Ведущая темы
ЛИЛИЯ ПАВЛОВА

Защита на

Корпоративные сети еще долго будут держаться за персональные компьютеры, но мобильные устройства наступают – и мобильная инфобезопасность становится не менее актуальной, чем классическая.

Это молодой рынок, на котором роли поставщиков решений не распределены окончательно, а большинству пользователей еще предстоит пройти путь от беспечности до неусыпной бдительности. Сообщество профессионалов информационной безопасности видит свою задачу в донесении до пользователей правил «мобильной гигиены».

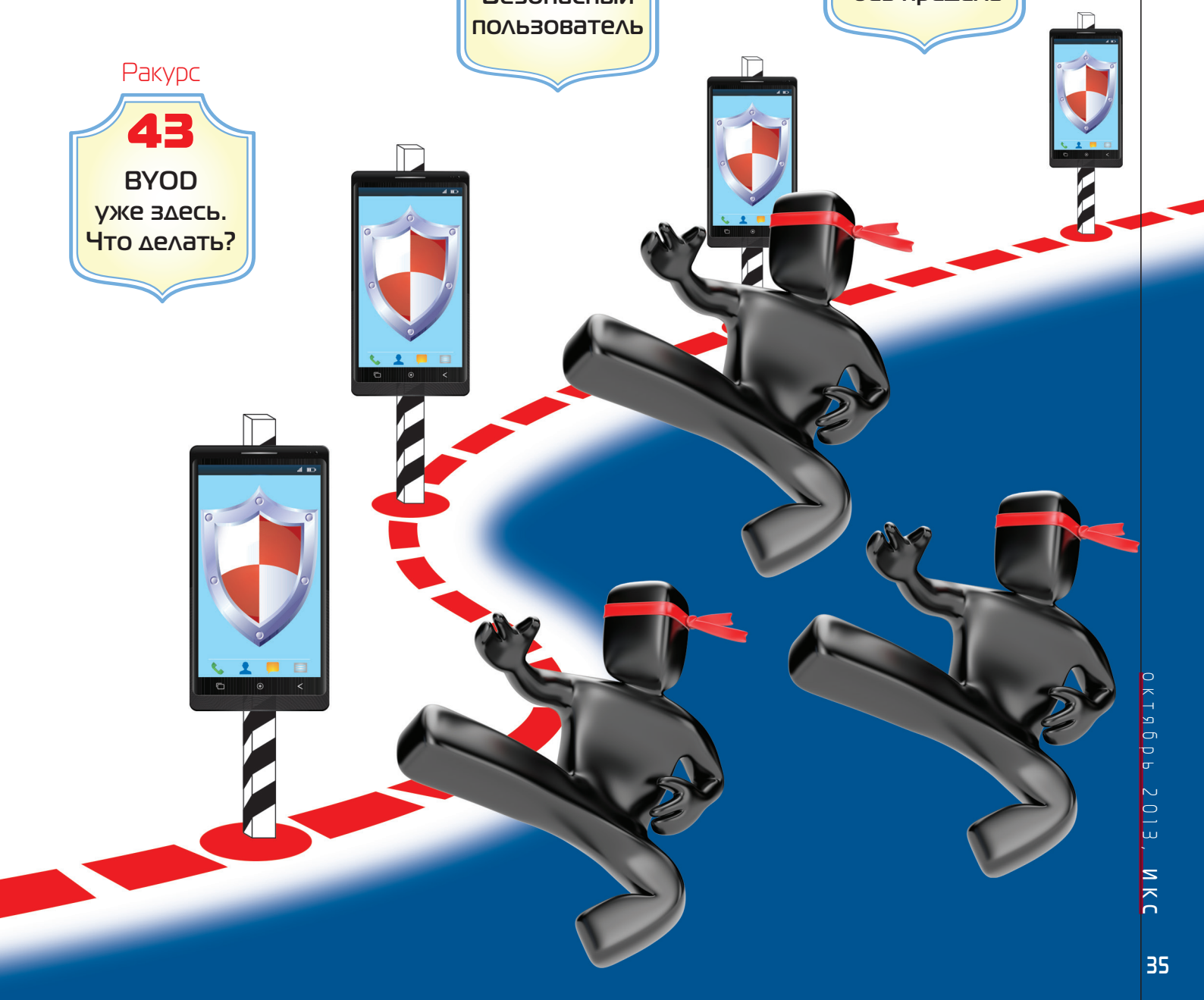
Сложности усугубляются тем, что технологии защиты пока не достигли уровня, позволяющего и удобно, и безопасно работать на любых удаленных устройствах. В этих условиях для инфобезопасности одним из главных рычагов становится дисциплина. Но каким правилам следовать?

В госсекторе управление взял в свои руки регулятор в лице ФСТЭК – и здесь, пока не появится очередной Сноуден, уязвимости не выплывут наружу. В корпоративном секторе вопросами мобильной инфобезопасности занимаются сами компании, обладающие квалифицированными специалистами. Но сотрудники компаний чаще всего обходят защитные барьеры, если они доставляют неудобства в работе. Пока коллизии разрешаются поиском баланса между удобством и рисками в области кибербезопасности. По мнению экспертов, «взвешивание» должен производить бизнес, поскольку у безопасников чаша весов непременно склонится в сторону защиты информации.

Наименее экипированным остается сегмент SMB, где мобильные устройства используются практически бесконтрольно. Однако, как считают эксперты «ИКС», именно в этом сегменте защита может быть реализована наиболее быстро и дешево благодаря операторам мобильной связи, предлагающим облачные услуги информационной безопасности.

Итак, к вызовам мобильной реальности готовься!

мобильных рубежах



фокус

Безопасность mecum porto

За тотальной «мобилизацией» последовал взрывной рост мобильных угроз, который вызывает стремление от этих угроз защититься. В этом триединстве формируется молодой рынок корпоративной мобильной инфобезопасности.

В русле мирового тренда

На рынке ИКТ в 2012–2020 гг., по мнению аналитиков IDC, наступает период «третьей платформы», технологическую основу которой составят мобильные устройства и приложения, а также облачные сервисы, социальные сети и «большие данные» (предыдущие две платформы характеризуются «правлением» ПК (1986–2012 гг.) и мейнфреймов – до 1986 г.).

Уже сейчас использование не только корпоративных, но и личных смартфонов и планшетов сотрудников стало нормой жизни большинства компаний. Мобильные устройства используются как минимум для доступа к корпоративной электронной почте, адресной книге, календарю. Как максимум – для работы с критичными для бизнеса приложениями. При этом и атаки, направленные на корпоративные ИТ-системы через смартфоны и планшеты, приобретают массовый характер. По данным Trend Micro, в 2013 г. число угроз для устройств на платформе Android (лидера на рынке мобильных ОС) превысит 1 млн. Кроме заражения вирусами подстерегают и другие опасности – утечка важных корпоративных данных по вине пользователя, утеря или кража устройства с конфиденциальной информацией. Как отмечают эксперты «ИКС», если еще недавно атаки направлялись на собственно мобильные устройства, то сейчас основная цель – информация, которая на них передается (принимается), обрабатывается и хранится. Соответственно, бизнес должен защищаться – и вслед за ростом мобилизации предприятий растет и мировой рынок мобильной безопасности, объем которого к 2016 г., по прогнозу IDC, достигнет $2,5 млрд против $628 млн в 2011 г.

Россия как одна из самых мобилизированных стран идет в русле мирового тренда. Безопасность мобильных устройств (смартфонов и планшетов) стала вызывать у компаний немалое беспокойство: 95% российских ИТ-специалистов, принявших участие в опросе «Лаборатории Касперского» в 2013 г., сообщили о том, что в их организациях был зарегистрирован по меньшей мере один инцидент информационной безопасности, связанный с использованием мобильных устройств. Между тем на рынке представлено множество решений, разработанных для того, чтобы инцидентов избежать или свести их к минимуму.

IDC выделяет пять основных сегментов рынка мобильной безопасности. По темпам роста (до 30% в год) лидирует сегмент управления политиками и уязвимостями; на втором месте по востребованности – сегмент шлюзов контроля доступа; в тройке лидеров также управление доступом пользователей с мобильных устройств. Защита и контроль данных и защита от мобильных угроз менее востребованы – вероятно, потому, что эти сегменты развивались самыми первыми и теперь на рынке наступило некоторое насыщение такими решениями. Однако в целом рынок переживает стадию активного формирования.

Границы государства

В деле мобильной инфобезопасности главная забота государства – госсектор. Сформулировав в ряде новых приказов относительно персональных данных и государственных информационных

систем требования к их защите, ФСТЭК ясно указала, что доступ к информации с мобильных устройств возможен, и это, как считает Юрий Черкас («Инфосистемы Джет»), самое важное. Еще три-четыре года назад принцип безопасного мобильного рабочего места на уровне государственной нормативной базы никак не описывался, что было своеобразным нонсенсом, ведь и средства организации мобильного доступа, и соответствующие средства защиты существовали и использовались. По мнению Алексея Сабанова («Аладдин Р.Д.»), поскольку в настоящее время в госорганах и на ряде госпредприятий мобильный доступ предоставляют все чаще и все большему числу сотрудников, регулятор должен заняться созданием нормативной базы, состоящей из документов о соблюдении норм и требований информационной безопасности, которые носят хотя бы рекомендательный характер.

