Насколько защищенными считают себя компании, и как на самом деле обстоят дела?

Когда дело касается мобильности, компании оказываются не настолько защищенными, насколько считают их руководители службы информационной безопасности. В рамках этого глобального опроса, в котором приняли участие 400 руководителей службы информационной безопасности, будет выявлено, насколько защищенными считают себя компании, и как на самом деле обстоят дела? Исследование включает в себя 5 ключевых параграфов, краткие выводы по каждому пункту представлены ниже.

Мобильная безопасность

- ✓ *44% респондентов считают, что безопасность их корпоративной мобильности находится на высоком уровне или на уровне выше среднего.*
- ✓ *Однако 41% участников опроса сталкивался со случаями нарушения мобильной защиты.*

На первый вопрос «Как вы оцениваете безопасность вашей корпоративной мобильности?» ответы оказались достаточно оптимистичными. 44% респондентов сказали, что уровень их мобильной защиты является выше среднего или находится на высоком уровне, при этом практически 42% уверены, что они, как минимум, находятся на среднем уровне.

Однако стоит обратить особое внимание на последующие вопросы и ответы, в которых содержится информация о реальном положении дел. Так, например, 41% участников опроса сталкивались со случаями нарушения мобильной защиты. Эти инциденты включают в себя как потерю данных по причине потери/кражи устройств, так и заражения вредоносным ПО и неавторизированный доступ.

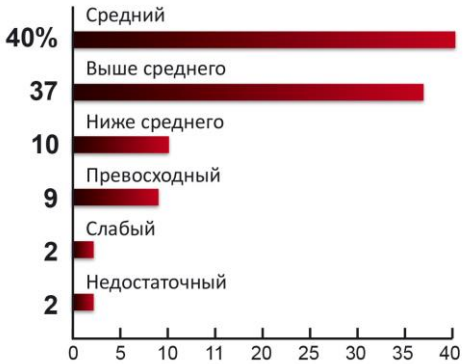
С какими типами нарушения безопасности, относящимися к мобильности, вы сталкивались в прошлом году?

Определение и обслуживание мобильных пользователей

✓ 54% участников опроса оценили на среднем уровне или на уровне ниже среднего способность их компаний определять, обеспечивать и защищать определенные группы мобильных пользователей. Практически 25% не могут различить уникальные группы пользователей.

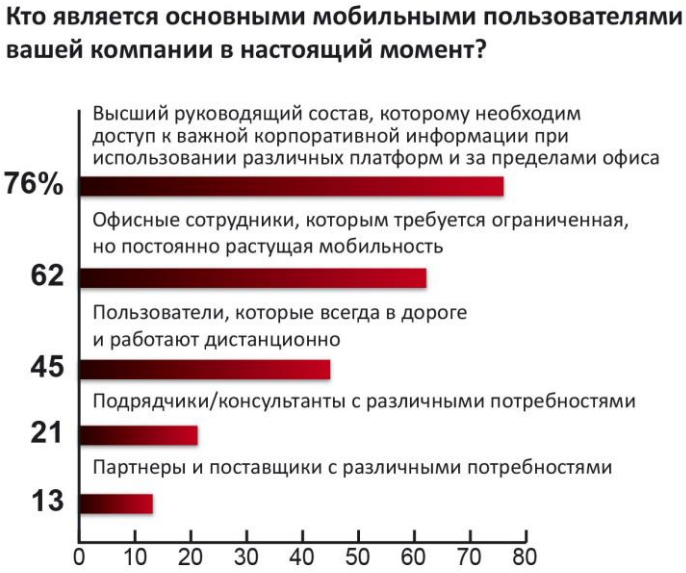
В очередной раз, когда участникам опроса задается общий вопрос, в данном случае о том, как они определяют и обслуживают определенные группы пользователей, 48% оценивают свои возможности как выше среднего или высокие.

Как вы можете оценить способность вашей компании определять, обеспечивать и защищать определенные группы мобильных пользователей?



Отвечая на вопрос о сотрудниках, которые являются основными мобильными пользователями компании, респонденты выделили следующие группы.
Конечно, высший руководящий состав возглавляет список. Они много времени проводят в деловых поездках, и им нужен постоянный и защищенный доступ к важной корпоративной информации.
Вторая группа – это традиционные сотрудники, работающие за пределами офиса. Они практически все время работают в мобильном режиме, поэтому им также нужен доступ к данным.
Но особое внимание следует обратить на третью группу сотрудников: традиционные офисные

сотрудники, которые лишь изредка работают в удаленном режиме, но которые все равно нуждаются во все большем количестве сервисов, включая приложения для обмена короткими сообщениями и файлами.



