КОРПОРАТИВНАЯ МОБИЛЬНОСТЬ
и безопасность бизнеса

М.Лукин, руководитель направления ИБ компании CTI

В статье рассматривается один из подходов для успешной реализации концепции BYOD на предприятии. Данный подход позволяет автоматизировать интеграцию личных пользовательских мобильных устройств в ИТ-инфраструктуру предприятия и при этом обеспечивает снижение рисков информационной безопасности. В статье описаны основные шаги и варианты решения, которые позволят успешно реализовать задачу корпоративной мобильности.

Использование персональных мобильных устройств для работы с корпоративными ресурсами, в том числе электронной почтой и телефонией, для просмотра видео и передачи сообщений становится стандартом де-факто для современного бизнеса. По прогнозам Gartner, к 2016 году 40% работников всего мира будут трудиться удаленно, из них 67% будут использовать для работы смартфоны. Использование личных мобильных устройств предоставляет бизнесу дополнительный потенциал производительности и обеспечивает эффективные бизнес-коммуникации. Возможность получить доступ к электронной почте, телефонии, корпоративным ресурсам из любого места с личного мобильного устройства позволяет повысить эффективность сотрудничества с коллегами и более оперативно обрабатывать запросы клиентов.

Однако не всегда очевидно, как эффективно интегрировать пользовательские устройства в ИТ-инфраструктуру и при этом обеспечить высокий уровень управляемости и защищенности. Учитывая опыт компании CTI и рекомендации производителей решений для корпоративной мобильности, можно определить основные меры, необходимые для реализации концепции BYOD (Bring Your Own Device).

Разработка мобильной стратегии

Разработка мобильной стратегии – залог успешного внедрения концепции BYOD. Мобильная стратегия может быть одной из частных корпоративных политик информационной безопасности (ИБ). Она позволяет повысить управляемость и снизить риски для ИБ. В рамках мобильной политики сопоставляются выгоды от внедрения BYOD с рисками ИБ и затратами на реализацию политики. Есть ряд основных моментов, на которые стоит обратить внимание при разработке мобильной политики.

Идентификация бизнес-целей позволяет ответить на вопрос о предоставлении доступа к ИТ-ресурсам с персональных мобильных устройств. Например, использование корпоративных унифицированных коммуникаций дает возможность значительно оптимизировать затраты на связь, повысить эффективность совместной работы и общую производительность труда. Организация гостевого доступа к электронной почте, корпоративным приложениям и телефонии,

эффективная работа консультантов – эти и другие бизнес-задачи могут лечь в основу мобильной стратегии.

Определение типов поддерживаемых устройств и ОС может значительно упростить процесс реализации концепции BYOD и ее дальнейшей поддержки. Для того чтобы определить, каким типам устройств можно предоставлять доступ к корпоративным ресурсам, нужно провести тестирование работы корпоративных приложений на устройстве, а также проверку средств контроля и управления мобильными устройствами.

На этапе разработки матрицы доступа необходимо сопоставить права пользователей и список доступных корпоративных ресурсов. Уровень доступа может зависеть от типа пользовательского устройства и его состояния.

Реализация мобильной стратегии

Для реализации мобильной стратегии необходимо применение технических решений, направленных на контроль сетевого доступа, т.е предоставления различного уровня доступа в зависимости от типа устройства, установленных на нем программ и обновлений, места и способа подключения. Для реализации мобильной стратегии может использоваться решение EMM (Enterprise Mobility Management) компании AirWatch.

Для контроля политик и предоставления различного уровня доступа к корпоративной инфраструктуре в зависимости от типа устройства, его состояния и места подключения могут применяться решения класса NAC (Network Access Control). В рамках отраслевого дизайна предлагается использовать решение Cisco ISE (Identity Service Engine), которое уже успело хорошо зарекомендовать себя на рынке. В комплексе эти решения обеспечивают централизованное управление мобильными устройствами, контроль доступа и реализацию корпоративных политик ИБ на мобильном рабочем месте.