Ряд экспертов «ИКС» полагают, что в более жестком регулировании рынок и не нуждается. В то же время регулятор мог бы стать драйвером мобильной инфобезопасности в России, пересмотрев, например, существующие национальные стандарты в этой области. С точки зрения Степана Дешёвых («Лаборатория Касперского»), сейчас они изолируют российский рынок от внешнего – перед игроками извне стоят серьезные технические и сертификационные барьеры. Пока это благоприятно сказывается на местных поставщиках, но в долгосрочной перспективе тепличные условия вредят: из-за ослабленной конкуренции продукты местных производителей начинают функционально и качественно уступать западным аналогам, поэтому было бы полезно со временем стандарты унифицировать с западными, уверен эксперт. Владимир Залогин («С-Терра СиЭсПи») отмечает, что государство могло бы также улучшить механизмы контроля таким образом, чтобы времени на согласование применения средств защиты тратилось существенно меньше, чем сейчас; учесть зарубежный опыт задействования механизмов саморегулируемых организаций; рассмотреть эффективность экономических механизмов (страхование ответственности, апостериорная безопасность и др.) для защиты потребителей информационных технологий от сопутствующих рисков.

Наконец, государство может сыграть решающую роль, приняв меры для обеспечения информационной безопасности личности. По мнению Игоря Корчагина (ИВК), в число таких мер должно войти развитие законодательства в сфере ИТ, учитывающего новые тенденции использования мобильных устройств как средства доступа к информации и ее публикации, оплаты услуг и товаров, ведения переписки, аудио/видеообщения через сети международного информационного обмена. Это, в свою очередь, должно стать гарантом соблюдения прав и свобод граждан; повышения уровня их технической грамотности и информационной культуры, в том числе в области информационной безопасности.

Особенности предложения: новая «классика жанра»

Можно выделить пять групп игроков этого рынка: вендоры мобильных устройств, производители ОС, разработчики ПО, интеграторы, операторы мобильной связи. Эксперты «ИКС» отмечают, что в корпоративной защите мобильных устройств преуспели традиционные лидеры ИБ-индустрии, а также монопродуктовые вендоры, развивающие свои решения исключительно в нише мобильной безопасности. К компонентам корпоративной системы мобильной безопасности относятся решения как «стационарные», так и специфические «мобильные»: антивирус, шифрование, надежная парольная защита, выделение корпоративных данных в защищенный контейнер, фильтрация звонков и SMS, веб-фильтрация, биометрическая идентификация, двухфакторная аутентификация, смарт-карты и электронные ключи, поиск устройства по GPS, GSM или Wi-Fi, блокировка устройства, SSL VPN-шлюзы и др. Но использование любого из названных механизмов без создания доверенной вычислительной среды не даст необходимого результата. Именно доверенная вычислительная среда и является «классикой жанра», уточняет Юрий Акаткин (ГК «Ростехнологии»).

При этом большинство экспертов «ИКС» сходятся во мнении, что «классикой жанра» в области защиты мобильной инфраструктуры в корпоративном сегменте следует считать системы управления мобильными устройствами Mobile Device Management (MDM). Это инструмент реализации единой политики безопасности в компании, централизованного управления всем парком мобильных устройств и рассылки настроек доступа к сервисам организации.

Главный драйвер развития систем MDM – распространение принципа BYOD (Bring Your Own Device)

Тренды мобильной безопасности – 2013

- рост продаж планшетов и смартфонов;
- рост количества вредоносного ПО для мобильных устройств;
- рост индустрии мобильных приложений и услуг, в том числе мобильного банкинга;
- использование злоумышленниками новых методов получения доступа к смартфонам, поддерживающим технологию NFC;
- распространение ботнетов на базе мобильных устройств;
- резкий рост угроз для Android, появление сложных многофункциональных вредоносных программ под эту ОС;
- повышение интереса органов госвласти и муниципальных органов к выпуску мобильных приложений доступа к электронным услугам различных ведомств;
- распространение подхода BYOD;
- повышение интереса к решениям MDM;
- смещение акцента с простых систем управления мобильными устройствами на комплексные системы управления безопасностью, приложениями и мобильными устройствами.

Источник: опрос «ИКС»

(см. с. 43). Объем мирового рынка MDM, по данным Gartner, составил в 2012 г. $780 млн, а в 2014 г. превысит $1,6 млрд. Лидеры здесь – компании, созданные относительно недавно и сделавшие ставку на мобильную безопасность. «Магический квадрант», построенный Gartner для сегмента MDM в 2011 г., свидетельствует, что рынок еще не был сформирован, на нем присутствовало много небольших компаний-стартапов. В последующие два года происходили крупные сделки M&A, со своими MDM-решениями вышли серьезные игроки, которые сейчас развивают это направление. В июне нынешнего года из сотни разработчиков решений аналитики выделили 18 компаний, активно играющих на этом поле (что радует, в их число вошла и российская «Лаборатория Касперского»). В группе лидеров – AirWater, MobileIron, Citrix, SAP, Good Technology, Fiberlink.

Системы MDM собирают данные об устройстве и его использовании, настраивают его, устанавливают и удаляют приложения, передают и стирают файлы, а в случае утери или кражи устройства позволяют удаленно инициировать его возврат к заводскому состоянию, с полной очисткой памяти от данных. Как отмечает Ольга Еремина (T-Systems CIS), подобных систем разработано немало и отличаются они как функциональностью, так и областью применения – некоторые работают лишь с отдельными версиями определенных ОС, другие охватывают широкий спектр возможных типов устройств.

Надо сказать, российский рынок осторожно отнесся к внедрению MDM-решений: в прошлом году это была тема обсуждений и публикаций в прессе, но не практические шаги. Сегодняшнее «молчание MDM» Ю. Черкас объясняет тем, что стартовали только «первые ласточки», успешных публичных кейсов нет просто потому, что проекты не завершены. Всплеск проектной активности в этом направлении – вопрос времени и наличия успешных внедрений, считает он. При этом эксперт подчеркивает, что ограничивать рынок мобильной безопасности только решениями класса MDM неправильно: нельзя забывать о безопасности доступа, конкретная реализация которого зависит от сценария, принятого в компании (VDI, NAC, шлюз SSL VPN).

Характерно, что в России одними из первых начали внедрять MDM операторы мобильной связи – не только для зашиты своей инфраструктуры, но и для предоставления облачного сервиса управления мобильными устройствами(см. с. 40).

Впрочем, у индустриальных продуктов появляются конкурирующие решения, встраиваемые производителями мобильных платформ в свои ОС. Так, по словам Сергея Ларина (Microsoft Россия), в Windows 8.1 с помощью связки с Windows Server устройство «знает», какие именно данные были получены из корпоративной сети, – и при необходимости эти данные можно стереть удаленно, не затрагивая всю остальную информацию.

Специфика спроса: три большие разницы

И госсектору, и крупным корпорациям, и компаниям SMB нужен одинаковый защитный функционал, поскольку угрозы для всех едины. Но эти три пользовательских сегмента различаются по регуляторным требованиям и по требованиям к уровню управления.

Государственному заказчику необходимо наличие сертификата соответствия на систему мобильной безо-пасности – как минимум от ФСТЭК, как максимум от ФСБ, отмечают эксперты «ИКС». Здесь безопасности мобильных устройств уделяется серьезное внимание, вплоть до использования смарт-карт для доступа к данным с планшетов и телефонов. С другой стороны, число таких пользователей невелико – как правило, это высшее руководство. Еще одну особенность мобильного доступа в госструктурах могут иметь режимные организации, деятельность которых регулируется традиционными требованиями к защите, в том числе и связанными с понятием государственной тайны. К сведениям, составляющим гостайну, доступ с планшета (тем более с личного) не позволит предоставлять никто и никогда. По мнению А. Сабанова, для применения мобильных платформ в госсекторе нужны изменения в нормативной правовой базе, а также продуманные организационные мероприятия.

Полная противоположность – SMB. Здесь сотрудники носят всю информацию с собой – мобильные устройства используются практически бесконтрольно. Максим Лукин (CTI) отмечает, что компании SMB зачастую строят системы защиты не на основании формализованных процессов и процедур, а на интуиции и представлениях системного администратора о том, какой должна быть безопасность. Но если в какой-то момент количество запросов от пользователей на

События мобильной безопасности – 2013

- первые внедрения решений MDM;
- выход новой версии Dr. Web AV-Desk для предоставления операторами облачной защиты мобильным пользователям;
- выход приказа ФСТЭК «Об утверждении требований к защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», в котором предусмотрены регламентация и контроль использования в информационных системах мобильных технических средств и защита мобильных технических средств, применяемых в информационных системах;
- сертификация криптопровайдера «Крипто-Про» для платформы Apple iOS;
- объявление Samsung Electronics о готовности к продвижению на российском рынке своих гаджетов с встроенной российской криптографией;
- обнаружение атаки Red October, целью которой был сбор конфиденциальной информации в дипломатических, правительственных, военных и научных организациях стран Восточной Европы, бывшего СССР и Центральной Азии и которая проводилась в том числе с использованием мобильных устройств.

Источник: опрос «ИКС»

подключение корпоративной почты с мобильного устройства увеличивается, именно в сегменте SMB может быть востребована услуга MDM из облака, которая требует наименьших капитальных затрат со стороны предприятия, а также человеческих ресурсов.

Корпоративный заказчик – самая благодатная поляна спроса. Ему необходимы системы централизованного мониторинга и управления мобильными устройствами, отслеживания установленных приложений, удаленного анализа событий, расследования инцидентов и т.п. Как отметил С. Дешёвых, крупные коммерческие компании обычно имеют в своем штате высокопрофессиональных специалистов по безопасности, которые умеют грамотно выстроить эшелонированную систему защиты периметра предприятия – но мобильные устройства постоянно проходят через периметр защиты и покидают его. Соответственно, пользователи за пределами периметра ожидают такой же легкости доступа к корпоративным данным, как и изнутри него, – и компания покупает и внедряет самые лучшие решения, не требуя сертификации ФСТЭК и ФСБ. При этом лишь 8% крупных компаний прямо выбирают запретительную стратегию в отношении использования мобильных устройств в корпоративной среде, свыше 50% предприятий подходят к вопросу более гибко и позволяют своим сотрудникам работать и дома, и даже в чужой стране (данные «Лаборатории Касперского»).

