Мобильные устройства в организации: контроль и аналитика

СЕРГЕЙ НЕНАШЕВ,
руководитель отдела,
НТЦ «Вулкан»

ГРИГОРИЙ ВАСИЛЬЕВ,
менеджер по продуктам,
НИИ СОКБ

Текст: Григорий Васильев, НИИ СОКБ
Сергей Ненашев, НТЦ «Вулкан»

...Итак, мы обеспечили защиту от утечек в рамках корпоративной локальной сети и удовлетворенно отступили на шаг, чтобы полюбоваться результатом кропотливой работы. Но стоит оторвать взгляд от привычной нам инфраструктуры организации и посмотреть на проблему чуть шире, как мы увидим, что есть повод вновь засучить рукава. Информация, которую мы так тщательно защищаем, бесконтрольно циркулирует между мобильными устройствами, может уйти с них в нежелательные руки в виде письма, MMS или быть утерянной вместе со смартфоном или планшетом.

БЕСКОНТРОЛЬНЫЕ МОБИЛЬНЫЕ УСТРОЙСТВА – ЧЕМ ОНИ ГРОЗЯТ?

Вовлечение в бизнес-процессы смартфонов и планшетов – одна из основных тенденций ИТ-индустрии. Сначала топ-менеджеры, а за ними и рядовые сотрудники оценили удобство работы на планшетах, возможность чтения корпоративной электронной почты на смартфоне, доступ к корпоративному порталу из любой точки мира. Однако интеграция мобильных устройств в корпоративную среду – это не только новые возможности, но и новые угрозы. И, к сожалению, сегодня они недооцениваются. Современный смартфон может стать мощным орудием в руках злоумышленников. Чтобы сделать и переслать фотографии документов, данных и паролей на мониторах коллег, диктофонные записи, достаточно нескольких нажатий кнопок.

Давно канули в Лету времена, когда мобильных антивирусов было больше, чем вредоносных программ. Только за II квартал 2012 года Лаборатория Касперского зафиксировала более 14 900 новых вирусов под ОС «Android». Почти половина из них является троянами, нацеленными на кражу данных с телефона. Особую опасность представляют «банковские» трояны, открывающие злоумышленникам доступ к расчетным счетам или позволяющие перехватывать SMS с кодами подтверждения финансовых операций.

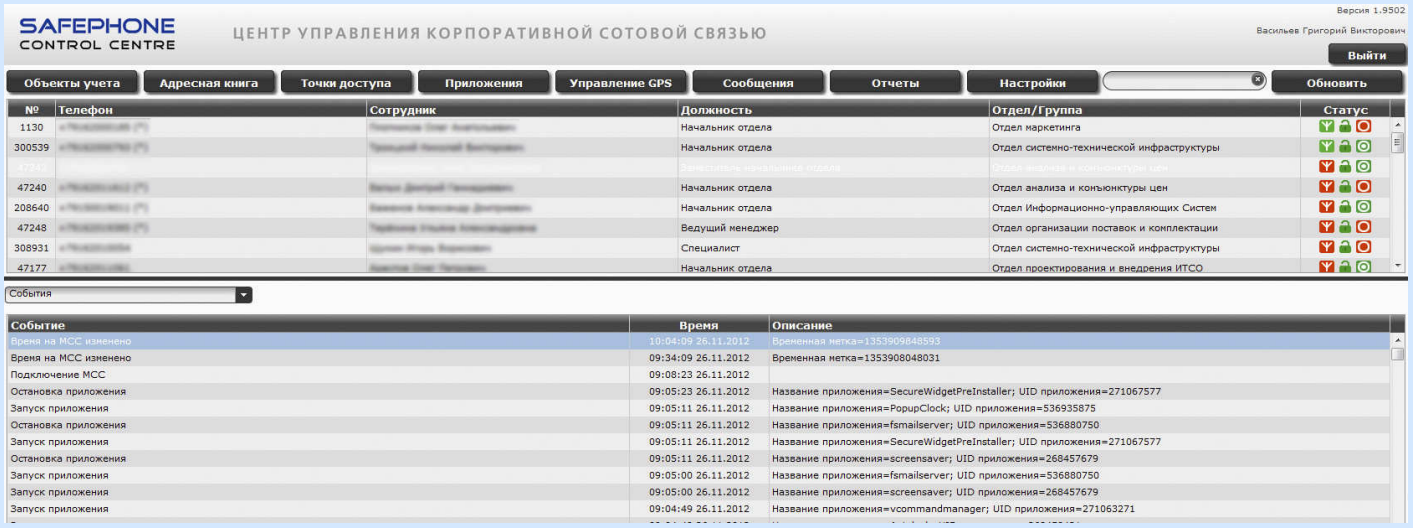
Мобильные устройства, используемые в организации, могут стать непосредственным источником утечки корпоративной конфиденциальной информации. Здесь наиболее эффективным инструментом хакера является скрытная установка на смартфон вредоносного программного обеспечения. Троянская программа может передать учетные данные сотрудника, предоставить доступ злоумышленнику к корпоративным приложениям для смартфонов и планшетов. Мобильные трояны позволяют незаметно для пользователя осуществлять мониторинг его звонков и SMS, фиксировать его географическое положение. Трояны могут записывать переговоры, в любой момент включать микрофон или фотокамеру, а затем скрытно транслировать данные, активируя, например, каналы Wi-Fi или GPRS.

