Автор: Артур Скальский © Babr24.com КОМПЬЮТЕРЫ , МИР 2914 13.11.2006, 19:06 357

Глобальное исследование показало непонимание роли информационных технологий в обеспечении корпоративной безопасности

Компания Cisco® опубликовала результаты второго глобального исследования особенностей работы удаленных сотрудников. Исследование показало, что удаленные сотрудники неправильно понимают роль ИТ-подразделений, и это может оказать отрицательное влияние на корпоративную и личную безопасность.

По мнению удаленных сотрудников, ИТ-подразделения слишком поздно реагируют на проблемы, а ИТ-менеджеры пользуются меньшим авторитетом, чем представители бизнеса.

В исследовании, проведенном независимой фирмой летом 2006 года, было опрошено более тысячи удаленных сотрудников и ИТ-менеджеров в 10 странах (США, Великобритании, Франции, Германии, Италии, Японии, Китае, Индии, Австралии и Бразилии). Опрос продолжил предыдущее исследование (результаты которого были опубликованы в октябре), показавшее противоречия между знаниями удаленных сотрудников и их практическим поведением в области безопасности. В рамках нового исследования были опрошены те же сотрудники с тем, чтобы выяснить их мнение о роли ИТ-подразделений в обеспечении безопасной работы. Были опрошены и ИТ-специалисты, чтобы узнать, какова, по их мнению, их роль в глазах конечных пользователей.

Результаты опроса оказались во многом неожиданными. В шести из 10 стран (включая США) большинство удаленных сотрудников считает, что контролировать их работу имеют право только прямые начальники, но не ИТ-подразделения. А во Франции многие респонденты (38%) заявили, что контролировать их работу не имеет право никто. Доля тех, кто признает такое право за ИТ-подразделениями, составила 33%.

В США и Франции, а также в Австралии, Бразилии, Китае и Великобритании удаленные сотрудники считают, что их работу должны контролировать только бизнес-менеджеры, но не менеджеры ИТ-подразделений. Респонденты из Индии, Италии, Японии и Германии высказали противоположное мнение, однако в Японии и Германии треть опрошенных заявили, что всю ответственность за безопасность их работы несут прямые начальники, независимо от прав и полномочий, которыми обладают ИТ-подразделения. Среди респондентов не было ИТ-профессионалов. Это означает, что, по их мнению, менеджеры по продажам, маркетингу, учету, кадрам, технической поддержке, эксплуатации и другим сферам бизнеса имеют больше прав по коррекции онлайнового поведения удаленных сотрудников, чем специалисты в области информационных технологий.

В среднем около 13% опрошенных вообще не признают никакого контроля за использованием служебных компьютеров. Больше всего таких людей во Франции (38%), но и в Италии их больше трети (35%). Среднемировой показатель превышен также в Японии (22%), США (14%) и Австралии (14%).

«Результаты исследования указывают на влияние социальной и корпоративной культуры на представления и поведение удаленных сотрудников, - говорит Джефф Плейтон (Jeff Platon), вице-президент Cisco по маркетингу в области безопасности. - Например, в Германии 71% опрошенных согласны с тем, что ИТ-подразделения должны контролировать их работу, но треть респондентов считает, что и менеджеры должны разделять ответственность за обеспечение безопасности. Каждый четвертый указывает, что ответственность за безопасность своей работы должны нести и сами сотрудники. Многие опрошенные в Германии ощущают общую ответственность всех сотрудников компании за информационную безопасность».

«Во всех странах, кроме Германии, руководители ИТ-подразделений сталкиваются с проблемой утверждения своего престижа в глазах конечных пользователей», - считает Джефф Плейтон. Поэтому не удивительны результаты опроса самих ИТ-сотрудников о том, какую роль отводят им удаленные сотрудники. Более

половины респондентов (53%) считают, что пользователи не считают, что ИТ-подразделения имеют право знать, как используются служебные компьютеры. Только в Индии и Бразилии большинство респондентов придерживаются противоположной точки зрения.

Как считает Джон Стюарт, руководитель службы информационной безопасности Cisco, «Это не проблема, а ниша, в которой ИТ-подразделения могут утвердить себя в качестве доверенных советников по вопросам безопасности».

