Анализ угроз безопасности при доступе к корпоративным ресурсам с мобильных устройств

Василенков Александр Сергеевич,
ведущий менеджер отдела научных исследований и развития продуктов ОАО «ИнфоТеКС»

Говоря о переносе бизнес-процессов в «облако», мы неминуемо подразумеваем возможность доступа к корпоративным ресурсам с мобильных устройств. Именно здесь, на сегодняшний момент, сосредоточены основные угрозы безопасности и возникает множество нерешенных вопросов.

Мобильное устройство сегодня - это больше чем полноценный узел сети, на нем множество сетевых интерфейсов, оно всегда онлайн, при этом оно синхронизируется с персональными компьютерами, содержит деньги на борту (сотовый оператор, ДБО, магазины приложений), содержит сервисы геопозиционирования.

При этом мобильное устройство - это менее защищенный узел сети, из-за ограничений по питанию и, следовательно, экономией на мониторинге безопасности, непрозрачным содержимом файловой системы, бесконтрольным доступом к правам суперпользователя и доступности интерфейсов съема информации.

При всех этих ограничениях, мобильное устройство еще и по разному позиционируется пользователями: для кого-то смартфон – это полноценный компьютер, а для кого-то просто телефон, при этом функционал смартфона в обоих случаях одинаков, недаром его назвали умный (smart) телефон.

Основой безопасности для таких устройств должна служить операционная система, но если взглянуть на отчеты аналитических агентств, видно, что операционные системы сегодня не всегда готовы выполнить на 100% задачу защиты пользовательских данных, а зачастую мы сами передаем их неизвестным облачным сервисам (iCloud, Amazon Cloud, Gmail и т.д.).

И даже если вы не пользуетесь облачными сервисами, всегда есть вероятность заразить свой смартфон или планшет трояном, который незаметно для вас будет «вытягивать» вашу ценную информацию и передавать злоумышленнику. Часто мы сами ставим вредоносное ПО при установке новых приложений, даже не подозревая об этом,

например кейлоггер распространяемый CarrierIQ был добровольно установлен более 1 000 000 (!!!) из официального магазина приложений.

Каким же образом обеспечить защиту мобильного устройства? Как получить защищенный доступ к корпоративным ресурсам и не беспокоиться за их сохранность на устройстве?

Компания «ИнфоТеКС» предлагает качественные сертифицированные решения для защиты мобильных платформ и удаленного доступа к корпоративным сетям.

Как часто мы оказываемся в ситуации, когда, будучи в командировке или вдалеке от офиса, необходимы документы, доступ к которым, в угоду политикам безопасности, можно получить только с рабочего места на территории офиса или своего кабинета. Вспомните, как много решений из-за этого приходится откладывать, как много свободного времени терять, в ожидании рейса самолета или в командировке. Решить эту проблему помогут программные продукты ViPNet Client iOS и ViPNet Client Android.

ViPNet Client Android это приложение, работающее под управлением операционной системы Android, предназначенное для обеспечения защиты мобильных устройств от сетевых атак, и, позволяющее обеспечить доступ посредством защищенного технологиями ViPNet VPN туннеля, к защищенным ресурсам корпоративной сети. ViPNet Client Android после установки на мобильное устройство перехватывает любой IP трафик, обеспечивая его прозрачное шифрование. После активации защитных функций ViPNet Client Android, доступ к открытым ресурсам Интернет возможен только с использованием защищенных корпоративных proxy-серверов, доступных через VPN туннель. Этим обеспечивается эффективная многоуровневая защита мобильного устройства – антивирусная защита и контентная фильтрация, причем без установки дополнительного программного обеспечения на каждое мобильное устройство, что немаловажно, учитывая ограниченные возможности автономной работы мобильных устройств. Для управления функциями ViPNet Client Android используется графический интерфейс, дизайн которого выполнен в стандартах операционной системы Android.

ViPNet Client iOS - приложение аналогичное по своим характеристикам Client Android, но предназначенное для устройств функционирующих под управлением ОС iOS.