Cisco Connected World. Глобальное исследование безопасности мобильного доступа: *основные данные и выводы исследования в отношении корпоративных ИТ*

Обзор

Чтобы получить более полную картину всех проблем в области безопасности, возникающих в связи с использованием мобильных устройств в бизнес-операциях, компания Cisco провела глобальное исследование, узнав у конечных пользователей со всего мира их опыт и мнение по этому вопросу. В отчете *Cisco Connected World. Глобальное исследование безопасности мобильного доступа* освещается ряд тем, в том числе:

- отношение сотрудников к использованию персональных (находящихся в их собственности) устройств и устройств, принадлежащих компании, для доступа к корпоративным сетям;
- типы личных и корпоративных устройств, используемых для доступа к сети;
- поведение сотрудников, использующих мобильные устройства, в сети Интернет;
- взгляды сотрудников на безопасность мобильных устройств.

Поскольку количество мобильных устройств на рабочем месте продолжает неуклонно расти, ИТ-организации и обслуживаемые ими компании могут воспользоваться результатами нашего исследования, чтобы решить, как лучше обеспечить своих сотрудников производительным, гибким и безопасным доступом к сети с любого устройства.

Введение

Во всем мире отмечается бурное развитие ИТ по двум направлениям. Это мобильный доступ в масштабе предприятия и рост популярности потребительских устройств, то есть использование сотрудниками предприятия потребительских устройств и облачных приложений в рабочих целях. Однако ИТ-подразделениям, особенно в крупных корпорациях, оказывается очень непросто идти в ногу с этими тенденциями и решать возникающие в связи с ними проблемы, например: ослабление традиционного периметра безопасности, резкий рост количества устройств, требующих обеспечения безопасности, а также требование со стороны сотрудников компаний (которое раздается все чаще и чаще) предоставить доступ к корпоративным ресурсам в любое время, из любого места и с использованием любого мобильного устройства по их выбору.

Перед ИТ-администраторами стоит непростая задача — найти оптимальный компромисс между защитой конфиденциальных корпоративных данных и предоставлением доступа к инструментам и информации, что необходимо для обеспечения высокой производительности работы сотрудников. Мобильные устройства могут быть легко утеряны или украдены, так же как и содержащаяся в них информация и данные для доступа. Сотрудники, использующие общедоступные сети для передачи данных на мобильные устройства, могут подвергнуть конфиденциальную информацию компании серьезным рискам. А пользователи, выходящие в Интернет со своих мобильных устройств, постоянно сталкиваются с опасностью веб-угроз, включая вредоносное ПО для кражи персональных данных.

Тем не менее, найти разумный баланс между этими двумя задачами необходимо хотя бы потому, что это вопрос не только безопасности. Развитие технологий мобильных устройств, интегрируемых в бизнес-операции, открывает перед нами возможности для постоянных экономически целесообразных инноваций, что, в свою очередь, обеспечивает повышение производительности и совершенствование совместной работы сотрудников. В мире повсеместных подключений, где правят бал сетевые технологии, использование мобильных устройств позволит организациям не только сохранить конкурентоспособность, но также привлечь и удержать наиболее талантливых и квалифицированных специалистов.

Прошлогодний *Технологический отчет Cisco Connected World*[1] изучал изменения во взглядах на работу, технологии и безопасность у студентов и молодых специалистов (нового поколения работников или конечных пользователей) по всему миру. Опрос Cisco Connected World. *Глобальное исследование безопасности мобильного доступа* охватывает сотрудников всех уровней. Исследование предполагает, что предприятиям еще предстоит внедрить множество базовых процедур безопасности как для мобильных устройств, так и для удаленного доступа к корпоративным данным. Не подлежит сомнению то, что организациям придется приложить особые усилия к созданию и исполнению надежных, но гибких политик, а также заняться обучением пользователей, чтобы научить их распознавать потенциальные угрозы и стараться их избегать.

Использование в работе персональных устройств и устройств, принадлежащих компании

Согласно результатам опроса *Cisco Connected World. Глобальное исследование безопасности мобильного доступа,* примерно равные количества респондентов используют для ежедневных рабочих задач персональные или служебные ноутбуки, настольные компьютеры, смартфоны или планшеты. Часть опрошенных используют и те, и другие.