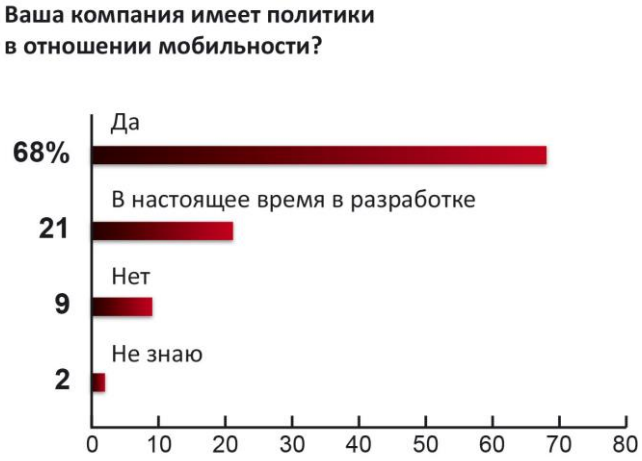
Кроме того, примерно 37% респондентов в настоящий момент определяют роли и доступ/привилегии, которые требуют эти роли, а 15% не разделяют группы вообще. Примерно 1/5 участников опроса в настоящий момент устанавливает элементы контроля безопасности в контекстном режиме, на основании динамической среды пользователя – где они находятся, какое устройство они используют, типы приложений и данных, к которым они пытаются получить доступ.

Определение и осуществление политик

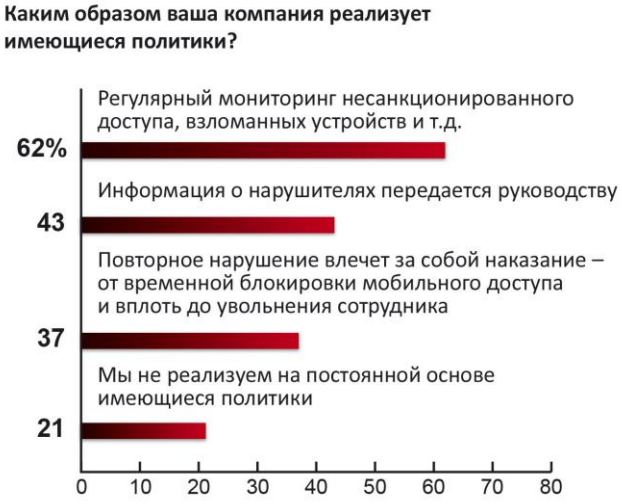
✓*1/3 респондентов не имеет политик обеспечения мобильной безопасности;*

✓*Из тех, кто имеет такие политики, только 62% сказали, что они выполняют регулярные проверки на предмет определения неавторизированного доступа, взломанных устройств, неразрешенных приложений и пр.*

С одной стороны, обнадеживает, что 2/3 компаний имеют политики. Однако уточняющий вопрос, который имеет очень важное значение, звучит так: Как часто эти политики проверяются и обновляются? Ведь даже принятая 3 года назад технология считается сильно устаревшей.



Удивительно, но 1/5 компаний не реализует на постоянной основе имеющиеся политики, а 2/3 респондентов не наказывают виновников нарушения политик.
62% сказали, что они выполняют регулярные проверки несанкционированного доступа, взломанных устройств и т.д. Но менее половины компаний заявили о том, что они передают руководству информацию о нарушителях политики.



Управление и мониторинг

✓*62% участников опроса поставили среднюю или ниже средней оценку при ответе на вопрос о способности их компаний защищать и контролировать корпоративную мобильность.*

✓*Основные средства контроля безопасности:*
Управление мобильными устройствами (58%)
Управление корпоративной мобильностью (37%)
Использование сетей VPN (35%)

В ходе данной части исследования выяснилось, что респонденты не слишком высоко оценивают способность своих компаний защищать и контролировать корпоративную мобильность. 62% респондентов определяют способность своих компаний как среднюю, и только 9% заявили, что она находится на высоком уровне.
Если посмотреть на используемые компаниями средства, то можно понять, почему участники опроса дали такие невысокие оценки.

