

Безопасность информационных систем в современном мире

Андрей Крючков
Microsoft
andreykr@microsoft.com

О чем мы сегодня поговорим

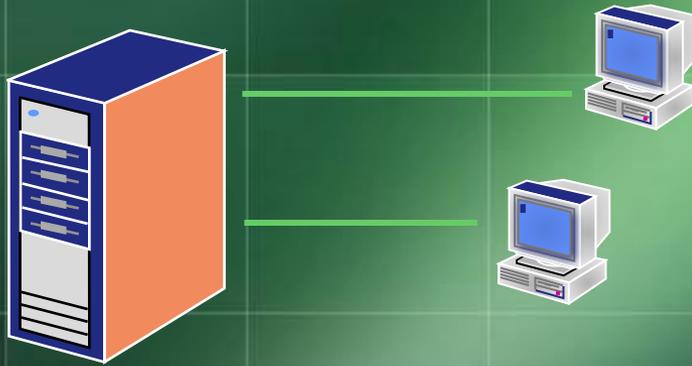
- Почему вопросам безопасности уделяется большое внимание
- Основные источники угроз информационным системам и методы борьбы с ними
- Стратегия Microsoft в области обеспечения безопасности
- Продукты и технологии Microsoft для управления безопасностью

Безопасность

Почему вопросам безопасности уделяется большое внимание



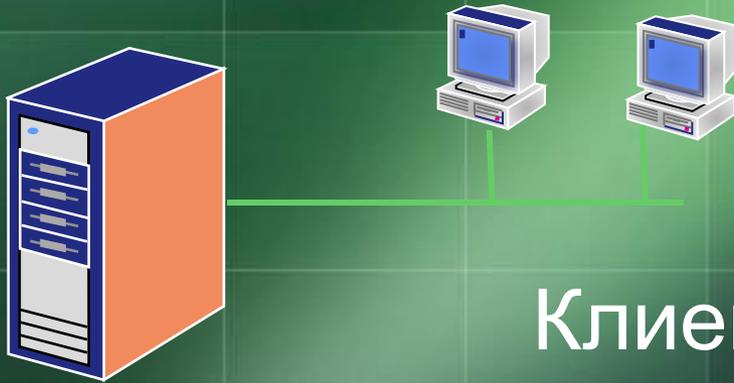
Когда-то очень давно жизнь была гораздо проще



«Большие ЭВМ»

- Доступ с терминалов
- “Стеклянный дом”
- Физическая безопасность, ограниченный доступ

Потом стало чуть сложнее, но
все равно достаточно
просто...



Клиент-Сервер

- Компьютеры объединены в ЛВС
- Серверы печати и файлы
- Ограниченный доступ извне

Но сегодня “Мы уже более не в Канзасе, Тото”* ...



Когда мир
становится
сложным и
большим...

Пришел Интернет

- Всегда включено
- Почта, сообщения
- Веб

*Прошу прощения у L. Frank Baum “The Wizard of Oz”

Что говорят факты

- Хакеры
 - 44% Веб-узлов были атакованы при наличии межсетевых экранов
- Внутренние нарушители
 - до 80% взломов происходит “изнутри”
- Отказ в обслуживании
 - 2000 г.: Yahoo, CNN, Amazon
- Вирусные атаки
 - I love You: ущерб составил до 1 млрд. дол.

Определение безопасности?

- Что защищено?
- От кого защищено?
- От чего защищено?
- Как долго защищено?

Пример: Интернет-банк может быть защищен от подложенной бомбы, но насколько он защищен от работающего в нем программиста с криминальными наклонностями?

Нельзя говорить о безопасности не определяя контекст самого слова защита

Реальна ли угроза?



По данным <http://www.cert.org/stats>

* 2002 данные по третий квартал

Безопасность сегодня

- Обеспечение безопасности - это процесс управления рисками (через управление людьми и средствами защиты)
- Системы безопасности включают:
 - Людей (культура и знания)
 - Процессы (процедуры, регламенты, правила)
 - Технологии (технические средства защиты)
- Надежность одного элемента защиты не обеспечивает безопасности системы в целом
- Технологии не являются единственным и достаточным решением

Круговорот не имеет конца

Обновление:
Доставить

Процесс:
Обнаружить,
Разработать



На будущее:
Включить
в новый
продукт

Новые
угрозы



Дизайн
продукта



Модель появления новых угроз развивается в соответствии законам Мура и Меткалфа

Программисты тоже люди и им тоже свойственно ошибаться

Технологии, Процесс, Люди

Что бросает вызов безопасности?

- В продуктах не хватает функций для безопасности
- Продукты содержат ошибки
- Многие проблемы не решают техническими стандартами
- Сложно поддерживать современное состояние

- Неверное распределение ролей и ответственности
- Отсутствие аудита, мониторинга и реагирования
- Отсутствие процедур поддержания системы актуальном состоянии

Технологии

Процесс

Люди

- Недостаток знаний
- Недостаток ответственности
- Человеческие ошибки

Уровень безопасности, цена или функционал?