Наиболее значимым выводом, конечно, является вывод о том, что использование личных устройств в рабочих целях становится вполне обычной практикой. Почти половина (45 %) опрошенных заявили, что работодатель выделяет им определенную сумму на приобретение собственного ноутбука, смартфона и других устройств по их выбору, а не снабжает всех сотрудников одинаковым оборудованием. Кроме того, многие работодатели оплачивают подписку на голосовую связь или передачу данных для тех личных устройств, которые сотрудники используют на работе.

Более половины респондентов считают, что принадлежащие компании устройства должны быть доступны для личного использования. Практически все опрошенные сочли немаловажным преимуществом обеспечение доступа к одним и тем же приложениям, рабочему столу и данным, а также к одинаковым пользовательским возможностям при работе на служебном или личном устройстве.

Задача для ИТ-подразделения:

- Как обеспечить защиту приложений и данных на всех устройствах?

[1] Технологический отчет Cisco Connected World , 2012 г.: http://www.cisco.com/en/US/netsol/ns1120/index.html.

Беспроблемный удаленный доступ

Согласно отчету *Cisco Connected World. Глобальное исследование безопасности мобильного доступа* , предприятиям все же удается в той или иной степени обеспечивать поддержку растущего количества мобильных и удаленных сотрудников. Свыше половины опрошенных отмечают, что в настоящее время у них есть возможность удобного подключения к корпоративной сети из любой точки и в любое время. При удаленном доступе к информации из корпоративной сети меньше всего трудностей приходится преодолевать респондентам из Бразилии, Индии и США. Это может свидетельствовать о том, что их работодатели обеспечили надежное подключение для своих удаленных и мобильных сотрудников. Однако выводы могут быть и прямо противоположными.

Интересно, что, хотя большинство опрошенных считают удаленный доступ привилегией, а не правом сотрудника, многие из них все же ожидают многого от удаленных подключений и жалуются на то, что их работодатели предоставляют недостаточно удобный доступ. В частности, респонденты из Китая, многие из которых рассматривают удаленный доступ как законное право сотрудника, указали на ограничения со стороны ИТ как причину наибольшей неудовлетворенности. В числе основных факторов, препятствующих удобному и беспроблемному удаленному доступу, другие опрошенные называют корпоративные политики, ограничения бюджета и нормативные требования отрасли.

Задача для ИТ-подразделения:

- Как обеспечить безопасность удаленных сотрудников — и не ухудшить пользовательские возможности?

Безопасные подключения

В то время как все больше сотрудников требует, чтобы им разрешили использовать на работе устройство по их выбору, многие также признают, что при внедрении концепции «Принеси на работу свое устройство» (BYOD) работодатель сталкивается с определенными рисками. Многие опрошенные полагают, что личный смартфон с подключением к Интернету создает большую угрозу безопасности, чем смартфон, принадлежащий компании.

Почти половина респондентов (46 %) уверены, что наиболее безопасный способ удаленного подключения — это использование ноутбука с проводным подключением. Однако преобладающее большинство сотрудников (60 %) заявили, что во время удаленной работы они иногда заимствуют беспроводное подключение у коллег или знакомых. (Примечание. 50 % пользователей из Индии утверждают, что постоянно заимствуют средства беспроводной связи.) Беспроводные подключения заимствуют прежде всего по двум причинам: из-за отсутствия доступа к другим интернет-подключениям, а также просто потому, что это удобно.

Задача для ИТ-подразделения:

- Как обеспечить безопасный удаленный доступ при беспроводном подключении?
- Как гарантировать, что наши средства безопасности одинаково хорошо работают на служебных и личных устройствах пользователей?

Поведение пользователей в сети Интернет и противостояние веб-угрозам

Согласно отчету *Cisco Connected World. Глобальное исследование безопасности мобильного доступа*, большинству сотрудников известно, что использование мобильных устройств связано с рисками для безопасности предприятия, однако многие тем не менее признаются, что позволяют себе рискованное поведение во время работы с мобильными устройствами. 26 % опрошенных заявили, что при использовании служебных устройств ведут себя более рискованно, чем при использовании личных устройств. По словам тех сотрудников, которые отваживаются на более рискованные действия при работе со служебными устройствами, причиной такого поведения является уверенность в том, что ИТ-отдел предоставит им необходимую поддержку, если что-то пойдет не так. (Это мнение, как правило, основано на убеждении в том, что установленное антивирусное ПО поможет обеспечить защиту.) Ниже перечислены примеры «рискованного» поведения при использовании мобильных устройств:

- **Использование приложений для совместной работы.** 40 % опрошенных заявили, что на своих мобильных устройствах они используют в рабочих целях такие приложения совместной работы, как средства голосовой связи, видеосвязи и веб-конференц-связи, приложения мгновенного обмена сообщениями, мобильные приложения и корпоративное социальное ПО. Часто приложения совместной работы имеют веб-интерфейс, и ИТ-отдел либо не в состоянии контролировать их использование, либо не осведомлен о том, что сотрудники пользуются этими средствами. Опрошенные работники из числа тех, кто не пользуется приложениями совместной работы на служебных или личных устройствах, в особенности в Китае, в качестве основного препятствия указывают соображения безопасности.
- **Загрузка конфиденциальных корпоративных данных на мобильное устройство.** Большинство опрошенных (63 %) заявили, что по меньшей мере иногда загружают конфиденциальные корпоративные данные на свой персональный компьютер или мобильное устройство. В некоторых регионах это особенно частое явление, например в Индии, где большинство конечных пользователей (58 %) «постоянно» загружают подобные данные. Поступавшие таким же образом респонденты из всех стран, участвовавших в опросе, в качестве причины называют то, что «информация должна быть повсюду со мной — неважно, безопасно это или нет».
- **Отсутствие защиты данных, загруженных на мобильное устройство.** Приблизительно 10 % участников опроса признаются, что они не принимают никаких мер, чтобы защитить данные, которые они загрузили на свое беспроводное мобильное устройство. Одна из причин такого поведения совершенно ясна — и может быть легко устранена путем обучения пользователей. Примерно половина тех, кто, по собственным словам, никогда не использует шифрование или пароли на своих беспроводных устройствах, отметили, что они не знают, как это сделать.

Еще один пункт, вызывающий опасения с точки зрения безопасности, — это веб-угрозы. Почти половина опрошенных работников сообщают, что при использовании служебных устройств они столкнулись с такими угрозами безопасности, как вирусы и фишинг. Еще большее количество сотрудников встретилось с аналогичными проблемами при использовании собственных устройств. Загрузка вредоносных файлов из Интернета, по-видимому, представляет собой не такую распространенную проблему. Лишь треть участников опроса заявили, что при работе на служебном или личном устройстве столкнулись с загрузкой вредоносных файлов.

Что касается сообщений об угрозе, появляющихся в виде всплывающих окон при работе на служебных или личных устройствах, то большинство респондентов открывают и внимательно просматривают уведомления, прежде чем решить, что делать дальше. (Правда, пользователи из Индии и Великобритании в среднем менее осторожны, чем работники из других стран, участвовавших в опросе, так как они чаще соглашаются с уведомлениями, не вникая в подробности.)

Задача для ИТ-подразделения:

- Как добиться «правильного поведения» от сотрудников, использующих мобильные устройства?
- Как защитить корпоративные данные на личных устройствах сотрудников?
- Эффективны ли предупреждения системы безопасности, которые получают пользователи?
- Проводится ли достаточное обучение пользователей?

Потерянные или украденные устройства

Потеря устройства, используемого для работы, будь то личное или служебное оборудование, может привести к серьезным последствиям для безопасности, включая потерю интеллектуальной собственности, что может повредить репутации компании, отрицательно сказаться на ее бренде или поставить под удар ее конкурентоспособность. Еще одним важнейшим вопросом безопасности для компаний являются нарушения требований по соблюдению безопасности данных, поскольку они могут снизить степень доверия заказчиков и привести к крупным штрафам или судебным разбирательствам.

Тем не менее большинство работников (60 %), принявших участие в опросе *Cisco Connected World. Глобальное исследование безопасности мобильного доступа*, утверждают, что они недавно совершали рискованные с точки зрения технологий поступки при использовании устройства, предназначенного для работы. Наиболее распространенные виды рискованного поведения — это заимствование чужих беспроводных подключений при работе удаленно или из дома, предоставление доступа к служебным устройствам лицам, не имеющих отношения к компании, или оставление устройства на виду внутри машины. Кроме того, по словам респондентов, за последние 12 месяцев у них были утеряны или украдены служебный либо личный планшет или портативный компьютер. Более чем у одной трети опрошенных были утеряны или украдены служебный или личный смартфон.

В общем и целом, пользователи полагают, что потеря устройства, принадлежащего компании, связана с несколько большими рисками, чем потеря личного устройства, используемого для работы. Примерно две трети участников опроса в числе основных угроз для корпоративной безопасности назвали следующие события: потерю служебного или личного устройства за пределами компании, запись учетных данных на листке бумаги или оставление устройства на виду в машине.