Какие именно средства контроля мобильной безопасности использует ваша компания?

Хотя 2/3 компаний еще предстоит сделать многое для того, чтобы улучшить свою систему защиты, радует то, что 1/3 компаний внедрила следующие решения:

- Защищенные мобильные контейнеры для зашифрованных данных и приложений;
- Оценка риска обнаружения взломанных устройств;
- Сети VPN.

С помощью данных решений основная масса респондентов контролирует доступ к электронной почте (75%), но практически половина компаний обращает внимание на использование устройств (58%), использование сетей (47%) и использование приложений (44%). Стоит отметить, что 14% компаний контролируют доступ на базе сценариев.

Еще один вопрос, который был задан участникам исследования: Что определяют компании во время проведения проверок? Как правило, это неавторизированные приложения (31%), неразрешенные устройства и пользователи. Но самое удивительное, что практически ¼ всех

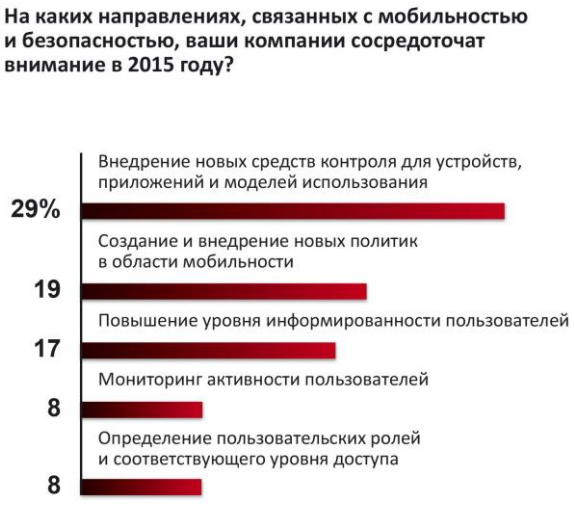
участников опроса не проводит регулярную проверку.

Планы компаний в отношении мобильности в 2015 году

✓Основные направления в отношении мобильности и безопасности в 2015 году: внедрение новых средств контроля для устройств, приложений и моделей использования (29%)

Отвечая на вопрос об угрозах, связанных с мобильностью, которые в первую очередь беспокоят респондентов, опасностью номер один было названо развитие мобильного вредоносного ПО. Другие угрозы включают в себя потерянные или украденные устройства, внутренние пользователи, которые непреднамеренно получили доступ к важной информации, и ненадежные пользователи, которые нарушают правила намеренно.

При этом в 2015 году 69% респондентов ожидают увеличение бюджета, а 15% полагают, что бюджет увеличится более чем на 10%.



Практически 1/5 респондентов собираются начать с создания и внедрения новых политик в области мобильности. А почти 1/3 хочет сделать следующий шаг и внедрить новые средства контроля для устройств, приложений и моделей использования. 28% респондентов планируют определить специальные пользовательские роли и соответствующий доступ/привилегии.

Говоря о подходе, который компании выберут для безопасности для основных групп пользователей, 28% респондентов планируют определить специальные пользовательские роли и соответствующий доступ/привилегии. А 27% планируют внедрить инструменты контроля безопасности на контекстной основе.

О компании Citrix

Компания Citrix (Citrix Systems, Inc. (NASDAQ:CTXS)) — лидер в области перехода к программно-определяемым рабочим местам, объединяющей виртуализации, управления мобильностью, сетевых технологий и решений по предоставлению программного обеспечения как услуги. Все эти направления помогают бизнесу и людям работать более продуктивно и лучше. Решения Citrix помогают организовать мобильность бизнеса, используя защищённые мобильные рабочие места, обеспечивающие сотрудникам непрерывный доступ к приложениям, десктопам, данным и коммуникациям с любого устройства, через любые сети и облака.

В 2014 году доход компании составил 3,14 миллиарда долларов США, решения Citrix используют более 330 000 организаций и более 100 миллионов пользователей во всем мире. Более подробная информация доступна по адресу www.citrix.ru

О компании Softprom by ERC

Softprom by ERC — ведущий Value Added Distributor программного обеспечения в СНГ, которому доверяют более 1000 партнеров. Официальный дистрибьютор компании Citrix на территории стран СНГ. www.softprom.com