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.

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.

А. ХРАМЦОВ

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.

Н. РОМАНОВ

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.

М. САВУШКИН

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.

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.

.В. ЗАЛОГИН

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