Задача для ИТ-подразделения:

- Как мы можем контролировать устройства в случае их потери или кражи?

Отношение к угрозам безопасности

Хотя большинство опрошенных признают, что потеря устройства за пределами рабочего места или поведение, способное привести к утрате данных для доступа к устройству, может подорвать корпоративную систему безопасности, результаты исследования свидетельствуют о том, что многие не уделяют должного внимания безопасности при работе с устройством — вне зависимости от того, пользуются они служебным или личным устройством.

В общем и целом, участники опроса *Cisco Connected World. Глобальное исследование безопасности мобильного доступа* указали на ряд причин, по которым они не всегда думают о соблюдении мер безопасности. Основная причина: на их взгляд, риски настолько малы, что не представляют собой угрозу безопасности. Некоторые пользователи отметили, что они не всегда уделяли внимание безопасности устройства, поскольку их ИТ-отдел не сообщил им о возможных угрозах.

Задача для ИТ-подразделения:

- Как лучше передать информацию о возможных угрозах безопасности, связанных с использованием устройств?

Отношение сотрудников к ИТ на работе

Согласно результатам опроса *Cisco Connected World. Глобальное исследование безопасности мобильного доступа,* политики и меры безопасности для защиты от угроз весьма различаются от компании к компании. И даже когда политики безопасности существуют, их часто игнорируют либо не реализуют или же они оказываются неэффективными.

58 % опрошенных отметили, что при первом приеме на работу они должны были подписать специальные соглашения по безопасности, касающиеся внутренних данных компании. Хотя большинство респондентов (77 %) сообщили, что они всегда соблюдают условия этих соглашений, почти четверть опрошенных заявили, что они не следуют им постоянно. Среди тех, кто не всегда соблюдает соглашение о безопасности, больше всего доля тех (42 %), кто, по собственным словам, «иногда забывает об этом».

Согласно результатам исследования, преобладающее большинство опрошенных (84 %) уверены в том, что ИТ-отдел их компании способен выявить угрозы безопасности. Свыше половины опрошенных сказали, что их ИТ-отдел регулярно проводит обучение по вопросам рисков для безопасности и управления безопасностью. Кроме того, свыше половины респондентов отметили, что ИТ-отдел заблаговременно предупреждает их о возможных рисках и угрозах. Как следствие, почти три четверти опрошенных признают, что стали более осторожными.

Задача для ИТ-подразделения:

- Как мы можем добиться выполнения политик?
- Эффективно ли мы обучаем пользователей — и насколько своевременно предоставляется такое обучение?

Заключение

Как следует из результатов опроса *Cisco Connected World. Глобальное исследование безопасности мобильного доступа*, мобильный доступ представляет собой неоднозначную тенденцию, ставящую ряд непростых задач перед предприятиями и ИТ-подразделениями по всему миру. Единого пути к достижению «безопасного мобильного доступа» не существует. Каждой крупной организации необходимо разработать собственный подход к мобильной безопасности, частично состоящий из политик, частично из обучения и частично из технологий, чтобы суметь удовлетворить потребности своих сотрудников, а также помочь им сохранить производительность и достичь основных бизнес-целей. Конечно, для формирования такого подхода потребуется время. [23]

Между тем, многие компании предпринимают важные шаги, как в направлении развития своей модели безопасности, чтобы она могла соответствовать потребностям современного мира повсеместных подключений, так и в попытках прийти к взаимопониманию с сотрудниками, требующими доступа к приложениям и устройствам, необходимым им для работы. Пытаясь найти «оптимальные» решения для множества задач и трудностей в сфере ИТ, кратко обрисованных в данном документе, руководство компаний проводит переоценку политик допустимого использования и кодекса корпоративной этики, обращая более пристальное внимание на предотвращение потери данных, а также стремится превратить безопасность компании в задачу № 1 для всех сотрудников на всех уровнях организации.

Защищенный доступ Cisco

Решение Cisco для защищенного доступа может помочь предприятиям и их ИТ-подразделениям удовлетворить растущим требованиям пользователей и устройств, при этом сведя к минимуму риски и нарушения безопасности, что обеспечивается благодаря созданию платформы, позволяющей объединять пользователей в любое время, в любой точке и посредством любого устройства. Благодаря этому решению вы сможете с уверенностью приступить к преобразованию рабочего пространства, внедряя концепцию BYOD, облачные технологии и средства совместной работы.

