Основы безопасности информационных систем

Докладчик
Microsoft

Содержание

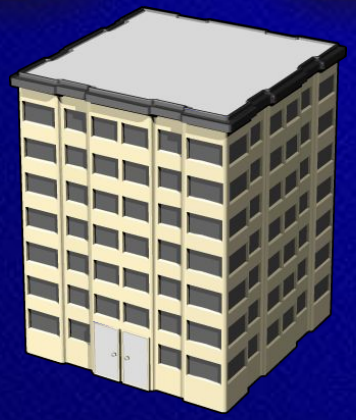
- Значение информационной безопасности
- Управление рисками
- Глубокая оборона
- Необходимые действия при защите от атак
- Десять законов информационной безопасности

Последствия нарушения безопасности

Потери доходов

Ухудшение репутации

Снижение доверия инвесторов



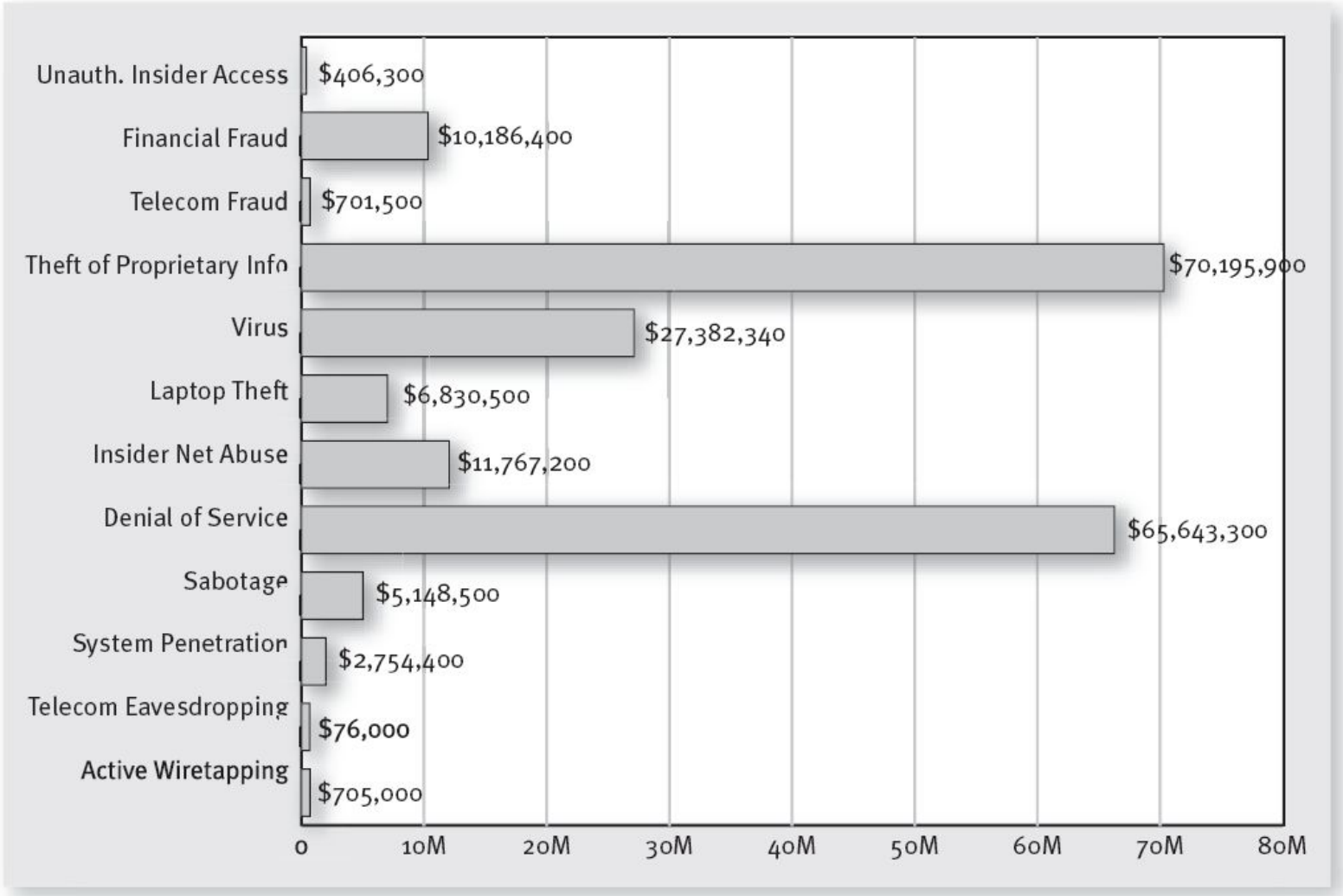
Потеря или компрометация данных

Снижение доверия клиентов

Правовые последствия

Нарушение бизнес-процесса

Финансовые потери



CSI/FBI 2003 Computer Crime and Security Survey
Source: Computer Security Institute

2003: 251 Respondents/47%

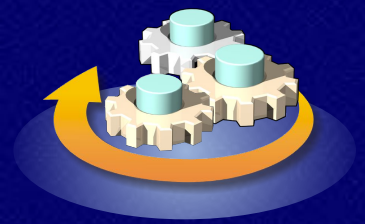
Содержание

- Значение информационной безопасности
- Управление рисками
- Глубокая оборона
- Необходимые действия при защите от атак
- Десять законов информационной безопасности

Дисциплина управления рисками

- Оценка
  - Анализ объектов
  - Идентификация угроз
  - Анализ и расстановка приоритетов
  - Планирование, назначение и отслеживание действий по работе с рисками

- Разработка и внедрение
  - Разработка и тестирование процесса исправления
  - Сохранение знаний



- Операции
  - Повторная оценка объектов и рисков
  - Стабилизация и применение новых или измененных контрмер

Оценка и анализ объектов

Приоритеты объектов (шкала от 1 до 10)

1. Сервер обеспечивает базовую функциональность и не влияет на финансовую сторону бизнеса