Есть варианты вредоносных программ, способные предпринимать активные действия от имени абонента, например, отправлять с телефона SMS или MMS. Более того, определив по номеру входящий звонок от самого злоумышленника, троян не позволит зараженному телефону ни звуковым сигналом, ни вибрацией, ни включением экрана проинформировать владельца о звонке, а просто установит соединение. Таким образом, злоумышленник в любой момент может прослушать переговоры, в которых участвует владелец мобильного устройства.

И, наконец, самое неприятное. Вирусописатели достаточно давно тестируют свои «творения» на преодоление защиты наиболее популярных антивирусов. И если речь идет о вредоносной программе, разработанной специально для целевой атаки на организацию, можно не сомневаться, что такое приложение будет совершенствоваться до тех пор, пока оно не сможет внедриться и выполнить свои функции, не «потревожив» мобильный антивирус.

РЕШЕНИЕ SAFEPHONE ДЛЯ ЗАЩИТЫ КОРПОРАТИВНОЙ СОТОВОЙ СВЯЗИ С ЦЕНТРАЛИЗОВАННЫМ УПРАВЛЕНИЕМ

Как же защитить корпоративную мобильную связь? Первое, что приходит на ум – мобильные антивирусные



приложения. Но даже их корпоративные версии представляют собой те же персональные решения, оснащенные единой консолью управления и обновления антивируса. Решением действительно корпоративного масштаба с развитой системой мониторинга и контролем выполнения политик безопасности является система Mobile Device Management (MDM). Одной из наиболее «строгих» таких систем является российское решение для защиты корпоративной сотовой связи SafePhone, разработанное компанией ООО «НИИ СОКБ».

В чем же ее «строгость»? Разработчикам продуктов информационной безопасности обычно приходится искать компромисс между уровнем защиты и удобством пользователя. При защите мобильных устройств эта проблема ощущается еще острее. Ведь зачастую используются личные гаджеты сотрудников (концепция BYOD – Bring Your Own Device). Здесь требования безопасности вступают в неразрешимое противоречие с законным правом владельца самому выбирать, какие приложения использовать и какие настройки применять. Разработчики SafePhone не пытались усидеть на двух стульях и представили решение, удовлетворяющее в первую очередь требованиям безопасности.

На мобильном устройстве устанавливается SafePhone Client, который невозможно ни остановить, ни удалить. Именно он следит за выполнением политик безопасности, обменивается информацией с центром управления и получает от него команды по доступному каналу (3G, GPRS или Wi-Fi). Установка и удаление программного обеспечения осуществляется только администратором из центра управления корпоративной сотовой связью SafePhone Center. Конечно, вряд ли владелец смартфона будет мириться с тем, что не может самостоятельно устанавливать приложения на собственное устройство, так что в основном система устанавливается на служебных смартфонах, предоставляемых организацией. И раз уж идет речь о корпоративных устройствах, то и возможностей для контроля и ограничения использования устройства на совершенно законных основаниях становится гораздо больше.

РАЗРАБОТЧИКИ SAFEPHONE ПРЕДСТАВИЛИ РЕШЕНИЕ, УДОВЛЕТВОРЯЮЩЕЕ В ПЕРВУЮ ОЧЕРЕДЬ ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ

Решение SafePhone предусматривает возможность дистанционного запрета использования потенциально опасных интерфейсов (Bluetooth, Wi-Fi), фотокамеры, «черных» и «белых» списков абонентов. Например, можно сделать недоступной связь с абонентами, не включенными в синхронизирующийся с ActiveDirectory список контактов сотрудников. Интеграция со СКУД дает возможность автоматически отключать нежелательные интерфейсы и приложения в тот момент, когда сотрудник попадает на территорию организации. При наступлении критических с точки зрения информационной безопасности событий (например, смене SIM-карты или наборе «тревожной» комбинации символов) предусмотрено выполнение заранее прописанных сценариев – от скрытой отправки сообщения, до полного удаления данных и возвращения устройства к заводским настройкам.

Известно, что при наличии оборудования телефонные переговоры и SMS могут быть легко перехвачены и расшифрованы. Повысить безопасность коммуникаций позволяет обмен внутренними голосовыми и текстовыми сообщениями между абонентами SafePhone по защищенному каналу. Этот обмен даже оператор сотовой связи видит лишь как поток зашифрованной информации.

СОЦИОЛОГИЯ МОБИЛЬНЫХ КОММУНИКАЦИЙ

Поскольку речь идет о корпоративных устройствах, то в соответствии с законодательством возможно контролировать их целевое использование. В системе SafePhone реализована возможность (с учетом категории владельца корпоративного устройства и политики безопасности) сохранения истории звонков и сообщений (в том числе внутренних), информации о запуске и остановке приложений. Также возможна фиксация данных об уровне заряда аккумулятора, об изменении настроек, а также запуске и остановке смартфона. При наличии в смартфоне GPS-модуля может осуществляться трекинг географического местоположения сотрудника.

Развитая система регистрации событий SafePhone несет в себе массу допол-

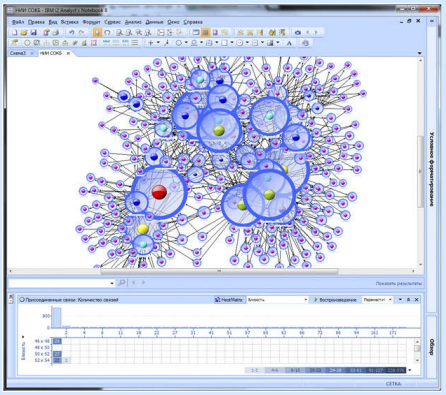
РЕШЕНИЕ IBM I2 ЗАРЕКОМЕНДОВАЛО СЕБЯ КАК НАДЕЖНОЕ СРЕДСТВО АНАЛИЗА СТРУКТУРИРОВАННОЙ ИНФОРМАЦИИ И ШИРОКО ПРИМЕНЯЕТСЯ СЛУЖБАМИ БЕЗОПАСНОСТИ И ПРАВООХРАНИТЕЛЬНЫМИ ОРГАНАМИ.

нительных возможностей по борьбе с инсайдом в среде персонала организации. Примерами аналитических задач, решения которых позволяют выявлять пути утечки чувствительной информации – а самое главное – предотвращать такие утечки, являются:

- выявление ключевых сотрудников (людей, на которых преимущественно замыкаются бизнес- и производственные коммуникации);
- определение потенциально небезопасных «внешних» абонентов;
- поиск возможных путей косвенного доступа к информации (цепочки общения, векторы «сарафанного радио»);
- поиск общих контактов для заданной группы лиц;
- выявление неформальных групп общения и неформальных лидеров внутри коллектива;
- выявление внеслужебных «горизонтальных» и «вертикальных» связей;
- увязка событий и инцидентов с коммуникационным профилем или его аномалиями.

Разумеется, решение подобных задач на больших данных ручными методами – работа непосильная. Здесь на помощь специалистам приходят инструментальные средства, одним из которых является информационно-аналитическая система IBM i2. Это решение зарекомендовало себя как надежное средство анализа структурированной информации и широко применяется службами безопасности и правоохранительными органами.

Несколько стандартных операций – и в аналитическом приложении i2 Analyst's Notebook появляются данные, зафиксированные системой регистрации SafePhone. Их дальнейшая обработка заключается в выявлении и визуализации различных закономерностей.



Первое, что может сгенерировать система – общая схема связей сотрудников. Уже этот начальный шаг показывает количество и уровень «центров притяжения», демонстрируя сложность коммуникационного профиля.

Сценарии дальнейшего анализа разнообразны и многочисленны. Скрывая «объекты с единственной связью», получаем сведения о контактах внешних абонентов более чем с одним сотрудником. Укладывается ли такая модель общения с клиентом или поставщиком в принятые процедуры? Если нет, что ж, i2 дает сигнал о возможных злоупотреблениях задолго до их реализации.

Одной из наиболее востребованных аналитических функций является выявление «ядра влияния» – построение схемы, на которой система автоматически выявляет ключевых лиц организации, сотрудников имеющих высокую степень влияния на коллектив. Что, если среди них появился «внешний» абонент? Как минимум тревожный звонок для службы безопасности. Аналогичным образом выявляется «ядро информированности» – перечень лиц, потенциально наиболее осведомленных о внутренних процессах и состоянии дел. Интересным будет и определение «ядра обеспечения» – автоматическое выявление субъектов, выполняющих ключевые посреднические функции (управления и организации). Вся эта аналитика наглядно визуализируется в виде коммуникационных графов.

В расследовании инцидента, связанного с утечкой, может оказать действенную помощь функция выявления косвенных связей. Система наглядно

РАЗВИТАЯ СИСТЕМА РЕГИСТРАЦИИ СОБЫТИЙ SAFEPHONE НЕСЕТ В СЕБЕ МАССУ ДОПОЛНИТЕЛЬНЫХ ВОЗМОЖНОСТЕЙ ПО БОРЬБЕ С ИНСАЙДОМ В СРЕДЕ ПЕРСОНАЛА ОРГАНИЗАЦИИ.

покажет, как сотрудник непрофильного подразделения мог получить доступ к важной информации и «слить» ее на сторону.

В системе i2 доступны и функции статистического анализа, например: наиболее «активные» и наиболее «популярные» абоненты (ранжирование по числу исходящих и входящих вызовов и сообщений), интенсивность коммуникаций по дням недели, по временным интервалам внутри суток, сравнительная «весомость» ключевых сотрудников. В рамках выполнения статистического анализа условия сравнения могут комбинироваться для составления сложных запросов.

Наконец, регистрация геоданных позволяет увязывать «коммуникационную» аналитику с локализацией событий на местности и учитывать в работе географический фактор. Также хорошие результаты дает возможность анализа коммуникаций на различных временных срезах.

СИНЕРГЕТИЧЕСКИЙ ЭФФЕКТ

И IBM i2, и SafePhone являются очень мощными решениями сами по себе, а при совместном использовании их эффективность существенно возрастает. Интеграция этих средств позволяет противодействовать угрозам как на техническом, так и на социально-организационном уровне, причем делать это проактивно, заблаговременно. Подобных примеров комплексного использования решений может быть достаточно много. Это интеграция со СКУД, с системами определения местонахождения сотрудников и оборудования в реальном времени (RTLS), с системами контентной фильтрации, совместная аналитика с использованием сторонних баз данных и работа с ГИС. Именно в умелом, взаимодополняющем использовании систем защиты и заключается искусство обеспечения комплексной безопасности организации. NBJ