угрозам.

McAfee LiveSafe реализует комплексный подход к обеспечению безопасности, предоставляя пользователям простую в использовании веб-консоль для централизованного управления защитой всех ПК, планшетов и смартфонов. Для повышения уровня безопасности McAfee LiveSafe предлагает специальное облачное хранилище McAfee Personal Locker, которое использует технологии распознавания речи и черт лица для идентификации пользователей, чтобы они могли надежно хранить свои наиболее важные документы, включая финансовые документы, копии водительских прав и паспортов. Новый сервис также предоставляет пользователям возможность легко и с высоким уровнем защиты управлять паролями и автоматически заходить в свои учетные записи в сети интернет, используя различные устройства.

McAfee LiveSafe обеспечивает надежную защиту за счет использования преимуществ технологий, применяемых в новейших процессорах Intel®. McAfee LiveSafe включает сервис McAfee Anti-Theft, который использует технологию Intel® Anti-Theft для защиты персональной информации пользователей и их устройств в случае потери или кражи (устройство блокируется дистанционно). McAfee LiveSafe также поддерживает технологию Intel® Identity Protection Technology (IPT), которая представляет собой устойчивое к взлому решение для проверки подлинности, реализованное на аппаратном уровне. С помощью технологии Intel IPT и технологии распознавания голоса и черт лица пользователи McAfee LiveSafe , использующие устройства Ultrabook™ на базе процессоров Intel Core™ 4-го поколения, смогут воспользоваться всеми преимуществами этого комплексного решения, обеспечивающего надежный уровень защиты. Кроме того, владельцы Ultrabook смогут использовать сервис McAfee Security Advisor для того, чтобы получить ответы на все вопросы, связанные с защитой личной информации.

С июля 2013 г. McAfee LiveSafe будет доступен в розничной торговле по цене 799 руб. за годовую подписку при покупке нового ПК, смартфона или планшета и по цене 2559 руб. за годовую подписку для владельцев существующих ПК и планшетов. McAfee LiveSafe будет устанавливаться на устройствах Ultrabook™ и ПК компании Dell с 9 июня 2013 г.