- Управляемая политиками унифицированная инфраструктура обеспечивает согласованную политику безопасного доступа для пользователей и устройств в корпоративной сети (проводной, беспроводной или VPN).
- Эффективная система безопасности включает также дополнительные уровни, что позволяет обеспечить высокую производительность и стабильные пользовательские возможности как на площадке заказчика, так и при удаленной работе.
- Упрощенное управление обеспечивает широкие возможности мониторинга, ускоряет устранение неполадок и позволяет организациям сосредоточить свои основные усилия на внедрении инноваций.

В основе решения Cisco для защищенного доступа лежит мощное сочетание защищенного мобильного клиента Cisco AnyConnect® Secure Mobility, межсетевых экранов нового поколения Cisco ASA 5500-X, платформы Cisco Identity Services Engine (ISE) и технологии Cisco TrustSec®.

Более подробную информацию о решении Cisco для защищенного доступа (Cisco Secure Access) и его компонентах вы найдете на странице http://www.cisco.com/en/US/netsol/ns1204/index.html - ~Products.

---

[2] Годовые отчеты Cisco по безопасности за 2011 и 2013 годы можно загрузить по адресу: http://www.cisco.com/en/US/prod/vpndevc/annual_security_report.html.

[3] Годовой отчет Cisco по безопасности за 2013 год: http://www.cisco.com/en/US/prod/vpndevc/annual_security_report.html.

Интеллектуальное решение Cisco BYOD

Cisco первой прокладывает дорогу в области внедрения концепции BYOD («Принеси на работу свое устройство»), предлагая компаниям гибкие варианты развертывания решений в сфере мобильного доступа или BYOD, а также простой выбор между платформой или сервисным подходом.

Кроме того, Cisco обеспечивает комплексный подход к эффективной разработке и контролю доступа к сети BYOD, а также к управлению доступом. Интеллектуальное решение Cisco BYOD предоставляет наиболее защищенную и комплексную систему управления оконечными устройствами и жизненным циклом сети. Благодаря комплексному управлению жизненным циклом сети оно упрощает ИТ-операции, обеспечивает беспрецедентное удобство работы для каждого пользователя, а также предоставляет организациям унифицированную политику защиты данных и инструменты управления, необходимые для поддержки рабочей среды BYOD.

Узнайте подробнее об интеллектуальном решении Cisco BYOD.

Инициатива Cisco «Любое устройство»

Cisco — одна из многих компаний по всему миру, работающих над обеспечением безопасности мобильного доступа для всех пользователей независимо от того, где они находятся или какое устройство хотят использовать. Сегодня Cisco управляет более чем 64 000 мобильных устройств, и сотрудники могут выбрать устройство себе по вкусу и безопасно подключиться к сервисам голосовой связи, видеосвязи и передачи данных из любой точки в соответствии с политикой Любое устройство.

Описание программы Cisco по внедрению концепции BYOD можно найти в двух последних *Годовых отчетах Cisco по безопасности*.[2] Когда Cisco достигнет последнего этапа этого запланированного «путешествия», которое займет несколько лет, компания станет в значительной степени независимой от местоположения и сервисов, а корпоративные данные по-прежнему будут в безопасности.[3]

МЕТОДОЛОГИЯ

Опрос 2012 года *Cisco Connected World. Глобальное исследование безопасности мобильного доступа* проводился в 10 странах на государственных языках соответствующих стран. В опросе приняло участие более 4600 человек. Мы отбирали респондентов по следующим критериям:

- житель Австралии, Бразилии, Великобритании, Германии, Индии, Италии, КНР, США, Франции или Японии;
- старше 21 года;
- работает на полную ставку;
- работает в компании с 10 или более сотрудниками;
- компания-работодатель не занимается маркетинговыми исследованиями, консалтингом в области ИТ и не является благотворительной организацией;
- сотрудник использует служебные или личные устройства в рабочих целях;
- несколько раз в год работает удаленно.

Штаб-квартира в США
Cisco Systems Inc.
Сан-Хосе, Калифорния

Штаб-квартира в Азиатско-Тихоокеанском регионе
Cisco Systems (USA) Pte. Ltd.
Сингапур

Штаб-квартира в Европе
Cisco Systems International BV Amsterdam,
Нидерланды

Корпорация Cisco насчитывает более 200 офисов и представительств по всему миру. Адреса, номера телефонов и факсов приведены на веб-сайте Cisco по адресу www.cisco.com/go/offices.

Отпечатано в США C11-728986-01 08/13