INFOWATCH®
BECAUSE YOUR DATA IS YOUR BUSINESS

т./ф.: (+7 495) 22-900-22

Россия, 123022, Москва
2-ая Звенигородская ул., д. 13, стр. 41

www.infowatch.ru

Предпосылки и следствия консьюмеризации

Консьюмеризация явочным порядком наступила — личные устройства сотрудников уже приносят пользу компаниям и организациям, однако технологические решения сегодня не всегда отвечают сложившейся корпоративной культуре.

04/2012, OSP.ru
Рустэм Хайретдинов

Несколько лет назад многие российские топ-менеджеры одной крупной нефтяной компании как по команде в один месяц закупили себе смартфоны — можно себе представить ужас руководителя службы информационной безопасности, вдруг осознавшего, что доступ к почте и внутренним корпоративным ресурсам организации теперь оказался вне его контроля. Консьюмеризация разрушала привычную картину мира — отныне внутри защищенного корпоративного периметра присутствовало чужеродное, не подконтрольное ИТ-департаменту устройство.

Корпоративная «мобилизация» пришла без предупреждения, причем в компаниях в первую очередь появились устройства, которые для корпоративной работы не предназначены, — вместо традиционной «книги», лучшим подарком стал iPhone, и руководство большинства компаний и госучреждений, следуя моде, обзавелось диковинными устройствами. А ведь всего два-три года назад продвинутые сотрудники умоляли администраторов дать им доступ со своих смартфонов к корпоративной электронной почте. Но тщетно: «это небезопасно», «нет двухфакторной аутентификации», «неясно, как встраивать в устройство токены» и тому подобные ответы можно было услышать от администраторов. Однако появление новых устройств у топ-менеджеров, а также возможность организации удобной работы для сотрудников, работающих в «поле», прорвали линию обороны ИТ-департамента, и мобильные устройства прочно обосновались в корпоративных сетях.

Поначалу казалось, что, перекроив волевым решением существовавшие политики информационной безопасности, топ-менеджмент «выпустил из бутылки» армию угроз — гуру от ИТ пророчили лавину инцидентов, на тематических конференциях и выставках стали массово проводить демонстрации взломов смартфонов через открытые каналы Bluetooth или через подставные беспроводные сети. Однако появления мобильных троянцев, «воспетых» в отчетах производителей антивирусного ПО, мы пока так и не дождались, а всплеска атак хакеров тоже не

т./ф.: (+7 495) 22-900-22

Россия, 123022, Москва
2-ая Звенигородская ул., д. 13, стр. 41

www.infowatch.ru

случилось. То ли все еще впереди, то ли возможности взлома сильно преувеличены. Тем не менее именно потери и кражи составляют сейчас львиную долю в числе всех инцидентов с мобильными устройствами. По данным отчета аналитического центра InfoWatch за 2011 год, наибольшее число утечек информации (19,1%) связано с бумажной документацией вследствие неправильной утилизации, потерь распечатанной конфиденциальной информации и т. п. При этом утечки информации через мобильные устройства составляют менее 10%, а в 2010 году этот показатель составил 12%.

Сотрудник vs компания

Производители смартфонов оставляют пользователю немного возможностей для управления внутренними настройками устройства — ограниченный функционал администрирования создает трудности и для злоумышленника, и для администратора корпоративной сети, в которой должно работать устройство. Но это вовсе не означает, что устройства нельзя сделать более «дружелюбными», управляемыми и безопасными. Обеспечить защиту мобильных устройств необходимо, но, возможно, защищать следует не сам смартфон, а информацию на нем, причем не забывая о человеческом факторе.

Технологии защиты мобильных устройств сегодня имеются и уже показали свою эффективность, но в силу изначальной направленности на потребителя ориентированы преимущественно на персональную защиту — от краж и вирусов. Адаптация мобильных устройств к механизмам централизованного администрирования для работы в корпоративных сетях потребовала от производителей некоторого времени, и сегодня для каждой платформы появились средства криптозащиты, удаленного блокирования или автоматического обнаружения устройства (возможно, например, фотографирование лица нового пользователя камерой самого устройства с последующей передачей в полицию фото и данных о местонахождении смартфона или планшета). Усилена и биометрическая часть аутентификации — созданы решения, позволяющие устройству узнавать пользователя в лицо или по радужной оболочке глаза.

Защита от хищения или потери — лишь первая линия обороны. С позиции корпоративной безопасности, устройство нужно защитить не только от воров, но и от самого пользователя, устанавливающего на него ненадежные приложения или слишком вольно обращающегося с доверенными ему корпоративными данными. Основное средство на этой линии обороны — решения категории MDM (Mobile Device Management).

Однако есть одна проблема — BYOD (Bring Your Own Device). Мобильные устройства компании не принадлежат — сотрудники их купили себе сами. С одной стороны, это экономия на закупках средств производства, а с другой — повышенные расходы на обеспечение информационной безопасности. И если, например, «противоугонные» средства, поставленные на автомобиль за счет компании, люди обычно приветствуют, то установку средств управления, ограничивающих возможности владельца смартфона, вовсе нет.

Кроме того, дополнительные средства могут еще собирать массу информации о пользователе: местоположение, история Web-серфинга, частная переписка, фотоальбомы и т. д., что вызвало появление вопроса: «Не нарушает ли установка агента MDM на устройства право на неприкосновенность частной жизни?». В чем-то это напоминает дискуссии десятилетней давности на тему «Не нарушают ли системы DLP право на тайну переписки». Тогда коллизии в каждом конкретном случае разрешались на уровне соглашений между работником и работодателем — если

т./ф.: (+7 495) 22-900-22

Россия, 123022, Москва
2-ая Звенигородская ул., д. 13, стр. 41

www.infowatch.ru

сотрудник желает пользоваться мобильным устройством для обработки корпоративной информации, то он соглашается на установку дополнительного управляющего ПО.

Имеется и еще одна аналогия с DLP — подход производителей таких решений к передаче конфиденциальных данных. Изначально большинство мобильных устройств проектировалось для личного использования, поэтому особый упор делался на функции переноса данных между приложениями — в рамках одного почтового клиента можно свободно получить письмо с одной учетной записи и отправить его с другой. Но такой удобный для частного пользователя сценарий создает для администратора дополнительную головную боль. Поэтому сегодня для корпоративных мобильных устройств рекомендуется иметь специальную учетную запись, контролируемую удаленно и предназначенную для работы с конфиденциальной информацией.

В зависимости от производителя и платформы техническая гибкость решения MDM в отношении защиты частной жизни может быть разной. Простейшие продукты претендуют на полный контроль устройства, а есть решения, создающие на устройстве только «сейф» для обработки корпоративной информации. Имеются решения, которые считают устройство, на котором они установлены, зараженным и скрывают все действия пользователя при доступе к конфиденциальной информации за «шумом» ложных действий, обманывая программы и приспособления считывания нажатий клавиш.

Катализатор инвестиций

Рано или поздно по запросу рынка или пользователей технологические решения появляются, но намного сложнее с идеологией — например, корпоративная «мобилизация» приблизила непонятные технологии и к рядовому пользователю, и к руководителю. Многие сложные ранее для понимания вещи типа TCO или ROI вдруг стали топ-менеджерам ясны и очевидны. Мобильные решения в руках руководителя вполне можно назвать «катализатором инвестиций», что весьма благоприятно сейчас сказывается на процессе выделения средств на обеспечение информационной безопасности — кражи и потери смартфонов изменили стереотипы поведения топ-менеджмента.

Освободившись от бдительной опеки службы безопасности, владельцы смартфонов изменили свое отношение к безопасности. Мало того, корпоративная «мобилизация» изменила цепочку принятия решений. Бизнес-пользователь на простых примерах воочию убедился, что информация имеет цену, а ее потеря наносит компании вполне ощутимый финансовый ущерб. Как следствие, роль бизнес-пользователя изменилась — теперь он точно знает, насколько ценна информация, которую он может потерять. Немаловажно и то, что спрашивать в случае потери будут именно с него.

В отличие от «корпоративного» типа поведения, когда ответственность и заботы об информационной безопасности целиком ложились на специальные службы, BYOD принес новый тип — «консьюмерский», предполагающий, что решение, а следовательно, и ответственность по защите информации на своем устройстве полностью лежат на пользователе. Действительно, администрирование смартфонов по аналогии с локальными ПК невозможно, хотя бы потому, что мобильный трафик идет через операторов связи, минуя сеть организации. Распространение «неуправляемых» пользовательских устройств требует повышения ответственности менеджера за доверенную ему информацию. В этой ситуации офицеры безопасности, сотрудники ИТ-службы становятся консультантами и исполнителями, а владельцы информации, по идее, должны выступать инициаторами внедрения средств защиты.

INFOWATCH®
BECAUSE YOUR DATA IS YOUR BUSINESS

т./ф.: (+7 495) 22-900-22

Россия, 123022, Москва
2-ая Звенигородская ул., д. 13, стр. 41

www.infowatch.ru

Еще совсем недавно руководитель лишь отдавал распоряжение — «в недельный срок обеспечить защиту», часто не зная, какую пользу это принесет, а теперь, после нескольких случаев с устройствами, забытыми топ-менеджерами в барах, он ясно представляет последствия инцидента лично для себя и готов сам разобраться в том, какие механизмы защиты нужно использовать. В итоге от абстрактных приказов руководство компаний и организаций переходит к конкретным решениям, требуя от всех пользователей шифровать данные, установить пароли на смартфоны, флешки и ноутбуки и т. д. Теперь уже не специалист по безопасности приходит к бизнесу с просьбами выделить средства на инструменты повышения надежности, а сами пользователи обращаются в службы с вопросом «Как сделать так, чтобы база клиентов с ноутбука директора по продажам не оказалась у конкурента?». Для производителей и интеграторов программных и аппаратных решений защиты информации это означает сокращение пути до лица, принимающего решения. Поэтому приложения для мобильных устрой

ств быстро стали популярны в среде разработчиков «тяжелых» корпоративных продуктов класса ERP, бизнес-аналитики и пр. За очень короткое время, по сути, родился новый рынок — практически каждый интегратор завел у себя «мобильную» практику и предлагает корпорациям услуги по управлению парком разнородных мобильных устройств. Большинство производителей корпоративных приложений, от ERP до внутренних порталов, оптимизируют интерфейсы под смартфоны. В магазинах приложений регулярно появляются новые специализированные программы для управления устройствами. Такие решения теперь есть и в линейке производителей антивирусов и систем DLP.

Владелец корпоративных секретов сегодня готов сам участвовать в процессе их защиты: директор по продажам внимательно выслушает специалиста по информационной безопасности, объясняющего, как предотвратить утечку прайс-листов и текстов договоров, а руководителя отдела кадров очень заинтересуют средства мониторинга исходящего из компании потока данных на предмет выявления фактов отправки сотрудником резюме, чтобы вовремя сделать ему «правильное» предложение.

В эпоху консьюмеризации для оценки эффективности средств защиты можно обойтись без сложных подсчетов соотношения вероятности угрозы и масштаба ущерба — все наглядно на уровне пользователя. А если так, то можно говорить о формировании реальной основы для стирания границы между бизнесом и ИТ. В этом, наверное, основная заслуга корпоративной «мобилизации».

***

Сегодня еще имеется много компаний, в которых запрещены мобильные персональные устройства, и, возможно, в них информация защищена лучше, однако конкуренты уже получают преимущество на рынке за счет более оперативного обслуживания клиентов и повышения производительности труда сотрудников, работающих на приобретенных за свои деньги устройствах и на площадях, аренду которых компании не нужно оплачивать. «Мобилизация» и «консьюмеризация» состоялись — теперь администраторам, пользователям, разработчикам защитного ПО, а также бизнесу придется корректировать свои взгляды с учетом новой корпоративной реальности.

Оригинал публикации: http://www.osp.ru/os/2012/03/13015152/