3. Сервер содержит важную информацию, данные могут быть быстро восстановлены
5. Сервер содержит важную информацию, восстановление данных потребует времени
8. Сервер содержит важные бизнес-данные, его потеря существенно повлияет на продуктивность всех пользователей
10. Сервер имеет критически важное значение для бизнеса, его потеря повредит конкурентоспособности компании

Классификация сервера	Приоритет
Контроллеры корневого домена	8
Контроллеры дочерних доменов	8
Корневой сервер DNS	4
Дочерние серверы DNS	5
Серверы WINS	3
Серверы DHCP	1
Серверы файлов и печати	8
Интранет-портал компании	10
Порталы отделов	8
Web-сервер отдела кадров	7

Идентификация угроз (STRIDE)

Тип угрозы	Примеры
Имитация (Spoofing)	◆ Подделка электронных сообщений ◆ Подделка ответных пакетов при аутентификации
Фальсификация (Tampering)	◆ Модификация данных, передаваемых по сети ◆ Модификация файлов
Отречение (Repudiation)	◆ Удаление критичного файла или совершение покупки с последующим отказом признавать свои действия
Раскрытие информации (Information disclosure)	◆ Несанкционированный доступ или незаконная публикация конфиденциальной информации
Отказ в обслуживании (Denial of service)	◆ Заполнение сети пакетами «SYN» ◆ Загрузка сетевого ресурса большим количеством поддельных пакетов ICMP
Повышение привилегий (Elevation of privilege)	◆ Получение системных привилегий через атаку с переполнением буфера ◆ Незаконное получение административных прав