А еще они не мучаются соотношением цена-качество.

Планшет для босса

Недавно ИТ-сообщество всколыхнуло известие о конкурсе по выбору поставщика специализированного планшета для главы «Газпрома». Контракт на сумму 114,5 млн (!) руб. выиграла компания «Сапран», которая создаст мобильное приложение для управления бизнес-процессами корпорации. Приложение будет интегрировано с существующими информационными системами «Газпрома» и станет их частью, интерфейс этого ПО будет установлен на планшетном компьютере Apple iPad.

При всем богатстве выбора мобильных продуктов на рынке не нашлось готового решения, сочетающего в себе и необходимый функционал, и безопасность требуемого уровня. Это известие вызвало не только лавину шуток, но и заставило многих задуматься о безопасности: защитить мобильный доступ к критическим данным – большая проблема. ИКС

Позиция

За периметром

Распространение и интеллектуализация мобильных устройств размывают понятие периметра безопасности. Сегодня защищают не «стену», а отдельные элементы, которые за нее выносятся. На каких столпах зиждется защита мобильных устройств?

Дмитрий КОСТРОВ, заместитель директора департамента управления радиочастотами и сетями связи, Минкомсвязь

Политика работы с мобильными устройствами есть у всех крупных компаний. Одни структуры прямо запрещают использовать мобильные устройства на своей территории – вплоть до того, что при входе у человека отключают все приборы с программным обеспечением: камеру, диктофон, телефон. Такой подход имеет право на существование, но его применяет ограниченный круг организаций. Другой подход – управляемость устройств, их защита.

На корпоративном уровне защиты огромную роль играют системы управления мобильными устройствами, MDM. Это молодой сегмент рынка, но на нем уже заметна определенная эволюция. Так, первоначально использовались системы, которые контролировали установленные в устройстве приложения, а также данные, стираемые при потере устройства. Теперь делается попытка системного управления устройством со стороны не ИТ-, а ИБ-службы, в частности организуется криптозащищенная «песочница» из тех программ, которые выдает компания. И это направление развивается.

Второй столп безопасности корпоративной мобильной среды – норматив-

ные правовые акты. К сожалению, в России нет такого универсального документа, которым могли бы пользоваться все организации, независимо от отраслевой принадлежности и размеров бизнеса. Но можно опереться на международный опыт. Скажем, в июле нынешнего года Национальный институт стандартов и технологий США (NIST) выпустил вторую версию руководства по управлению безопасностью мобильных устройств в корпоративной среде (SP 800-124). В этом документе отмечается, что компаниям следует выработать политику безопасности мобильных устройств, организовать безопасность всего их жизненного цикла и использовать централизованное MDM-решение. По всем трем пунктам даны детальные рекомендации.

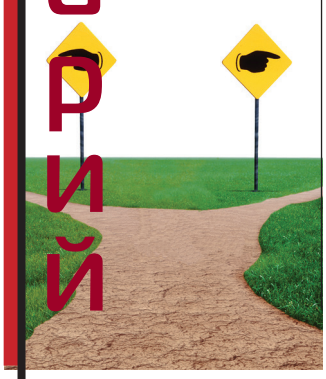
Очевидно, рынок сам отрегулирует все вопросы инфобезопасности корпоративной мобильной среды. Но государство должно обозначить правила игры. Пока у нас в этом плане есть перекосы. Например, 152-ФЗ определяет жесткие требования для информационных систем, обрабатывающих персональные данные. Они не выполняются и не могут быть выполнены в полном объеме. Вместе с тем за утечку этих данных нет практически никакого наказания. А следовало бы установить общие подходы к защите, чтобы каждая организация уровень защиты выбирала сама. Некоторые решат, что им вообще не надо защищаться. Но за утечку данных необходимо штрафовать – на миллион долларов, на 10, на 100 миллионов. Вот тогда рынок сам отрегулируется.

Третий столп – пользователи. Их обучение должна взять на себя служба ИБ. Не пугая, надо рассказывать и показывать в картинках, какие могут возникнуть ситуации и проблемы в области информационной безопасности. Даже простые вопросы типа «Можно ли закачивать программы из любых магазинов?» заставят задуматься об информационной безопасности мобильных устройств.

Наконец, операторы мобильной связи могут предоставлять облачные сервисы инфобезопасности как корпоративным, так и частным клиентам. Удивительно, но уже как минимум пять-шесть лет операторы говорят о нежелании стать лишь «битовой трубой», а ведь самый простой путь избежать этой доли состоит в предоставлении клиентам сервисов информационной безопасности. Бизнес-модель MSSP (Managed Security Service Provider) известна давно. В России рынок как раз переживает такой момент, когда и операторы и клиенты созрели для внедрения этих сервисов. В активе оператора не только «труба» для передачи данных, но и, что более важно, клиентская база, которой могут быть интересны новые сервисы. Спектр услуг – фильтрация веб-трафика, PKI, AaaS, сетевой антивирус, антиспам, анти-DDoS, managed VPN и т.д. В принципе в рамках операторского бизнеса возможна реализация любых решений.

В России «чистых» MSSP пока нет, однако большинство операторов уже осваивают эту модель. Надо признать, есть еще проблемы доверия клиентов к системе, страхования рисков утечек. Решения этих проблем нам предстоит найти в скором будущем. ИКС

Сценарий



Кто привьет массам «мобильную гигиену»?

Операторы мобильной связи могут и должны играть ключевую роль в обеспечении безопасности персональных устройств своих клиентов, считает Дмитрий УСТЮЖАНИН, руководитель Департамента информационной безопасности «ВымпелКома».

Дмитрий УСТЮЖАНИН

– Дмитрий Дмитриевич, какие тенденции или события этого года вы бы выделили как наиболее важные для рынка мобильной безопасности?

– После существенного уменьшения роли BlackBerry мировой рынок окончательно перестал делиться на устройства для корпоративного и частного использования. Планшеты и смартфоны берут верх над ноутбуками и компьютерами. В ответ на эти вызовы на рынке появились первые коммерческие продукты, позволяющие выделить внутри одного устройства область, которая может функционировать полноценно и обособленно от остальной среды.

Новая роль по сценарию

Информационная безопасность мобильного доступа основана на тех же принципах, что и вся система корпоративной ИБ. Но без специфических решений здесь не обойтись.

Прежде всего, это внедрение решений MDM, которые позволяют автоматизировать установку на мобильное устройство необходимого программного обеспечения, включая средства антивирусной защиты, и контроль доступа к нему. Системы MDM обеспечивают также настройки безопасности устройств, мониторинг их использования и дистанционное удаление всех корпоративных данных с них в случае угрозы утечки (при утере или краже).

По данным Gartner, в 2012 г. мировой рынок MDM-решений вырос до $784 млн против $350 млн в 2011 г. А к 2014 г., по прогнозам аналитиков, объем этого рынка превысит $1,6 млрд в год. Что примечательно, наблюдается тенденция перевода решений MDM в форму облачных услуг: если в 2011 г. только 5% мобильных подключений к корпоративным сетям управлялись с помощью облачных MDM-решений, то в 2012 г. их доля выросла до 17%.

Это означает, что у оператора сотовой связи появляется новая роль в обеспечении информационной безопасности мобильного доступа к корпоративным сетям: он может выступать в качестве провайдера облачных услуг MDM для сторонних компаний, в том числе малого и среднего бизнеса. В частности, МТС рассматривает возможность предоставления облачных услуг MDM своим клиентам. Такой подход позволит клиентам сэкономить средства и получить квалифицированные услуги при доступном уровне затрат.

Сергей ВЛАСОВ, начальник отдела безопасности корпоративных информационных систем, МТС

– Это стирание граней – хорошая новость или плохая? Ведь с точки зрения инфобезопасности личные мобильные устройства сотрудников – самое слабое звено в корпоративной сети...

– Предлагаю осмыслить этот вопрос иначе. Мобильный телефон человек обычно приобретает самостоятельно или получает в подарок. В аппарате хранятся личные контакты, музыка, фотографии, переписка; смартфон является проводником в социальных сетях. Я считаю, что человек будет гораздо трепетнее относиться к своему индивидуальному устройству, чем к корпоративному. А поскольку безопасность играет в жизни все большую роль, он также более грамотно будет подходить к соблюдению мер безопасности. Поэтому считать мобильный телефон слабым звеном, наверное, не стоит. Встроив корпоративную среду в персональный девайс, мы можем получить вполне доверенную среду, которая будет всегда органично сопровождать сотрудника. А поскольку телефон всегда при нас, можно, наоборот, усилить безопасность корпоративной среды, привнеся дополнительную персональную аутентификацию.

Сегодня мобильный аппарат приблизился к персональным компьютерам уже не только по вычислительным мощностям, но и по предоставляемому функционалу, и действующие политики в области информационной безопасности, применимые к компьютерам, легко переносятся на мобильные устройства. Уверен, что «переделать» пользователя не получится, и в конце концов корпоративные правила позволят ему менять компьютер на телефон так же, как до этого он менял один компьютер на другой.

