Автор: Артур Скальский КОМПЬЮТЕРЫ, МИР 2535 10.10.2007, 14:43 153

Основные советы по обеспечению сетевой безопасности бизнеса

ИТ-среда невероятно сложная, а потребность в повышении уровня безопасности ежедневно растет. Европейцы, похоже, хорошо понимают, насколько важную роль в успехе их бизнеса играет безопасность.

Согласно исследованию Forrester Research, проведенному в 2007 г. среди европейских компаний, безопасность является наиважнейшим фактором. 42% организаций планируют увеличить свои расходы на безопасность в 2007 г. по сравнению с 2006 г., столько же компаний не собираются изменять свои бюджеты в данной области, и лишь семь процентов планируют сократить свои расходы на безопасность.

Когда речь заходит об обеспечении безопасности данных, предполагается, что ответственность за безопасность и выполнение мероприятий по снижению уровня риска в этой области возьмут на себя ИТ-менеджеры. Компании могут предпринимать целый ряд мер по обеспечению безопасности, но эти отдельные меры являются лишь частью организованного комплексного подхода. Определение иерархии уровней безопасности и обучение всех сотрудников являются важными элементами продуманного корпоративного подхода, который и позволяет отличить хорошо спланированную систему защиты от слабой и поверхностной.

Существуют как внешние, так и внутренние угрозы для информационных активов компании; как следствие, критически важно, чтобы организации предприняли меры предосторожности в отношении и тех, и других. По результатам недавнего исследования, проведенного корпорацией Intel, 52% ИТ-менеджеров в Европе считают своей главной задачей поддержание высокого уровня безопасности бизнес-процессов.

Корпорация Intel обладает успешным опытом в области обеспечения защиты важных данных по всему миру. Вот некоторые советы по достижению высокого уровня безопасности – в какой бы области компания ни вела свой бизнес:

• Установите приоритеты для информационных активов: выясните коммерческую значимость данных и соответствующим образом расставьте приоритеты уровней безопасности.

• Разработайте соответствующую политику по информационной безопасности: сформулируйте действующую политику по информационной безопасности, нацеленную на достижение коммерческих целей компании. Будьте реалистичными в своих ожиданиях.

• Сокращение энергопотребления: компании могут снизить расходы, сократив дорогостоящие и отнимающие много времени посещения рабочих мест пользователей техническими специалистами, а также усовершенствовав схему потребления электроэнергии, используя функцию отключения ПК и безопасного его включения при необходимости.

• Будьте осведомлены о внутренних угрозах: убедитесь в том, что доступ к информации открыт лишь авторизованным пользователям. Очень часто компании сосредотачиваются на обеспечении безопасности от внешних угроз, забывая о том, что основной риск для активов компании могут представлять внутренние угрозы. Управление доступом и разграничение обязанностей играют важную роль в защите критических данных и информации.

• Обучение: обучайте своих людей. Очень важно, чтобы команда понимала важность и значимость политики обеспечения информационной безопасности и была в состоянии выполнять соответствующие действия. Регулярное обучение важно для разработки всеобъемлющей и интегрированной стратегии по обеспечению информационной безопасности.

• Проактивный мониторинг и управление рисками: создайте в компании группу «быстрого реагирования» из сотрудников различных отделов, должным образом обученных и готовых при необходимости взять на себя руководство по обеспечению информационной безопасности.

• «Правильная технология»: используйте для работы правильные инструменты. При правильном использовании технология может предотвратить нарушение политики информационной безопасности и ускорить исправление ситуации. Компаниям необходимо действовать проактивно и быть готовыми применять текущие решения для обеспечения безопасности, чтобы суметь остаться на плаву в условиях постоянно меняющихся угроз.

• Встроенное, а не «пристроенное»: ключом ко всему является интеграция – вкладывайте средства в компьютерное оборудование со встроенными функциями обеспечения безопасности на аппаратном уровне, вместо того чтобы полагаться на отдельные средства, на интеграцию которых ИТ-менеджер потратит часы своего рабочего времени.

Автор: Артур Скальский © Babr24.com КОМПЬЮТЕРЫ, МИР 2535 10.10.2007, 14:43 153
URL: https://babr24.com/?ADE=40380 Bytes: 4202 / 4202 Версия для печати

Телеграм: @babrobot_bot
эл.почта: eqquatoria@gmail.com

СТРАТЕГИЧЕСКОЕ СОТРУДНИЧЕСТВО:

эл.почта: babrmarket@gmail.com