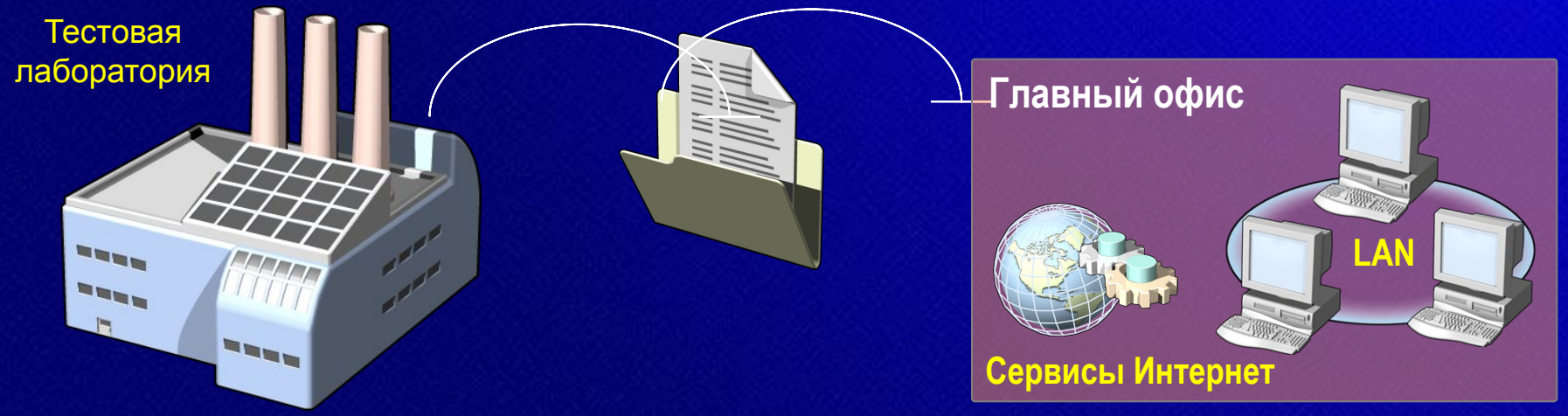
Анализ рисков

- Основные цели анализа рисков
  - Идентификация угроз
  - Определение степени воздействия угрозы
  - Обеспечение баланса между степенью риска и стоимостью противодействия
- Вычисление рейтингов угроз по модели DREAD
  - Установить рейтинг (от 1 до 10) для каждой из пяти областей и взять среднее значение
    - Ущерб (**D**amage)
    - Воспроизводимость (**R**eproducibility)
    - Используемость (**E**xploitability)
    - Затрагиваемые пользователи (**A**ffected Users)
    - Открытость (**D**iscoverability)
- Степень риска = Приоритет объекта * Рейтинг угрозы

Разработка и внедрение политики безопасности

- Управление конфигурациями
- Управление обновлениями
- Мониторинг систем
- Аудит систем
- Операционные политики
- Операционные процедуры

Сохранение знаний и обучение



- Формализация процесса накопления знаний и опыта, полученных при анализе угроз и уязвимостей системы
- Последующее обучение персонала

Повторная оценка и изменения

- При изменении или при появлении новых объектов необходимо проводить повторную оценку и анализ
  - Модификация политики безопасности

Общая картина операций по управлению рисками

Содержание

- Значение информационной безопасности
- Управление рисками
- Глубокая оборона
- Необходимые действия при защите от атак
- Десять законов информационной безопасности

Защита на всех уровнях

- Упрощает процесс обнаружения вторжения
- Снижает шансы атакующего на успех

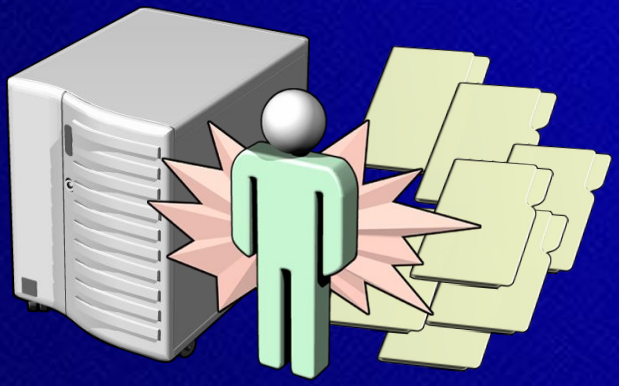
Пользователи часто забывают о безопасности

Социальный инжиниринг

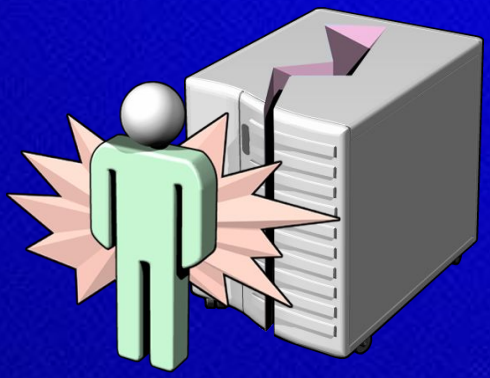
Политики, процедуры и обучение

Своевременное обучение пользователей правилам и процедурам защиты

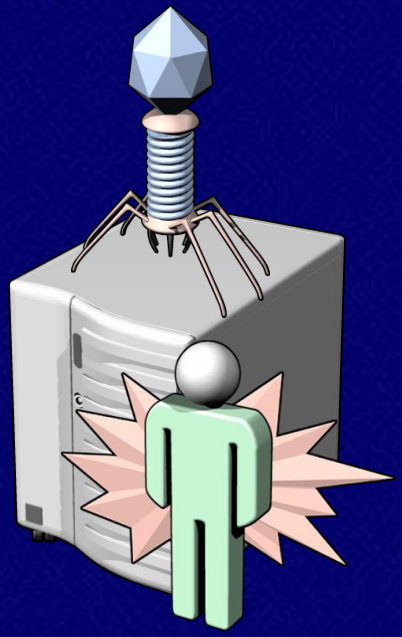
Воздействия при физическом доступе



Просмотр, изменение, удаление файлов



Порча оборудования



Установка вредного программного кода

Демонтаж оборудования

Физическая защита

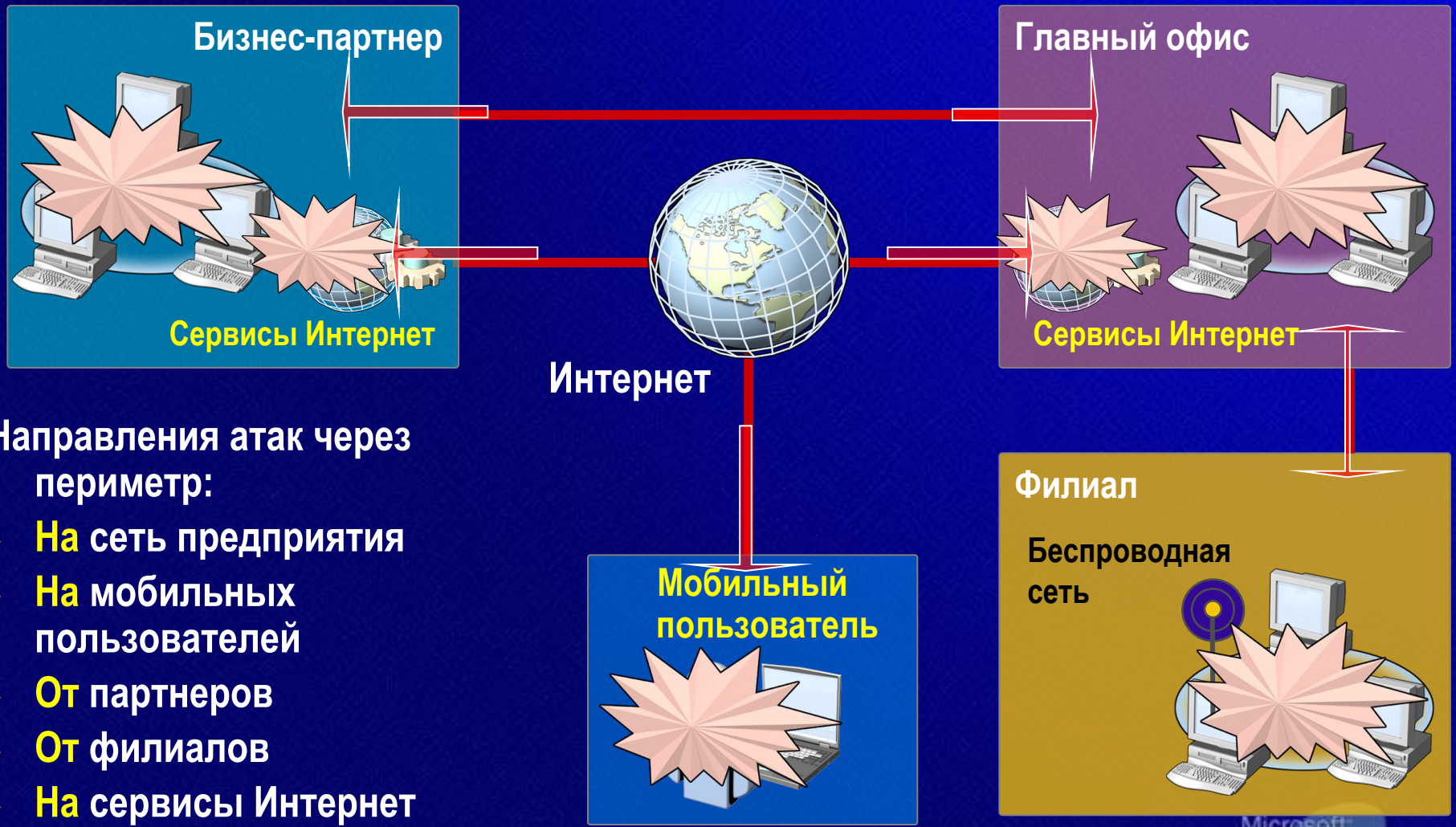
- Блокировка дверей, средства слежения и сигнализации
- Выделенный персонал для охраны
- Жесткая регламентация процедур доступа в серверные помещения
- Системы видео-наблюдения
- Удаление лишних устройств ввода данных
- Средства удаленного администрирования

Периметр информационной системы

В периметр системы входят подключения к

- Интернет
- Филиалам
- Сетям партнеров
- Мобильным пользователям
- Беспроводным сетям
- Интернет-приложениям

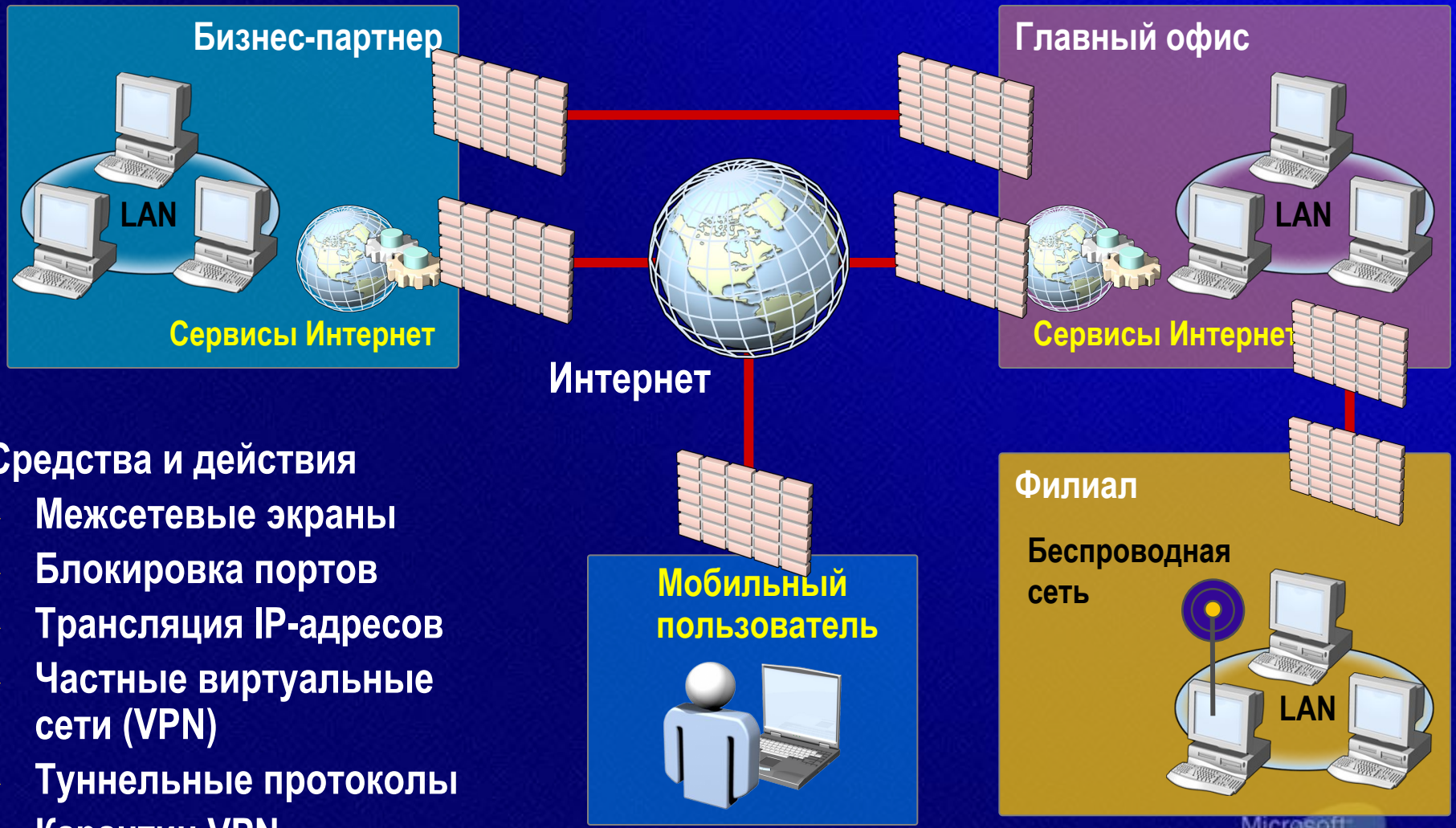
Компрометация периметра



Направления атак через периметр:

- На сеть предприятия
- На мобильных пользователей
- От партнеров
- От филиалов
- На сервисы Интернет
- Из Интернет

Защита периметра



Средства и действия

- Межсетевые экраны
- Блокировка портов
- Трансляция IP-адресов
- Частные виртуальные сети (VPN)
- Туннельные протоколы
- Карантин VPN

Угрозы локальной сети

Защита локальной сети

- Взаимная аутентификация пользователей и сетевых ресурсов
- Сегментация локальной сети
- Шифрование сетевого трафика
- Блокировка неиспользуемых портов
- Контроль доступа к сетевым устройствам
- Цифровая подпись сетевых пакетов

Компрометация компьютера

Небезопасная конфигурация операционной системы

Неконтролируемый доступ

Распространение вирусов

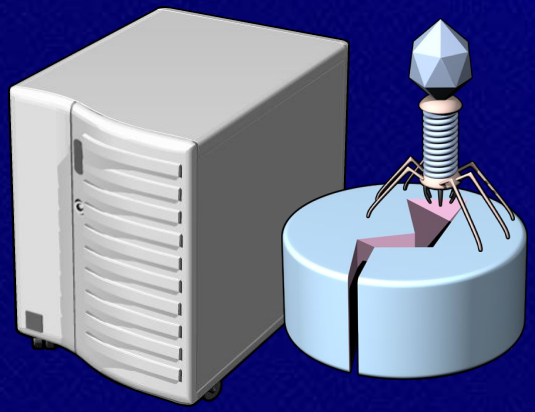
Использование уязвимостей операционной системы

Защита компьютеров

- Взаимная аутентификация пользователей, серверов и рабочих станций
- Защита операционной системы
- Установка обновлений безопасности
- Аудит успешных и неуспешных событий
- Отключение неиспользуемых сервисов
- Установка и обновление антивирусных систем

Компрометация приложений

- Потеря приложения
- Исполнение вредного кода
- Экстремальная загрузка приложения (DoS)
- Несанкционированные и некорректные операции



Серверные приложения
(Exchange Server, SQL Server и др.)