Думаю, есть только одна сфера, где личные устройства могут оказаться неприменимы. Это деятельность, связанная с государственной тайной. А в остальных сферах наш мобильный телефон должен сопровождать нас, помогать нам справляться с нашими проблемами.

– Вы отметили выход на рынок новых продуктов. Как реагируют на них потенциальные покупатели, насколько они осведомлены о возможностях этих решений (например, MDM)?

– В настоящее время тема уязвимости мобильных платформ обсуждается только профессионалами и не слишком широким кругом продвинутых пользователей. Количество реализованных угроз пока невелико, и они не затрагивают широкие слои. В большинстве случаев пользователь предпочитает решать проблемы самостоятельно, поскольку еще не слишком хорошо понимает их специфику. Важная задача, которая стоит перед обеспечивающим безопасность сообществом, – донести до масс правила мобильной «гигиены», а затем и провести мобильную «диспансеризацию». На сегодня мы удовлетворены динамикой роста использования решений безопасности для мобильных устройств, и в целом эта динамика коррелирует с выявляемыми и анонсируемыми угрозами. Хочется, чтобы пользователи превентивно защищали свои аппараты как самостоятельно, так и с помощью предлагаемых решений.

В «ВымпелКоме» MDM-решение уже внедрено, но нельзя сказать, что продукты этого класса широко представлены в корпоративном секторе. Наверное, потому, что количество реализованных угроз, которые покрываются возможностями MDM, еще не превысило некий критический уровень, после которого развертывание такого рода систем становится необходимостью. Но полагаю, что об их внедрении стоит задуматься. На мой взгляд, решения MDM эволюционируют от средств контроля девайсов к полнофункциональному виртуальному рабочему пространству, которое всегда будет рядом со специалистом и ло-

гически никак не будет пересекаться с его личным пространством внутри персонального мобильного устройства.

– Существует ли специфика обеспечения безопасности в корпоративной мобильной среде для крупных коммерческих компаний и для предприятий SMB?

– Крупные компании, располагая штатом инженеров и необходимыми мощностями, предпочитают строить собственные платформы. Предприятия SMB останавливают свой взгляд на недорогих решениях, но приобретают их не часто. Можно даже вывести такую закономерность: чем крупнее компания, тем более вероятно появление в ней решений обеспечения безопасности мобильных устройств. Но что роднит предприятия крупного и малого бизнеса, так это желание уйти в облака. Для крупных компаний это снижение издержек на поддержку, более высокое качество сервиса и большая гибкость. Для мелких – возможность приобрести сервис, не вкладываясь в оборудование и персонал, и получить высокую функциональность продукта.

– На рынке мобильной безопасности «играют» производители устройств, поставщики программных решений, системные интеграторы, операторы, причем нередко конкурируют «перекрестно». Как вы считаете, должны ли компании выполнять только свои функции или освоение смежных рынков неизбежно?

– Каждая компания должна концентрироваться на тех решениях или услугах, которые у нее лучше всего получаются, где чувствуются конкурентные преимущества и некий драйв, так сказать. Безусловно, четко очертить границы, где должны действовать поставщики, где – вендоры или интеграторы, а где – операторы, невозможно. Все зависит от команды и бизнес-стратегии, причем стратегия может меняться как в зависимости от условий рынка, так и от конкретных задач.

– Какую роль в этом случае будут играть операторы связи?

– Человек, держащий мобильное устройство, связан с внешним миром через оператора мобильной связи. Никто не может так много сказать об абоненте, как оператор. Именно оператор связи имеет все шансы стать оператором предоставления интегрированного сервиса с учетом безопасности персонального устройства. Именно у оператора есть все, что нужно для построения такого рода систем. Естественно, при необходимости будут использованы интеграционные возможности других игроков рынка. Такие возможности не будут зависеть от принадлежности устройства, они могут быть экстерриториальны, не ограничены во времени и оптимальны по отношению к трафику и потреблению ресурсов. ИКС

Особое мнение

Когда офис последует за работником

С мобильной безопасностью проблема не в технологиях, а в неготовности многих руководителей бизнеса разрешить своим сотрудникам работать удаленно.

Алексей ЛУКАЦКИЙ,
эксперт по информационной безопасности, Cisco

Опережая сознание потребителей

Мобильность наряду с облаками и технологиями взаимодействия относится к основным тенденциям современной ИТ-отрасли. Это накладывает отпечаток на действия многих компаний, в портфелях которых появляются решения по мобильной безопасности. Традиционные вендоры в области ИБ (RSA, «Лаборатория Касперского», IBM и др.), вендоры в области сетевой безопасности (например, Cisco), традиционные поставщики мобильных решений (BlackBerry, Good Technology, MobileIron и т.п.) начинают играть заметную роль в этом сегменте, постепенно вытесняя «чистых» игроков рынка мобильной безопасности – Mobile Active Defense, NetMotion Wireless, NQ Mobile и др., которые либо сдают свои позиции, либо поглощаются более крупными «коллегами» (например, Authentec, Credant, PhoneFactor).

Этот рынок очень динамичный, ситуация на нем меняется быстро. Можно выделить несколько направлений, на которые сейчас смотрят его игроки: консьюмеризация; невмешательство в частную жизнь; мобильные угрозы; потребность в защите данных; защита информации о местоположении; вирту-

ализация на мобильных устройствах, позволяющая отделить личное от рабочего; гетерогенность и защита на уровне приложений.

Технологии еще не вышли на уровень адекватного восприятия и применения со стороны корпоративного заказчика. И проблема тут не столько в самих технологиях, которые чего-то «не умеют», сколько в менталитете многих руководителей бизнеса, которые не готовы разрешать своим сотрудникам мобильную (удаленную) работу. Это требует некоторого переворота в сознании, когда офис следует за работником, а не наоборот. За переменами в сознании идет изменение бизнес-процессов (работы с кадрами, постановки задач, их контроля). И только потом наступает время технологий. Можно сказать, что сейчас развитие технологий опережает развитие сознания потребителя.

От удаленного VPN-доступа – к BYOD

Желание работать с тем, что модно или удобно, присуще сотруднику любой компании – от небольшого киоска, торгующего сигаретами, до транснациональной газовой корпорации. Даже в государственных органах, где исторически были наложены существенные ограничения на работу беспроводных и мобильных устройств, началось движение в сторону мобилизации (но контролируемой и регламентируемой).

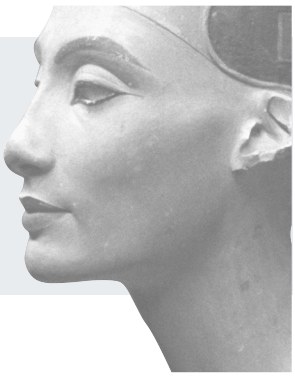
В компании Cisco тоже не сразу пришли к внедрению мобильных устройств. Сначала активно использовался удаленный VPN-доступ с лэптопов, потом был запущен пилотный проект по оснащению сотрудников корпоративными мобильными устройствами определенной модели – с такого устройства доступ был разрешен только к корпоративной почте, календарю и адресной книге. Потом был расширен спектр возможных платформ и принята концепция BYOD.

Примечательно, что в компании основным риском для мобильных устройств является их утеря. Именно поэтому на одном из этапов развития мобильного защищенного доступа к корпоративным ресурсам было решено внедрять модель BYOD. В ней риски утери перекладываются на сотрудника; на нем же лежит задача покупки и обновления устройства, а также выполнения разработанных политик корпоративной мобильной безопасности.

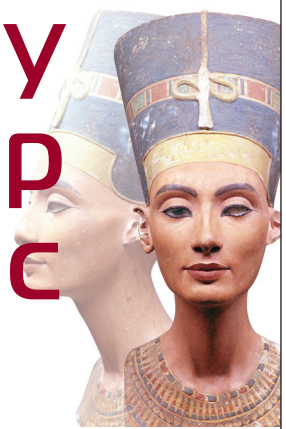
Затем подошел черед внедрения MDM-решений, и сейчас для сотрудников компании нет разницы между корпоративным лэптопом и личным смартфоном – они оба имеют доступ к приложениям внутри корпоративной сети (хватило бы вычислительных ресурсов и размера экрана). Правила, политики и технические средства одинаковы для всех типов устройств. Различия начинаются только на уровне юридическом. Но компания шла к этому не один месяц и даже не один год – отталкиваясь от бизнес-потребностей, на каждом этапе считала риски и отдачу и только в случае положительного сальдо переходила к следующему этапу.

Принятие концепции BYOD позволило в разы сократить капитальные затраты на приобретение мобильных устройств для сотрудников (при том, что за один календарный год количество личных устройств выросло в 2,5 раза), а также на 19% снизило нагрузку на ИТ-департамент и службу поддержки. Затраты в пересчете на одного сотрудника снизились на 29%, а удовлетворенность последних выросла на 33%. Поэтому можно сказать, что эффект от внедрения концепции BYOD не просто положительный, а конкретно измеримый и ощутимый в масштабах компании. ИКС

ракурс



BYOD уже здесь
Что делать?



В последние год-два редкое исследование рынка инфобезопасности обходилось без подсчетов и прогнозов распространения BYOD. К 2014 г. 90% компаний в мире будут поддерживать корпоративные приложения на личных устройствах сотрудников, прогнозирует Gartner. В России в 2013 г. этот показатель достиг 74%, причем, по результатам исследования «Микротеста», лишь 1% опрошенных заявили о предоставлении компанией мобильных устройств с уже настроенными политиками безопасности. Впрочем, несколько другие цифры дал опрос, проведенный «Лабораторией Касперского»: более 50% сторонников BYOD и 8% крупных компаний, выбирающих запретительную стратегию в отношении работы в корпоративной среде с помощью мобильных устройств.

Общий вектор очевиден: все больше личных мобильных устройств используется в служебных целях – для деловой

переписки, работы над документами и др. При этом эксперты отмечают рост популярности видеосвязи, общения с коллегами через Skype и ВКС. Этот тренд сказался и на рынке ВКС-решений, в том числе традиционных. Например, Polycom выпускает защищенные приложения для проведения видеоконференций не только из конференц-залов, но и с личных планшетов или смартфонов, причем, отмечает Сергей Хомяков, вице-президент Polycom в России и СНГ, эти решения обеспечивают пользователям, находящимся как под защитой межсетевого экрана, так и за его пределами, безопасный доступ к сервисам видеосвязи, где бы они ни находились и какое бы устройство они при этом ни задействовали.

О плюсах BYOD сказано уже немало. К категории сомнений эксперты «ИКС» относят некоторые аспекты человеческого фактора: администраторы не поддерживают ОС определенных типов устройств, публикация корпоративных приложений для которых кажется невозможной или сложной; департамент безопасности не верит разработчикам мобильных устройств и не считает средства их защиты достаточно надежными; персональная ответственность сотрудника за утрату мобильного устройства, подключенного к корпоративной среде, настолько тяжела, что исключает желание им пользоваться; отношение к вовлечению личных средств в работу у разных людей разнится: для кого-то личная жизнь и работа – единое целое, а кто-то их четко разделяет и никогда не смешивает. И жирный минус – повышенные риски заражения вредоносным ПО, взломов и утечек корпоративных данных. BYOD-конфликт между безопасностью и удобством далеко не исчерпан, мобильные устройства сотрудников превратились в отдельный класс угроз.

Уровень же знаний о правилах безопасного использования мобильных устройств крайне низок. Все эксперты «ИКС» признают это (→ см. с. 50), как и то, что сейчас профессионалы в области инфобезопасности должны нести знания в BYOD'ированные массы. И они готовы поделиться с читателями своими рекомендациями. ИКС

Защита движущихся мишеней

Антон РАЗУМОВ,
руководитель группы консультантов по безопасности, Check Point Software Technologies

Первый закон Ньютона гласит, что движущееся тело всегда будет стремиться сохранять свое движение. Так же ведет себя и бизнес-информация в мобильных устройствах: однажды придя в движение, она навсегда остается в этом состоянии, потенциально рискуя попасть в руки мошенников. Как найти верный подход к защите мобильных корпоративных данных?

Почем утечка мобильных данных

О том, что ситуация быстро выходит из-под контроля ИТ-служб, свидетельствуют результаты исследования «Влияние мобильных устройств на безопасность информации», недавно проведенного Check Point среди почти 800 ИТ-специалистов из разных стран мира. 79% участников опроса подтвердили, что за последние 12 месяцев в их компаниях имели место случаи утечки мобильных данных. Это влекло за собой немалые потери: для 42% компаний такие инциденты, если учесть рабочее время персонала, оплату услуг юристов, штрафы и расходы на исправление ситуации, в прошлом году стоили более $100 тыс. Трудно представить, но 16% опрошенных сообщили, что ликвидация последствий обошлась их организациям более чем в $500 тыс.

Не слишком ли велики количество инцидентов с безопасностью мобильных данных и связанные с ними потери? Результаты опроса дают объяснение: в 88% организаций число персональных мобильных устройств, подключаемых к корпоративным сетям, за последние два года увеличилось более чем в два раза. На них находится разнообразная конфиденциальная информация: электронная деловая переписка (88%), контактная информация (74%), календари сотрудников (72%) и данные клиентов (53%).

Неконтролируемая и неуправляемая

Проблема обеспечения безопасности мобильной информации вышла за рамки ИТ-отделов – множество персональных смартфонов и планшетов используются бесконтрольно, несмотря на риск утечки данных. 63% респондентов признались, что они даже не пытались управлять корпоративной информацией, хранящейся на персональных устройствах сотрудников, и лишь 23% используют средства контроля за мобильными данными или защищенные контейнеры на устройствах.

Почему же стратегии защиты данных на персональных устройствах сотрудников так сильно отстали? Частично это объясняется тем, что время и ресурсы ИТ-отделов, отводимые на обеспечение защиты мобильных данных, небесконечны. Специалистам приходится расставлять приоритеты – и, к сожалению, ресурсов управления персональными устройствами недостаточно, чтобы справиться с их лавинообразным распространением.

Возможно, организации полагаются на грамотность своих сотрудников в области безопасного обращения с корпоративными данными на персональных устройствах – и многие специалисты действительно оправдывают это доверие. Но у сотрудников, как правило, на первом месте стоит эффективность собственной работы, а не снижение риска, которому подвергается корпоративная информация.

В большинстве случаев у персонала нет злого умысла, и данные остаются в надежных руках. Однако время от времени случайная утечка данных все же происходит. В ходе опроса 66% ИТ-специалистов высказали мнение, что беспечность сотрудников представляет гораздо большую угрозу для безопасности организации, чем деятельность киберпреступников.

Дело в содержании, а не в устройстве

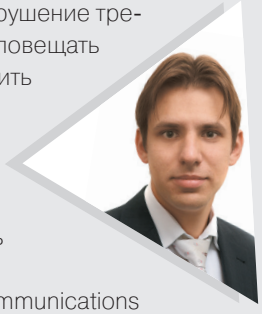
Каков же оптимальный подход к защите конфиденциальной информации от утери или кражи с мобильных устройств сотрудников? Главное, что следует помнить, – информация сегодня стала мобильной. Поэтому организации должны стремиться управлять не устройствами своих сотрудников, а той коммерческой информацией, которая на них хранится. Попытки контролировать устройства могут затруднять работу персонала и нарушать их личное пространство, а это, в свою очередь, может привести к тому, что они будут идти в обход политики безопасности. Именно нацеленность на управление корпоративными данными во многом упрощает обеспечение безопасности в концепции BYOD.

Кроме того, необходимо уделить особое внимание выявлению, изоляции и шифрованию бизнес-информации, где бы она ни хранилась. В этом случае, даже если пользователь с благими намерениями копирует корпоративные данные на свое устройство либо получает доступ к ним через электронную почту или другое приложение, данные остаются защищенными от утечки. Еще лучше, если защита данных осуществляется автоматически на уровне политики, т.е. они остаются в безопасности при любых обстоятельствах – при копировании на мобильное устройство, электронной рассылке и т.д. Чем меньше пользователь замечает работу

Девять правил защиты BYOD

BYOD-стратегия защиты корпоративных данных универсальна, вне зависимости от того, какие решения и ПО входят в корпоративную сеть.

1. **Определите потребности вашей компании.** Определите, насколько ваша компания устойчива к рискам утери информации и насколько надежна корпоративная информационная среда. Возможно, в вашей отрасли существуют законодательные ограничения использования BYOD. Ваша стратегия должна прежде всего учитывать потребности и нюансы вашего бизнеса.
2. **Объедините подразделения.** Так как BYOD имеет отношение не только к ИТ-департаменту, подключите и другие отделы, так или иначе заинтересованные в рациональном использовании сотрудниками их собственных устройств. К составлению и реализации плана по внедрению BYOD имеет смысл привлечь HR-отдел, юридическую службу и финансистов.
3. **Оцените и используйте все доступные средства защиты.** Задействуйте все решения, которые могут помочь обезопасить коммуникационную среду вашего бизнеса, – систему аутентификации, NAT/брандмауэр, шифрование и т.д.
4. **Определите критерии допуска.** Сформулируйте алгоритм допуска того или иного устройства в корпоративную сеть. Так, в решениях видеосвязи некоторых производителей уже заложена функция, позволяющая составить список надежных устройств.
5. **Ориентируйтесь на нужды своих сотрудников.** Разделите всех корпоративных пользователей на условные группы, исходя из их профессиональных потребностей и деятельности, разработайте для них различные уровни привилегий и убедите коллектив в необходимости подобной системы для функционирования компании.
6. **Разработайте план поддержки.** Определите, какого рода поддержка потребуется личным устройствам ваших сотрудников со стороны ИТ-отдела. В большинстве случаев необходима лишь помощь при их подключении к корпоративной сети.
7. **Будьте проактивными.** Убедитесь, что все сотрудники, участвующие в программе BYOD, понимают принятую политику безопасности и осознают риски, которые могут создавать используемые ими устройства.
8. **Соблюдайте установленные правила.** Никому не хочется быть «плохим парнем», но нарушение требований безопасности может иметь печальные последствия. Придумайте, как вы будете оповещать сотрудников о нарушении ими политики информационной безопасности, и будьте готовы ограничить или вовсе закрыть доступ их устройств в корпоративную сеть.
9. **Регулярно обновляйте политику информационной безопасности.** Как только вы расслабитесь и подумаете, что охватили все стороны вопроса обеспечения безопасности при BYOD, может возникнуть новое устройство или новое приложение, которое заставит вас пересмотреть установленные ранее правила. Поэтому принятая вами программа должна быть достаточно гибкой, чтобы подстраиваться под новые веяния и тренды.



Александр БАРИНОВ, региональный директор в России и СНГ, LifeSize Communications

решения для обеспечения безопасности (это характерно для представителей последнего поколения таких решений), чем меньше оно нарушает привычный рабочий процесс, тем в большей безопасности оказываются данные.

Еще одна обязательная составляющая стратегии защиты – соответствующее обучение сотрудников, информирование пользователей о политике компании по обеспечению безопасности данных и о возможных последствиях их утечки. ИКС

Зашифрованная мобильность

Катажина ХОФФМАНН-СЕЛИЦКА,
менеджер по продажам,
HID Global
в Восточной Европе

На фоне растущей популярности тренда BYOD и неослабевающей активности киберпреступников ключом к безопасности бизнеса может стать формирование защищенных зон для корпоративных данных и приложений.

Использование сотрудниками личных смартфонов и планшетов для работы с корпоративными информационными ресурсами и приложениями открывает большие перспективы для развития бизнеса. Но в таких условиях вполне закономерна активизация хакерской деятельности для получения доступа к паролям пользователей и ценной корпоративной информации. А это, в свою очередь, увеличивает риски ИБ.

Один из наиболее эффективных подходов к созданию безопасного мобильного пространства основан на раздельном хранении в устройстве персональных и корпоративных данных и формировании для последних дистанционно управляемой зашифрованной зоны. На обмен данными между зоной, содержащей корпоративную информацию, и остальным пространством на устройстве накладываются ограничения согласно политике, установленной в организации, а для доступа к корпоративным ресурсам используется строгая двухфакторная аутентификация.

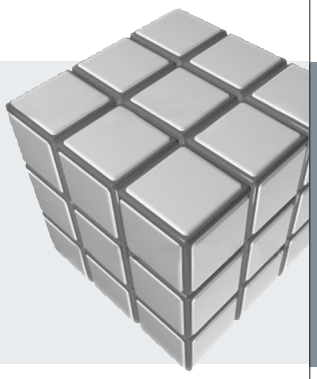
Таким образом, благодаря выделению конфиденциальной информации в отдельную зону, где применяется шифрование, между личными и бизнес-данными образуется четкая и безопасная граница. Такая демаркация данных в совокупности с разграничением доступа обеспечивает эффективное управление информацией в мобильных средах: обращаться к данным могут только те стороны, которым это разрешено политикой. Кроме того, сотрудники могут быть уверены, что их личные данные, хранящиеся на мобильных устройствах, защищены и не окажутся случайно удалены при увольнении человека из организации. Что особенно важно, параметры защищенной зоны могут задаваться и в дальнейшем обновляться сотрудниками, отвечающими за политику безопасности, на основании поведенческих реакций каждого пользователя.

Разумеется, разработать универсальное решение для защиты любых данных в любой компании практически невозможно ввиду большого разнообразия пользовательских устройств и методов работы сотрудников. В каждой организации должна быть реализована собственная политика безопасности, основанная на четких правилах: кто из сотрудников имеет право на получение той или иной информации.

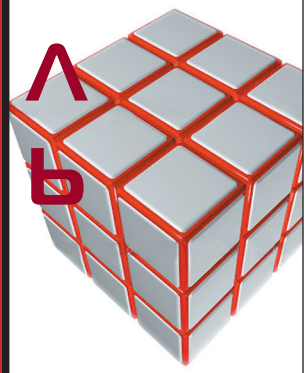
Выделим три дополнительных элемента безопасности, которые могут быть использованы при формировании в мобильном устройстве отдельной зоны для корпоративных данных. Первый – аутентификация самого пользователя, когда он, например, включает телефон и вводит PIN-код. Второй – аутентификация для доступа к ресурсам, которые либо уже находятся на мобильном устройстве, либо к ним можно получить доступ с его помощью. Третий элемент – это ввод учетной информации для входа в корпоративное приложение или базу данных. Организациям рекомендуется применять для этих целей двухфакторную аутентификацию. В настоящее время она не исчерпывается генерацией одноразовых паролей с помощью электронных токенов. Одноразовые пароли можно создавать и через программные софт-токены, запущенные на мобильных устройствах. Чтобы оптимизировать доступ к различной информации с одного устройства, можно комбинировать токены и бестокенные решения – например, аутентификацию с помощью карты доступа и смартфона или планшета, поддерживающего технологию NFC (Near Field Communication), или методы, основанные на поведении пользователя при вводе пароля.

Исследование, проведенное компанией Forrester, показало, что 60% случаев утечек корпоративных данных происходит по причине невнимательности сотрудников. Зонирование данных и приложений вкупе с организацией многоуровневого контроля доступа и аутентификацией обеспечивают безопасность всей мобильной среды и существенно снижают риск утечки данных, предоставляя организациям возможность добиться баланса между удобством доступа к данным и реализацией нормативных мер защиты. ИКС

Модель



Безопасный пользователь



Как заметили в одной компании, «безопасность у нас такая безопасная, что рассказать опасаемся». Тем не менее без хотя бы фрагментарных фактов о пользовательском опыте сложно составить общую картину мобильной защиты.

Девайсы во власти

Члены нашего правительства очень уважают Twitter – очевидно, для секретной переписки у них другие каналы. Насколько они безопасные – пока не объявится очередной Сноуден, известно не будет. Вспыхивающие время от времени скандалы вокруг публикаций стенограмм телефонных разговоров первых лиц государства некоторое время будоражат общественность, но потом забываются. А вот в Германии решили перестраховаться: компания T-Systems получила заказ от одного немецкого ведомства на новые мобильные устройства для канцлера Ангелы Меркель и других высокопоставленных немецких политиков, имеющих доступ к государственной тайне, для обмена секретными данными. По данным T-Systems, на новых смартфонах впервые появится функция шифрования как голосовых вызовов, так и электронных писем. Раньше политикам приходилось использовать разные телефоны. В новых устройствах рабочие и личные функции будут разделены. В рамках рабочих функций пользователи смогут безопасно отправлять даже документы с грифом «секретно». Помимо этого, пользователи смогут установить на свои смартфоны приложения Facebook и Twitter, которые сейчас заблокированы по соображениям безопасности (что актуально и для некоторых российских политиков).

В законодательной власти у нас информация, судя по всему, за железной стеной. На недавнем круглом столе по киберугрозам один молодой сенатор посетовал, что не может смотреть свою рабочую почту со смартфона и поэтому, когда он находится в поездке, помощник «ручками перебрасывает» ему на смартфон все, что приходит на его почтовый ящик. Но допуска к гостайне у него нет, так почему хотя бы удаленный доступ к почте не разрешить? Как заметила по этому поводу Наталья Касперская, когда устанавливаются жесткие ограничения, причем построенные на представлениях о безопасности 20-летней давности, их начинают обходить именно из-за их жесткости. И вот перед нами не «стена», а всего лишь «кирпичик», который легко перешагнуть и идти дальше. Сегодня существует столько способов обхода подобных запретов, что вместо безопасности мы получаем вседозволенность с отсутствием безопасности, считает глава InfoWatch.

Что касается «четвертой власти», то, как признал Илья Лазарев, зам. главного редактора «РИА Новости», в последнее время все чаще предпринимаются попытки, и небезуспешные, проникнуть в корпоративную систему агентства через социальные сети и личные аккаунты его сотрудников для распространения ложной информации. «Мы расцениваем это как новый тренд в дискредитации СМИ, – заявил И. Лазарев. – Кроме того, мы понимаем, что сегодня для нас принципиально важно защищать свою информацию. Она может не носить секретного характера, это может быть информация, которая интересна конкурентам». В то же время, оказывается, сотрудники «РИА Новости» используют

для работы собственные устройства, не обремененные корпоративными средствами защиты. Забота же о защите содержащейся в этих девайсах информации возлагается на самих авторов репортажей и новостей. ИКС

MDM и SSL VPN в промышленности

В нынешнем году сотрудники конструкторского бюро «Авиадвигатель» (разрабатывает авиадвигатели для самолетов Ил-96, Ту-204, Ту-214, Ил-76МФ и др., газотурбинные установки для энергетики и газоперекачки, поставляет газотурбинные электростанции) получили возможность удаленной и безопасной работы с бизнес-приложениями на своих мобильных устройствах. На предприятии внедрено комплексное решение для реализации политики безопасности в области BYOD: MDM-система, которая позволяет централизованно управлять мобильными устройствами, и подсистема SSL VPN, обеспечивающая защищенный доступ к внутренним информационным ресурсам. По словам Сергея Бормалева, директора по ИТ «Авиадвигателя», на предприятии и раньше понимали, что корпоративная «мобилизация» – великолепная возможность решать бизнес-задачи, организуя работу сотрудников независимо от того, где они находятся. Однако перспектива значительно увеличить риски утечки конфиденциальных данных при использовании разноплатформенных устройств вызывала опасения.

Как отмечает Константин Астахов из компании КРОК, осуществившей внедрение системы мобильной безопасности, российский бизнес серьезно задумался о разработке мер по защите данных, попадающих в личные устройства работников, лишь года два назад. Особенно актуальна эта проблема для компаний со штатом 300 и более сотрудников (в «Авиадвигателе» работают более 2,5 тыс. человек), поскольку стоимость информации в таких организациях выше, чем расходы на ее защиту.

Реализованный проект дает бизнесу такой же уровень защиты и контроля над мобильными устройствами, какой устанавливается ИТ-службами для персональных компьютеров. При внедрении системы удалось обеспечить сохранность информации на мобильных устройствах, централизованное распространение программного обеспечения и обновлений. Интеграция двух решений позволила разграничить права доступа пользователей к различным информационным ресурсам предприятия и гарантировать конфиденциальность данных при их передаче по открытым каналам связи.

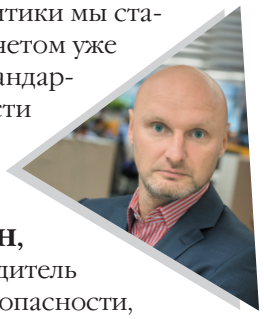
Л. П.

Золотая середина в банке

Наш подход – это безопасность для бизнеса. Трудность в том, что порой необходимо находить золотую середину между бизнес-процессом и соблюдением информационной безопасности.

Поскольку наш банк работает исключительно по виртуальной модели, мы по своей сути ближе к ИТ-компании и хотим предоставить сотрудникам полную свободу для повышения их эффективности. Так, сотрудники банка активно используют для работы свои личные мобильные устройства, на которых установлены все необходимые приложения. В то же время мы не забываем об обеспечении безопасности корпоративных данных. Поэтому не все сотрудники имеют со своих устройств доступ к рабочим ресурсам и электронной почте как одному из важнейших и критичных ресурсов.

Конечно, на своем девайсе каждый волен установить все, что захочет. Но с точки зрения информационной безопасности публичные сервисы, социальные сети, мгновенный обмен сообщениями вызывают обеспокоенность. А то, что осведомленность пользователей не всегда находится на том уровне, который можно считать достаточным, мы воспринимаем как хороший вызов для ИБ-службы в плане повышения культуры инфобезопасности. Политики мы стараемся формировать «на лету», с учетом уже разработанных требований и стандартов информационной безопасности (как международных, так и отечественных). Это передовой подход и желательно ему следовать.



Станислав ПАВЛУНИН,
руководитель
департамента безопасности,
банк «Тинькофф Кредитные Системы»

Свобода и ограничения у оператора

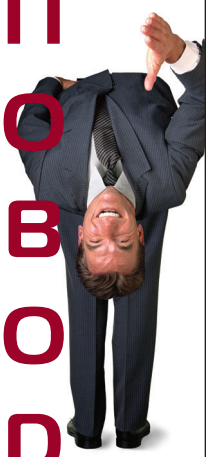
В нашей компании мобильная компонента используется достаточно широко. У ключевых сотрудников на корпоративных и личных устройствах могут быть установлены одни и те же приложения – электронная почта, мгновенный обмен сообщениями, системы поддержки бизнеса. Мы давно уже работаем по принципу BYOD и к настоящему времени накопили опыт, который в целом подтверждает наше изначально позитивное отношение к этому подходу и позволяет и дальше систематически его применять. Например, с учетом мобильной работы и BYOD разрабатывается пользовательский интерфейс ИТ-систем, с помощью которых наша компания контролирует различные аспекты своей основной деятельности – предоставления услуг двухстороннего спутникового доступа в интернет.

Чтобы обеспечить нужный нам уровень информационной безопасности, мы внедрили комплекс мер. Так, доступ четко регламентирован, он осуществляется только по сети VPN, с надежными средствами аутентификации. Естественно, компьютеры защищены антивирусами. На офисных компьютерах не разрешено устанавливать клиентские приложения социальных сетей.

Сегодня все системы требуют пристального внимания службы информационной безопасности. В частности, мы проводим аудит использования мобильных приложений и доступа. Также важно не забывать и о более простых вещах, например о том, чтобы сотрудники ясно понимали, какая информация является конфиденциальной, какие варианты работы с мобильными устройствами значительно повышают их уязвимость. Эти знания надо доводить до сотрудников в рамках четкой процедуры, а не полагаться на то, что они сами во всем разберутся.

Александр КЛИНЦОВ,
гендиректор, StarBlazer

Концептуальный поворот



Мобильность и облака объединяются Безопасно?

Создание брокеров облачных услуг – один из способов преодолеть предубеждение против мобильных облачных вычислений.

Константин АСТАХОВ,
руководитель направления портальных и мобильных решений, КРОК

Мобильные облачные вычисления (МОВ), растущий тренд ИТ-рынка, привлекают внимание бизнеса как выгодная альтернатива традиционным ИТ-решениям. Они делают возможным сокращение времени и расходов на разработку мобильных приложений, и это позволяет использовать большее количество услуг по более низким ценам. МОВ перемещают вычислительные мощности и данные из мобильных устройств в облако, благодаря чему работать с приложением может широкий круг абонентов мобильной связи, а не только пользователи мощных смартфонов. Кроме того, перенос объемных вычислений в облако разгружает память мобильного устройства и снижает потребляемую приложением мощность на 45%.

Уже сегодня МОВ нашли применение в бизнесе. Например, в мобильной коммерции они обычно выполняют такие задачи, как мобильные транзакции и платежи, информирование, продажа билетов и др. Кроме того, МОВ можно использовать для мобильного обучения, расширив таким образом среду традиционного дистанционного образования. Или для «мобильного здоровья» – системы, предоставляющей удаленный доступ к медицинским ресурсам, например к электронной карте пациента.

Однако при всех плюсах МОВ интеграция двух различных сфер – облаков и мобильных сетей – порождает ряд сложностей, как с мобильной, так и с облачной стороны.

С мобильной стороны это недостаточно быстрые каналы связи, негарантированная доступность (пользователи не могут подключиться к облаку из-за перегрузки или сбоя в сети либо при отсутствии сигнала), неоднородность среды.

Можно выделить пять направлений разрешения этих проблем.

Во-первых, развитие каналов связи, в частности, повышение эффективности распределения полосы пропускания.

Во-вторых, улучшение управления доступом к сети, что не только повысит производительность линии связи для пользователей, но и оптимизирует использование полосы пропускания.

В-третьих, повышение уровня качества обслуживания – обеспечение доступа к серверам, расположенным в облаке.

В-четвертых, стандартизация интерфейса. Сейчас взаимодействие пользователя с облаком в основном базируется на веб-интерфейсах. Однако это, возможно, не самый лучший вариант из-за зачастую невысокой производительности браузеров, установленных на мобильных устройствах. Кроме того, широкая совместимость с устройствами – проблема для веб-интерфейса.

В-пятых, конвергенция услуг. Развитие и конкуренция поставщиков облачных сервисов могут привести к тому, что эти услуги будут дифференцированы в зависимости от типа, стоимости, доступности и качества. Более того, в некоторых случаях для удовлетворения потребностей всех пользователей одного облака недостаточно, поэтому необходим новый подход, при котором пользователи смогут обращаться к нескольким облакам через «единое окно». Одно из возможных решений этой проблемы и следующий шаг в развитии облачных вычислений – выход на рынок брокеров облачных услуг.

С облачной стороны, в свою очередь, потребуется повысить эффективность доступа к данным, поскольку с увеличением числа облачных сервисов поток обращений к данным, хранящимся в облаке, растет.

Одновременно с этим необходимо повысить уровень информационной безопасности МОВ. При том, что надежность хранения данных и работы приложений в облаке выше, чем при их размещении на мобильных устройствах (они имеют копии и хранятся на нескольких компьютерах одновременно), для защиты мобильных облачных вычислений необходимо использовать комплекс технологических решений, в который входят средства антивирусной защиты, «контейнеризация» приложений и технологии SSL VPN для защиты соединений.

Потребление сервисов от единого поставщика – брокера облачных услуг, о котором уже говорилось выше, – может также повысить уровень информационной безопасности за счет использования единой ИТ-инфраструктуры. ИКС

Дискуссионный клуб «ИКС»

За безопасность без предела

Эксперты «ИКС» могут диаметрально расходиться в оценках, мнениях и прогнозах, к чему, впрочем, располагает молодость самого рынка.

Маятник конкуренции

«ИКС»: Как вы оцениваете уровень конкуренции на рынке мобильной безопасности?

М. БАШЛЫКОВ

Михаил БАШЛЫКОВ, руководитель направления информационной безопасности, КРОК: Мы наблюдаем серьезную конкуренцию. Но не стоит забывать о том, что рынок мобильной безопасности четко сегментирован. Можно выделить несколько типов решений – например, для разграничения доступа к мобильным устройствам, шифрования данных, антивирусной защиты или централизованного управления мобильными устройствами и данными. Основные игроки также различаются.

Есть сильные компании, предлагающие комплексные решения в области безопасности мобильных устройств и покрывающие все перечисленные сегменты. А есть игроки, выпускающие специализированные решения не с таким широким набором функциональных возможностей, но с более глубокой проработкой продукта по отдельным сегментам.


Р. ХАЙРЕТДИНОВ

Рустэм ХАЙРЕТДИНОВ, исполнительный директор, Appercut Security: Конкуренция на сравнительно новом рынке невелика – еще не определены четкие критерии сравнения продуктов. Ни одно из решений не существует на рынке достаточно долго и не имеет достаточного функционала для доминирования. Разнообразие «бэкграунда» производителей – от производства антивирусов до ERP вкупе с абсолютно новыми, созданными с нуля компаниями – создает очень неоднородную картину предложения. Нет однозначных требований и в спросе – большинство решений выбираются впервые, поэтому будущие пользователи продуктов мобильной безопасности исходят не из опыта использования, а из умозрительных предпочтений.


А. ЧЕЧЕТКИН

Андрей ЧЕЧЕТКИН, консультант по информационной безопасности, LETA: Уровень конкуренции весьма велик. Заказчики при выборе какого-либо решения предпочитают тестировать несколько продуктов, не зацикливаясь на чем-то конкретном. За последние пару лет на рынке сформировалась устоявшаяся группа вендоров, предлагающих решения MDM, поэтому новым игрокам на этом рынке сложно конкурировать на равных с лидерами, тем более что функционал таких решений по большей части одинаков.


С. ДЕШЁВЫХ

Степан ДЕШЁВЫХ, старший менеджер по продуктам, «Лаборатория Касперского»: Мы видим, с одной стороны, обострение конкуренции на рынке, с другой – появление новых технологий, которые расширяют выбор заказчиков и расслаивают рынок. Конкуренция за одних и тех же клиентов появляется не только между решениями, но и между технологиями.

Алексей САБАНОВ, заместитель гендиректора, «Аладдин Р.Д.»: Уровень конкуренции пока невысок. Он наблюдается только между производителями антиспама, антивирусных и антишпионских программ для мобильных ОС. Предстоит серьезное развитие этого сегмента рынка инфобезопасности. Существенная особенность мобильной безопасности заключается в том, что смартфон – это заведомо недоверенная среда. Кроме того, мобильная операционная система, как правило, создана на Западе и может быть полностью закрыта производителем для обновлений, выполняемых не разработчиком (типичный пример – iOS).


А. САБАНОВ

Олег ГУБКА, директор департамента по работе с клиентами, «Аванпост»: За обеспечение мобильной безопасности ухватились многие ведущие игроки рынка инфобезопасности, но, на мой взгляд, сфера корпоративной защиты мобильных устройств еще не вышла на плато продуктивности и этап разочарований у нее впереди. В частности, в отличие от антивирусной защиты, здесь типичный заказчик еще не выработал требования к решениям; в этой ситуации тон задают вендоры. Конкуренцию между вендорами можно оценить как умеренную. Каждое решение находит своего клиента.


О. ГУБКА

Сергей ХАЛЯПИН, руководитель системных инженеров, Citrix Systems: Несмотря на то что уровень конкуренции на рынке мобильной безопасности достаточно высок, складывается интересная картина: заказчики активно интересуются решениями, тестируют их, но при этом не могут сформулировать требования, которым эти решения должны соответствовать.


Д. СЛОБОДЕНЮК

Дмитрий СЛОБОДЕНЮК, коммерческий директор, ARinteg: Популярны простые в использовании и доступные по цене продукты, предоставляющие высокий уровень защиты. Стоит отметить: еще не все пользователи осознали, что мобильные устройства необходимо защищать так же, как и стационарный компьютер.

Юрий АКАТКИН, директор, ФГУП «КБ полупроводникового машиностроения» ГК «Ростехнологии»: Поскольку нет требований к обеспечению комплексной безопасности мобильных устройств, на рынке конкурируют решения, скорее создающие у пользователя иллюзию информационной безопасности. Серьезные решения есть, но на рынке они представлены слабо. Пользователи пока не считают вопросы защищенности мобильных устройств актуальными для себя.

Границы бизнеса

«ИКС»: Какую роль могут/должны играть операторы связи в обеспечении инфобезопасности в корпоративных мобильных сетях?

О. ГУБКА: Основная задача операторов – предоставление услуг связи, обеспечение базовой безопасности и борьба с мошенничеством. В этом смысле их роль схожа с государственной. Защита корпоративных данных в мобильной сети – это задача их владельца.


Ю. АКАТКИН

Ю. АКАТКИН: С нашей точки зрения, это поле деятельности не для операторов связи. Здесь основную роль должны играть поставщики контента.


А. ХРАМЦОВ

Александр ХРАМЦОВ, исполнительный директор, «Телеком-Защита»: Операторы связи могут предоставлять (и предоставляют) корпоративным клиентам услуги, связанные с дополнительным анализом корпоративного трафика по заданным критериям (DPI, DLP). Решение этой задачи на стороне организации требует существенных инвестиционных затрат на приобретение специализированного оборудования, программного обеспечения для анализа трафика, услуг по внедрению и настройке.


Н. РОМАНОВ

Николай РОМАНОВ, технический консультант, Trend Micro Россия и СНГ: В контексте корпоративных ИТ-систем операторы связи никому ничего не должны. Единственная актуальная проблема, в решении которой могли бы принять участие и операторы, и государство, – регулирование рынка премиальных сервисов через короткие номера.


М. САВУШКИН

Михаил САВУШКИН, технический консультант, Symantec: При дальнейшем росте популярности решений для управления и защиты мобильных устройств станет актуальным управление защитой на уровне мобильного оператора. Это позволит контролировать передачу данных «близко» к устройству, переложить затраты на развертывание и поддержание системы защиты мобильных устройств непосредственно на оператора, получая услуги по подписке.

Андрей МЕЛУЗОВ, руководитель департамента ИТ-аутсорсинга, ГК «КОРУС Консалтинг»: В обеспечении информационной безопасности операторы связи сегодня играют минимальную роль. Скорее всего, такое положение сохранится и в дальнейшем. В мобильных сетях у операторов отсутствуют механизмы и возможности регулировать конфиденциальность как таковую. На мой взгляд, эту проблему максимально полно могут решить только специалисты внутри организации, сотрудники которой используют мобильные сети. Некоторые операторы мобильной связи предлагают ряд полезных в данном случае инструментов – удаленный канал VPN, различные мобильные офисные программы. Тем не менее создаваемые ими решения не покрывают всех требований, которые предъявляются к инфобезопасности в корпоративной среде.


А. МЕЛУЗОВ

С. ДЕШЁВЫХ: Операторы на этом рынке – одни из самых перспективных игроков. Они могут начать с простого, а именно с предустановки антивируса на устройства, которые продают. Но могут пойти и дальше: развернуть на своих мощностях полноценный MDM-сервис с поддержкой управления безопасностью мобильных устройств. Более того, операторы способны контролировать трафик своих клиентов, а это тоже возможность для предоставления дополнительных услуг безопасности.


.В. ЗАЛОГИН

Владимир ЗАЛОГИН, директор по специальным проектам, «С-Терра СиЭсПи»: Операторы связи добавляют к инфраструктуре безопасности корпоративных заказчиков новые монетизируемые услуги, отвечающие концепции «безопасность как сервис», в том числе системы аутентификации, использующие согласованные каналы доставки и идентификаторы устройств (сим-карт), размещение сервисов ИТ и безопасности в своих распределенных ЦОДах, предоставление заказчикам в пользование сертифицированных средств защиты.

А. ЧЕЧЕТКИН: Операторы уже предоставляют защищенные каналы связи для сотрудников компаний, позволяют ограничивать использование работниками интернета (путем блокирования развлекатель-

ных сайтов, установления максимального размера скачиваемого файла и т.д.). Также необходимо развивать механизмы, которые ограждают пользователей от посещения мошеннических сайтов, скачивания вредоносного ПО. Кроме того, можно совместно с ИБ- и ИТ-службами компании осуществлять профилактические действия: рассылать пользователям мобильных устройств памятки по информационной безопасности, новости об угрозах мобильным устройствам и т.п.

Пределы беспечности

«ИКС»: Как вы оцениваете уровень осведомленности корпоративных пользователей о безопасности мобильных устройств? Какими первоочередными знаниями в области мобильной инфобезопасности они должны обладать?


А. ВАСИЛЕНКО

Александр ВАСИЛЕНКО, глава представительства в России и СНГ, VMware: К сожалению, сегодня сотрудники большинства компаний плохо знакомы с корпоративной политикой информационной безопасности: они выносят конфиденциальную информацию за пределы компании, публикуют данные о проектах и заказчиках в социальных сетях, выкладывают корпоративные файлы в облачные хранилища (iCloud, Dropbox) и т.д. Вместе с тем компании редко ведут периодическое обучение своих сотрудников правилам инфобезопасности, требуют подписывать соответствующие документы при приеме на работу, информируют персонал о происходящих изменениях и т.п.


С. ЛАРИН

Сергей ЛАРИН, специалист по инфраструктурным решениям, Microsoft Россия: Осведомленность пользователей зависит от работы ИТ-службы компании, сотрудников, отвечающих за безопасность, и даже от работы HR-отдела. Сотрудник обязательно должен знать политику компании и, возможно, подписать дополнительное соглашение по этому поводу. Он должен понимать, что в своем ноутбуке он уносит кусочек компании, и относиться к этим данным так же, как к тому, что лежит у него на рабочем столе. Сотрудник также должен четко понимать, что делать, например, в случае утери или кражи устройства. В свою очередь, ИТ-службы должны быть готовы к подобным сценариям, т.е. данные должны быть зашифрованы, должна иметься система управления мобильными устройствами, которая позволит удаленно стереть данные или заблокировать оборудование и т.п.

С. ХАЛЯПИН: Пока приходится констатировать, что уровень осведомленности невысок. А набор знаний достаточно прост: устройства должны быть защищены сложным PIN-кодом; этот PIN-код не надо записывать на самом устройстве или выкладывать в общедоступное место; не следует проводить установку ПО из непроверенных источников от неизвестных производителей; для работы с корпоративными приложениями и данными необходимо использовать двухфакторную аутентификацию (смарт-карты, одноразовые пароли и т.д.); всё, что попало в облако, удалено оттуда быть не может.


С. ХАЛЯПИН

Василий ШУБИН, инженер по поддержке продаж в России и СНГ, LifeSize Communications: Пользователь должен понимать, «что такое хорошо, а что такое плохо». И в этом ему должны помочь коллеги из соответствующих подразделений компании. К примеру, сотрудник не должен бояться забыть сложный пароль (сбросить его не представляет проблемы), но опасаться несанкционированного доступа к ИТ-системе предприятия, если пароль будет угадан злоумышленником, он должен.


В. ШУБИН

О. ГУБКА: Безусловно, культура использования мобильных устройств еще низка, и здесь напрашивается аналогия с интернетом. Неосведомленность и беспечность – это серьезная проблема, которую надо решать. В деле повышения осведомленности пользователей мобильных устройств должны объединить усилия и корпоративные службы информационной безопасности, и операторы связи, и вендоры, и интеграторы, и отраслевые или иные ассоциации организаций-заказчиков, и государство – в рамках борьбы с мошенничеством.

ПОЛНЫЙ ТЕКСТ
Дискуссионного клуба читайте на
www iksmedia.ru