- Всегда есть баланс между безопасностью, ценой решения и функционалом (удобство использования, производительность)
- Определите адекватную степень безопасности:
 - Угрозы с которыми вы сталкиваетесь
 - Степень риска с которой можно жить
 - Стоимость ваших данных
- Не забудьте посчитать стоимость административных затрат и стоимость потерь от потери удобства использования и производительности

Абсолютная безопасность недостижима

В идеале:

Только те, кому это положено получают доступ к нужной им информации в любое время с максимальной производительностью с минимальными затратами

Объекты для защиты

Данные

- Номера кредиток
- Маркетинговые планы
- Исходные коды
- Финансовую информацию

Сервисы

- Веб узлы
- Доступ в Интернет
- Контроллеры доменов
- ERP системы

Сети

- Логины
- Платежные транзакции
- Почта

Из чего состоит атака

Угроза + Мотив + Метод + Уязвимость = АТАКА!



Рассмотрим по отдельности

- Основные источники угроз для информационных систем и как с ними бороться
- Мотивы
- Методы
- Уязвимости



Источники угроз



□ Ошибка обычного пользователя может быть фактором опасности и планировать защиту от ошибок нужно так же, как и защиту от хакеров

□ Существуют подходы к решению задач борьбы с отказами технических средств и природными катаклизмами, но данные вопросы лежат вне сегодняшней темы

Рассмотрим по отдельности

- Угрозы
- Мотивы, которые толкают людей на преступление
- Методы
- Уязвимости



Какие мотивы?

Хулиганство

- Изменение, уничтожение или повреждение информации
- Отказ в обслуживании
- Порча общественного имиджа компании

Личные

- Самоутверждение
- Политические заявления или терроризм
- Шутка
- Просто потому что могу



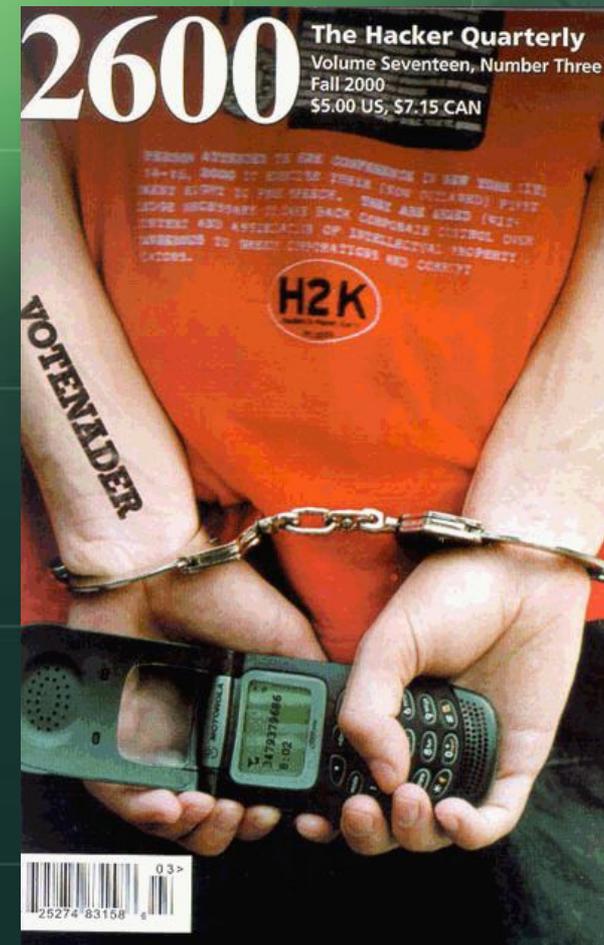
Корыстные

- Украсть информацию
- Шантаж
- Финансовые махинации

Портрет хакера?

- Типичный стереотип:
 - Тинэйджер или молодой человек около двадцати лет
 - Собственная субкультура и сообщество
 - Много времени, но мало денег
 - Узкий крут настоящих специалистов -- разработчиков утилит, знаний и руководств по взлому
 - Большинство пользуются готовыми скриптами «script kiddies»
 - Престиж среди своих
 - Мотивация скорее личное любопытство нежели корысть

- Плюс к этому хакером может стать: «обиженный» сотрудник, конкурент, обычный преступник, кибер-террорист



Рассмотрим по отдельности

- Угрозы
- Мотивы
- Методы используемые для осуществления атак
- Уязвимости



Методики атак (нарушений)

- Подбор/взлом паролей
- Вирусы
- Троянские кони
- Черви
- Атаки на отказ в обслуживании
- Подмена адреса E-mail
- