Проблема непрерывности бизнеса

Проф. Думная Н.Н.

Обеспечение **непрерывность бизнеса компании -** сохранение его работоспособности в нештатных ситуациях, вызванных действием природных, технических, человеческих факторов.

Корпорация *Symantec* выпускает периодические доклады (***Internet Security Threat Report***), посвященные анализу атак, ведущихся из Интернета, уязвимых мест компьютерных систем, вредоносных программ.

Наибольшее число компьютерных атак - из США, далее идут Китай и Германия.

Угрозы непрерывности бизнеса

- **Увеличивается потенциальная опасность раскрытия конфиденциальной информации.**

  Связана с широким распространением «троянских» компонентов – шпионских программ.

  Среди 50 наиболее распространенных образцов вредоносного кода 54 % относились к угрозам утечки конфиденциальной информации. Девять из десяти наиболее часто обнаруживаемых шпионских программ поставлялись вместе с другим программным обеспечением.

Symantec

Угрозы непрерывности бизнеса

- Растет число атак, связанных с финансовым мошенничеством фишингом (от англ. *phishing* — метод хищения конфиденциальных сведений, относящихся к финансам, например, паролей, номеров кредитных карточек и т. п.).
  В 2004 г. фильтры *Symantec Brightmail AntiSpam* блокировали в среднем 33 млн. попыток фишинга.

Угрозы непрерывности бизнеса

- Особая группа риска – мобильные сотрудники.

  Почти 71 % респондентов заявили, что корпоративные мобильные компьютеры используются вне офиса и затем подключаются к сети, что создает большой риск для их компаний.

Symantec

Угрозы непрерывности бизнеса

- Компьютерное хулиганство - хакерские атаки.
- Вирусные эпидемии. Общее число разновидностей вирусной инфекции для 32-разрядных версий Windows составило почти 17,5 тыс.
- Другие угрозы: сбой электропитания, разрядка аккумуляторных батарей,, и т.п.

Мнение пользователей

- 91 % опрошенных называют качество защиты информационных ресурсов своей компании хорошим, хотя 35 % участников опроса не смогли помешать программе-шпиону отослать конфиденциальную информацию за пределы компании.
- 8 % предприятий, принявших участие в опросе, не предпринимали никаких мер защиты, кроме установки сетевого экрана и антивирусных продуктов.

Исследование Stress in Security компании Websense

Интересен опыт США, где высокий уровень риска в деятельности компаний привел к необходимости разработки нормативно-правовой базы, регламентирующей направление «непрерывности бизнеса».

Таблица. Законодательные требования по BCP в США

Сектор экономики	Требования
Медицина	Наличие документированного, протестированного BCP.
Финансовые услуги и банковское дело	Совет директоров несет ответственность за обеспечение полноценного восстановления бизнеса и сопряженного с ним работоспособного BCP. Устанавливаются требования к банковским организациям по разработке и поддержке BCP. Устанавливаются общие требования к широкому планированию этого направления работ.
Публичные компании	Устанавливается ответственность совета директоров и управляющих высшего звена к защите информации.
Все компании	Действует закон о резервировании и требованиях по восстановлению компьютерных данных, содержащих информацию о налогах.
Электронная коммерция	Организации обязаны резервировать данные, хранящиеся в электронных системах денежных переводов, включая пункты продаж.
Федеральное правительство	Должны существовать планы обеспечения безопасности всех федеральных компьютерных систем. Все департаменты и агентства должны планировать поддержку непрерывности важнейших операций.
Правительство	Проводится политика присвоения персональной ответственности за План обеспечения непрерывности бизнеса внутри государственных структур.