УДК 004.05

БЕЗОПАСНОСТЬ ИСПОЛЬЗОВАНИЯ МОБИЛЬНЫХ УСТРОЙСТВ

Тарановская Алина Руслановна, Коршак Татьяна Петровна
Государственный ВУЗ «Национальный горный университет»

В работе рассмотрен вариант безопасного использования мобильных устройств - концепция Mobile Device Management (MDM), которая позволит централизованно удаленно управлять конфигурациями мобильного устройства и отдельных его функций, также управлять программным обеспечением устройства и обеспечивать безопасность его использования.

Ключевые слова - Mobile Device Management (MDM); мобильность; обеспечение безопасности.

ВСТУПЛЕНИЕ

Повышение эффективности бизнес-процессов является важнейшим конкурентным преимуществом в любом виде бизнеса. Одним из способов такого повышения является использование мобильных устройств в работе, в результате чего ключевые сотрудники компании перестают быть привязанными к своему рабочему месту. Использование таких устройств имеет ряд преимуществ:

Первое из них - это новая, в том числе с точки зрения безопасности, архитектура, отличная от привычной Intel x86.

Второе - это высокая скорость перехода мобильных устройств из одной среды передачи информации в другую. Например, смартфон с легкостью меняет подключение по Wi-Fi на 3G-связь. Более того, не исключена возможность "гладкого" перехода между режимами передачи во время одной сессии.

Третье - наличие отдельного класса специализированных ОС для мобильных устройств. Сегодня существует большое разнообразие как видов, так и подвидов таких ОС. Они часто обновляются, причем нередко обновления включают изменения ядра (например, ОС Android).

Четвертое, вытекающее из названия, - это мобильность. Причем не просто возможность физического переноса прибора. Современная мобильность подразумевает автономность и свободу от ограничений по времени, месту, способу доступа к необходимой информации, средствам связи и приложениям.

При этом в первую очередь встает вопрос обеспечения безопасности.

Быстрое и повсеместное развитие мобильных технологий - одна из ключевых мировых тенденций современного IT-рынка. Тем не менее, использование таких технологий тесно связано с высокой степенью информационных рисков и необходимостью соответствия требованиям и нормативам по обеспечению информационной безопасности.

Использование новых технологий влечет за собой появление новых рисков:

- утечка конфиденциальной информации при использовании мобильных устройств (в результате утери или кражи, заражения устройства вредоносным ПО);
- использование мобильных устройств для осуществления несанкционированного доступа к ресурсам компании.

Компания, принявшая решение об использовании мобильных устройств, должна оценить эти риски и предусмотреть механизм, позволяющий снизить их до приемлемого уровня. Таким механизмом может стать система обеспечения безопасности мобильных устройств. Она представляет собой комплексное решение, обеспечивающее оптимальный уровень ИБ за счет организационных мер, технических средств и обучения пользователей.

ОРГАНИЗАЦИОННЫЕ МЕРЫ

Первым шагом по обеспечению безопасности мобильных устройств должно стать появление документа, который определяет основные положения их использования и формулирует цели использования мобильных устройств.

Такие требования могут быть собраны в отдельный документ (например, "Политика защиты мобильных устройств") либо внесены в уже существующие частные ИБ- и IT-политики компании.

ТЕХНИЧЕСКИЕ МЕРЫ

Помимо организационных, необходимы меры, обеспечивающие техническую реализацию и контроль выполнения требований. Основой таких мер является решение класса Mobile Device Management (MDM), которое (в зависимости от своего типа и типа устройства) позволяет обеспечить:

- централизованное удаленное управление конфигурациями мобильного устройства:

1. управление использованием отдельных функций устройства (Bluetooth, Wi-Fi, IrDA, камеры);
2. управление встроенными механизмами защиты мобильного устройства (аутентификации, криптографической защиты);
3. управление программным обеспечением устройства;

- удаленное уничтожение данных с мобильного устройства;
- определение местонахождения устройства;
- хранение и обработку всей информации компании в криптографическом контейнере (являющемся частью MDM-клиента), благодаря чему обеспечивается функционал Mobile DLP.

В зависимости от актуальных рисков использования мобильных устройств может потребоваться дополнительно использовать:

- средства антивирусной защиты;
- средства построения защищенных каналов связи;
- средства контроля и ограничения доступа к ресурсам ЛВС компании на основании контекста доступа и профилей устройств.

РАБОТА С ПОЛЬЗОВАТЕЛЯМИ

По статистике, самым слабым звеном в системе защиты информации является человек. Поэтому важно доводить до работников основные правила безопасного использования мобильных устройств и разъяснять их. Процесс обеспечения осведомленности работников содержит:

- вводный инструктаж по вопросам обеспечения ИБ;
- проверочное тестирование по вопросам безопасного использования мобильных устройств, проводимое, например, в рамках ежегодной аттестации работника.

ВЫВОДЫ

Современный бизнес требует наличие высокой доступности своих сотрудников и своих ресурсов. Обеспечение доступа с любых устройств – ключевая мировая тенденция современного IT-рынка. Достижение баланса между мобильностью и безопасностью - непростая задача. Мобильная технология делает информацию более доступной, но в то же время трудно контролировать мобильный доступ, остающийся вне структуры ИТ-управления организации. Концепция MDM сочетает в себе гибкость мобильных устройств с «железной» безопасностью. MDM повышает безопасность удаленного доступа, усиливая отдельные инструменты контроля и политики доступа, связанные с приложениями, идентификацией пользователей и состоянием используемых устройств.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. The World Wide Web Consortium (W3C) / Способ доступа: URL: http://www.air-watch.com/solutions/mobile-device-management/. - «Управление мобильным устройством»

2. Д. М. Михайлов, И. Ю. Жуков. Защита мобильных телефонов от атак, 2011.- 130 с.

3. The World Wide Web Consortium (W3C) / Способ доступа: URL: http://www.itsec.ru/articles2/mobile-security/obespechenie-ib-korporativnyh-mobilnyh-ustroystv. - Журнал "Information Security/ Информационная безопасность" #3,201. -«Обеспечение ИБ корпоративных мобильных устройств»

4. The World Wide Web Consortium (W3C) / Способ доступа: URL: http://www.itsec.ru/articles2/mobile-security/bezopasnost-mobilnosti-ili-mobilnost-bezopasnosti?. - Журнал "Information Security/ Информационная безопасность" #4, 2012. -«Средства защиты информации для мобильных платформ»