Настольные приложения для создания и модификации данных

Защита приложений

- Включать только необходимые службы и функции приложений
- Настройка параметров защиты приложений
- Установка обновлений безопасности
- Запуск приложений в контексте с минимальными привилегиями
- Установка и обновление антивирусных систем

Компрометация данных

Несанкционированный доступ к файлам хранилища службы каталогов

Защита данных

- Защита файлов средствами Шифрующей файловой системы (EFS)
- Настройка ограничений в Списках контроля доступа
- Система резервного копирования и восстановления
- Защита на уровне документов с помощью Windows Right Management Services

Содержание

- Значение информационной безопасности
- Управление рисками
- Глубокая оборона
- **Необходимые действия при защите от атак**
- Десять законов информационной безопасности

Атака червя на порт UDP 135 (Blaster)

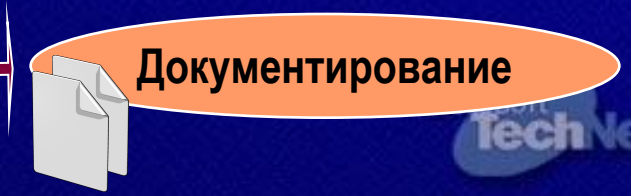
- Периметр
  - Межсетевой экран должен блокировать порт 135
- Внутренняя сеть
  - Просканировать сеть и обнаружить уязвимые компьютеры
  - Проверить машины, подключаемые через Службу удаленного доступа, на наличие обновлений
    - Windows Server 2003 RRAS Quarantine
- Компьютер
  - Установить соответствующие обновления
  - Разрешить входящий трафик для порта UDP 135 только на машинах, которым требуется RPC
    - Фильтры IP Security
  - Заблокировать ненужный входящий трафик
    - Internet Connection Firewall

Почтовые черви

- Периметр
  - Сканирование всех вложений на шлюзе SMTP
- Внутренняя сеть
  - Проверить хосты, подключаемые через Службу удаленного доступа, на наличие актуальных обновлений и сигнатур вирусов
- Приложения
  - Microsoft Office 98
    - Установить обновления безопасности Microsoft Outlook® 98
  - Office 2000
    - Установить Service Pack 2 или более поздний
  - Office XP et Office 2003
    - Усиленная защита от почтовых вирусов включена по умолчанию
- Пользователи
  - Правила обращения с файлами в почтовых вложениях
    - «Не открывайте файлы, если вы не уверены, что это безопасно»

Стандартный процесс обработки инцидента

- Выключить и отсоединить пораженные компьютеры от сети
- Заблокировать входящий и исходящий сетевой трафик
- Исследовать пораженные компьютеры
- Зафиксировать улики вторжения



Содержание

- Значение информационной безопасности
- Управление рисками
- Глубокая оборона
- Необходимые действия при защите от атак
- **Десять законов информационной безопасности**

Законы информационной безопасности

1. Если “плохой парень” может запускать свои программы на Вашем компьютере – это больше не Ваш компьютер.
2. Если “плохой парень” может изменить настройки операционной системы на Вашем компьютере – это больше не Ваш компьютер.
3. Если “плохой парень” имеет неограниченный физический доступ к Вашему компьютеру – это больше не Ваш компьютер.
4. Если Вы разрешаете “плохому парню” загружать исполняемые файлы на Ваш Web-сайт – это больше не Ваш Web-сайт.
5. Слабые пароли сводят на нет сильную систему защиты.

Законы информационной безопасности

6. Машина защищена ровно настолько, насколько Вы уверены в своем администраторе.

7. Зашифрованные данные защищены ровно настолько, насколько защищен ключ шифрования.

8. Устаревший антивирусный сканер не намного лучше, чем отсутствие сканера вообще.

9. Абсолютной анонимности практически не бывает, ни в реальной жизни, ни в Интернете.

10. Технологии – не панацея.

http://www.microsoft.com/technet/columns/security/essays/10imlaws.asp

Информация

- Информационный ресурс Microsoft по безопасности
  - www.microsoft.com/security
  - Для профессионалов IT: www.microsoft.com/technet/security
  - На русском языке: http://www.microsoft.com/rus/security
- Руководства Microsoft по защите информационных систем
  - www.microsoft.com/security/guidance
- Computer Security Institute
  - http://www.gocsi.com