5 ПЕРЕДОВЫХ МЕТОДОВ ПО ОБЕСПЕЧЕНИЮ ЗАИНТЕРЕСОВАННОСТИ ВСЕХ СОТРУДНИКОВ В БЕЗОПАСНОСТИ

Наибольший риск для информационной безопасности представляют ваши сотрудники. Используйте эти пять проверенных методов, чтобы усилить свою стратегию обеспечения безопасности и защитить свой бизнес.

«Если правила составляются вместе со всем коллективом, а знание требований безопасности является частью корпоративной культуры, они редко нарушаются»,

— СТЭН БЛЭК, ГЛАВНЫЙ ДИРЕКТОР CITRIX ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Современные высокомобильные сотрудники, количество возможных угроз перед которыми только увеличивается, находятся на передовой в борьбе за безопасность предприятия. Поэтому надежные стратегии обеспечения безопасности должны не только включать продуманные политики, жесткий контроль за их соблюдением и тщательный мониторинг / отчетность, но и отвечать потребностям и привычкам корпоративных пользователей.

«Именно в работе конечных пользователей безопасность проверяется на прочность», — заявляет Курт Рёмер, главный специалист Citrix по вопросам стратегии безопасности.

К сожалению, совместить безопасность и удовлетворенность сотрудников — дело не из легких. Сотрудники хотят получать доступ к информации из любого места, в любое время и с любого устройства, не замедляя работу из-за громоздкой системы защиты безопасности. Управляющие компании хотят защитить важную информацию без замедления темпов роста, инновационного развития и конкурентоспособности. ИТ-отделы хотят сохранить производительность персонала, сознавая при этом, что сотрудники и их устройства зачастую оказываются слабыми звеньями в цепи обеспечения безопасности.

Чтобы уравновесить эти конкурирующие интересы, руководители по обеспечению безопасности должны применять следующие передовые методы.

1. Обучайте пользователей

Осведомленный и бдительный персонал — первая линия защиты любой компании от угроз безопасности, поэтому обучение сотрудников безопасным способам работы независимо от местоположения и устройства должно стать приоритетной задачей.

Простое ознакомление с передовыми методами — верный шаг к провалу. Тщательно обдумайте, что из себя представляют ваши пользователи, чем они занимаются и что им необходимо. После этого доступным языком объясните им правила безопасности вашей компании, относящиеся к выполняемым ими должностным обязанностям.

«Все дело в релевантности, — говорит г-н Рёмер. — Всё, с чем вы знакомите сотрудника, должно отражать специфику его работы, а не основываться на универсальном подходе».

«Кроме того, эта информация должна быть индивидуальной», — добавляет Стэн Блэк, главный директор Citrix по обеспечению информационной безопасности. Например, в дополнение к обучению вопросам безопасности на работе компания Citrix дает своим сотрудникам советы на такие темы, как защита беспроводной домашней сети и обучение детей безопасному использованию Интернета.

«Мы стараемся соединить все образовательные занятия так, чтобы они отражали обучение безопасности во всех сферах жизни, а не только при работе в офисе», — подчеркивает г-н Блэк. Таким образом, обучение вопросам безопасности становится более значимым для сотрудников, и при этом охраняет конфиденциальные данные от плохо защищенных личных устройств.

2. Поддерживайте связь с организациями направления вашей деятельности

Тесное сотрудничество между руководителями ИТ-отделов и менеджерами направлений деятельности является основополагающей составляющей обеспечения надежной безопасности. Благодаря регулярным встречам с лицами, ответственными за принятие бизнес-решений, руководители по обеспечению безопасности могут уже на начальном этапе внедрять соответствующие защитные механизмы в новые бизнес-инициативы. Кроме того, подобные встречи служат источником необходимого детального перспективного обзора специфичных для бизнес-группы рисков и требований.

«Вы узнаете о рабочем процессе и потенциальных угрозах бизнесу то, что не смогли бы узнать в другой ситуации», — говорит г-н Блэк. — После этого вы сможете применять эту информацию при составлении своих планов обеспечения безопасности, делая их еще эффективнее».

3. Смотрите на правила безопасности с позиции современных возможностей и мобильности

При всей своей важности обучение в одиночку не сможет обеспечить надежную безопасность. Множество устройств, сетей и систем хранения данных, на которые сегодня полагаются сотрудники, неподвластны контролю ИТ-отдела.