«ИТ-подразделения понимают, что сотрудники знают о проблемах безопасности, но часто не понимают, что их собственное поведение ставит корпоративную безопасность под угрозу, - говорит он. - Обучение сотрудников и распространение правильных подходов - вот ключи к решению этой проблемы. ИТ-подразделения и службы безопасности вместе с высшим руководством компании должны разработать программы по обучению сотрудников навыкам безопасной работы и повышению их ответственности. Хотя для защиты от сетевых угроз (а эти угрозы возникают всегда, если к одной сети подключается множество людей с разными интересами) ИТ-подразделения обязательно должны использовать упреждающие "проактивные" технологии, но в конечном итоге безопасная корпоративная культура возникает только при сочетании упреждающих методов с хорошо защищенными продуктами и обучением сотрудников».

Джефф Плейтон считает, что результаты первого опроса, опубликованные в прошлом месяце («Теория и практика поведения удаленных сотрудников: несмотря на осведомленность о рисках, многие из них предпринимают рискованные действия», http://www.cisco.com/global/RU/news/releases/0872.shtml), подчеркивают важность слов Стюарта.

«Две трети удаленных сотрудников знают, что удаленная работа требует повышенной осторожности. – говорит Плейтон. – Однако многие из них допускают рискованные действия при использовании служебных компьютеров. Таким образом, знания сотрудников противоречат их поведению».

К рискованным действиям относится подключение к соседским беспроводным сетям, открытие подозрительных электронных писем, доступ к корпоративной информации с помощью личных устройств и доступ посторонних лиц к служебному компьютеру. В свое оправдание удаленные сотрудники приводят множество доводов, например: «не думаю, что это увеличивает угрозу», «моя компания не знает об этом, а если знает, то не возражает», «другие сотрудники поступают так же».

Противоречие между знаниями удаленных сотрудников и их практическим поведением, приводимые "оправдательные доводы" и отношение сотрудников к роли ИТ-подразделений говорят о том, что руководителей ИТ-служб и служб безопасности должны занять позицию доверенного советника по безопасности в своей компании, - говорит Стюарт. - Исследование показало, что безопасность – дело каждого сотрудника. ИТ-подразделения могут и обязаны довести эту идею до всех сотрудников, чтобы те осознали тесную связь между своим поведением и угрозами.

Укрепление безопасности включает формирование единой позиции по этому вопросу в высшем руководстве компании, назначение советников по безопасности, обучение сотрудников, проведение «адресных» мероприятий и введение наград и других стимулов. Все эти меры нужно предпринимать глобально, во всей компании, но с учетом региональных особенностей.

"Большинство служб ИТ-безопасности все еще находятся «в тени», занимая выжидательную позицию, и руководство просто не знает, что эти службы могут предотвращать падение производительности и потерю данных. – добавляет Стюарт. – Проводя консультации и обучая конечных пользователей, ИТ-подразделения могут закрепить за собой репутацию доверенного советника по безопасности. Это то, что крайне необходимо не только руководителям ИТ-служб и служб безопасности, но и всей компании".

Автор: Артур Скальский © Babr24.com КОМПЬЮТЕРЫ , МИР 2914 13.11.2006, 19:06 357
URL: https://babr24.com/?ADE=33893 Bytes: 7313 / 7313 Версия для печати Скачать PDF

Связаться с редакцией Бабра:
newsbabr@gmail.com

НАПИСАТЬ ГЛАВРЕДУ:

Телеграм: @babr24_link_bot
Эл.почта: newsbabr@gmail.com

ЗАКАЗАТЬ РАССЛЕДОВАНИЕ:

эл.почта: bratska.net.net@gmail.com

КОНТАКТЫ

Бурятия и Монголия: Станислав Цырь
Телеграм: @bur24_link_bot
эл.почта: bur.babr@gmail.com

Иркутск: Анастасия Суворова
Телеграм: @irk24_link_bot
эл.почта: irkbabr24@gmail.com

Красноярск: Ирина Манская
Телеграм: @kras24_link_bot
эл.почта: krasyar.babr@gmail.com

Новосибирск: Алина Обская
Телеграм: @nsk24_link_bot
эл.почта: nsk.babr@gmail.com

Томск: Николай Ушайкин
Телеграм: @tomsk24_link_bot
эл.почта: tomsk.babr@gmail.com

Прислать свою новость

ЗАКАЗАТЬ РАЗМЕЩЕНИЕ:

Рекламная группа "Экватор"
Телеграм: @babrobot_bot
эл.почта: eqquatoria@gmail.com

СТРАТЕГИЧЕСКОЕ СОТРУДНИЧЕСТВО:

эл.почта: babrmarket@gmail.com

Подробнее о размещении

Отказ от ответственности

Правила перепечаток

Соглашение о франчайзинге

Что такое Бабр24

Вакансии

Статистика сайта

Архив

Календарь

Зеркала сайта