Основные решения

Решение для централизованного управления Cisco ISE позволяет определять политики ИБ и эффективно управлять ими в масштабе всей организации. ISE решает задачу поддержки устройств с помощью политики контроля доступа в корпоративной сети. Оно различает корпоративные и личные пользовательские устройства и обеспечивает ИБ всей организации при помощи средств контроля доступа, реализованных на уровне сети. Высокий уровень безопасности достигается при помощи аутентификации по протоколу IEEE 802.1x, совместно с которым возможно расширение функционала решения при помощи механизмов профилирования и оценки состояния подключаемых клиентов по множеству критериев. Кроме устройств, которые поддерживают протокол 802.1x, ISE позволяет аутентифицировать устройства по протоколу MAB (MAC Authentication Bypass). Это решает проблему безопасного подключения для принтеров, IP-камер, систем бесперебойного питания, терминалов, станций видеоконференц-связи, турникетов и других устройств.

Решение по корпоративной мобильности AirWatch EMM (Enterprise Mobility Management) состоит из четырех модулей:

- Mobile Device Management;
- Mobile Application Management;
- Mobile Email Management;
- Mobile Content Management.

Модуль Mobile Device Management (MDM) обеспечивает централизованное управление мобильными устройствам и реализацию корпоративных политик ИБ на мобильном рабочем месте. Он позволяет снабдить централизованное управление приложениями (включая инвентаризацию и защиту от мошеннических приложений, процесс управления обновлениями), организовать защищенный доступ к корпоративным сервисам, в случае необходимости выполнить удаленную блокировку и полную очистку устройства. MDM отвечает за управление мобильным устройством, автоматизацию настроек, реализацию различных типов конфигураций (профилей) мобильного устройства, реализацию политики ИБ для мобильного развертывания, карантин устройств и управление в индивидуальном порядке, автоматизацию ИТ- и рабочих процессов и информирование обо всех мобильных ресурсах и политиках.

Модуль Mobile Application Management (MAM) позволяет создавать корпоративные каталоги приложений, централизованно управлять установкой приложений и обновлений на мобильных устройствах. MAM дает возможность реализовывать политики "запрещенных" и "разрешенных" приложений. В его задачи входит управление корпоративными, приобретенными приложениями и приложениями общего пользования, интеграция с App Store, Google Play, Amazon, создание пользовательского каталога корпоративных приложений (КПП), создание продвинутых корпоративных приложений с использованием инструментов разработчика, просмотр информации с перечнем приложений, их версий и соответствий, включение функции единого входа в систему для корпоративных приложений, а также проверка внутренних и общедоступных приложений на предмет содержания вредоносного кода.

Модуль Mobile E-mail Mangement (MEM) обеспечивает управление почтовыми сервисами на мобильном устройстве и реализацию политик безопасности при использовании электронной почты с мобильного устройства. В его задачи входит интеграция с инфраструктурой корпоративной электронной почты, автоматизация настроек параметров и учетных данных, блокирование доступа к электронной почте на основе данных о марке, модели или операционной системе устройства, установка, удаление или управление сертификатами электронной почты, шифрование вложений электронной почты для предотвращения потери данных, уничтожение информации во вложениях, отправленных со взломанных устройств, а также мониторинг активности пользования корпоративной электронной почтой.

Модуль Mobile Content Management (MCM) позволяет организовать защищенный доступ с мобильного устройства к корпоративным ресурсам. В его задачи входит доступ к файловым хранилищам и корпоративным порталам, отправление корпоративных документов через AirWatch SCL (Secure Content Locker), разрешение двусторонней синхронизации ПК и мобильного устройства через AirWatch Sync, создание корпоративного контейнера для документов, интеграция с хранилищем информации в облаке или на собственном оборудовании, обеспечение многофакторной аутентификации пользователей, а также управление правами доступа пользователя и настройками конфиденциальности файла.

BYOD внедряется повсеместно и останется трендом ближайших лет. Это удобно сотрудникам и выгодно бизнесу. Если сотрудник постоянно на связи, читает почту дома и в машине, то уделяет своим должностным обязанностям больше времени по сравнению с работой в офисе по графику. Внедрение IP-телефонии и ее использование сотрудниками на своих мобильных устройствах позволяет работодателю значительно сократить затраты на корпоративную связь. В том или ином виде во многих организациях уже применяется концепция BYOD. Вопрос лишь в том, планирует ли организация сделать этот процесс управляемым или пустить его на самотек. Если организация планирует управлять этим процессом, то разработка мобильной стратегии и применение технических средств, обеспечивающих управление мобильными устройствами, позволяет внедрить BYOD оперативно и без ощутимых дополнительных затрат. ■