«ИТ-отдел должен обновлять традиционные правила безопасности в соответствии с новой реальностью мобильных и облачных сервисов», — заключает г-н Рёмер.

Для начала обдумайте, насколько строгим будет ограничение доступа к данным вашей компании в соответствии с местоположением сотрудника и используемым им устройством. Большинство компаний применяют ступенчатые политики, согласно которым конфиденциальная информация защищается более тщательным образом, чем общедоступная, а доступ с потребительских и собственных устройств более ограничен, чем с защищенных корпоративных устройств.

Затем следует проверить, отражают ли ваши правила безопасности такие угрозы, как хранение корпоративных данных на личных устройствах, размещение паролей на мониторе компьютера или использование случайно найденного USB-накопителя.

4. Объективно и постоянно следите за соблюдением правил

Со временем к правилам безопасности перестанут относиться серьезно, если пользователи будут считать, что их нарушение не повлечет за собой никаких последствий, или, что еще хуже, если они будут считать, что обход правил повышает производительность. Правила необходимо пересматривать и обновлять в соответствии с развитием бизнеса. Поэтому руководители по обеспечению безопасности должны объективно и постоянно следить за соблюдением правил.

«Если правила составляются вместе со всем коллективом, а знание требований безопасности является частью корпоративной культуры, они редко нарушаются», — говорит г-н Блэк.

5. Обеспечьте бесперебойную автоматизацию безопасности

Чтобы еще больше снизить случаи нарушения правил, автоматизируйте процедуру контроля за их соблюдением с помощью программ для обеспечения безопасности. Так, множество решений для обеспечения безопасности могут по умолчанию выполнять назначенные сценарии, например шифровать корпоративные данные на мобильных устройствах. Кроме того, они могут внедрять более жесткие правила безопасности в ключевые составляющие взаимодействия пользователя с устройством, например автоматически запрещая сотрудникам запускать неразрешенные приложения внутри корпоративной сети или ограничивая набор приложений, с помощью которых можно открывать вложения электронной почты. Другие решения обеспечивают функции ведения журнала и отчетности, благодаря чему вы сможете доказать аудиторам, что вы добросовестно соблюдаете необходимые правила.

Но даже в этом случае программное обеспечение — лишь одна из составляющих системы безопасности.

«Для настоящей защиты своей компании вы должны знать группы направления своей деятельности и своих конечных пользователей», — утверждает г-н Рёмер.

Безусловно, самые лучшие стратегии обеспечения безопасности держатся на людях так же, как и на технологиях. ■

УПРОСТИТЕ И ЗАЩИТИТЕ ИСПОЛЬЗОВАНИЕ СОБСТВЕННЫХ УСТРОЙСТВ СОТРУДНИКОВ (BYOD) С ПОМОЩЬЮ ТЕХНОЛОГИЙ CITRIX

Свобода выбора очень скоро приведет к тому, что в большинстве организаций собственные устройства сотрудников станут предпочтительным средством работы. Это преобразует и то, как работают сотрудники — повышая производительность, степень их взаимодействия и уровень мобильности, — и то, как ИТ-отделы обеспечивают их бизнес-приложениями и данными.

Наиболее эффективный подход к работе с использованием собственных устройств сотрудников представляет собой четко определенную и исполняемую политику, опирающуюся на надежные технологии. Формальная политика должна пояснять, на кого она распространяется, использование каких устройств разрешено и какие для них будут доступны сервисы. Кроме того, она должна определять, кто и за что несет финансовую ответственность и в какой степени применима политика приемлемого использования. С решениями Citrix ИТ-отделы могут упростить управление и снизить затраты, позволяя при этом сотрудникам работать удобно, безопасно и непрерывно на устройстве любого типа вне зависимости от его принадлежности.

Использование возможности детального управления данными и приложениями позволяет обеспечить защищенный доступ к конфиденциальной деловой информации на личных устройствах сотрудников. ИТ-отдел получает возможность провижининга и контроля данных, приложений и устройств на основе идентификаторов пользователей для защиты информации от утери и хищения, соблюдая при этом конфиденциальность, требования регулирующих органов и стандарты управления рисками.

Чтобы узнать больше, посетите веб-сайт www.citrix.ru/secure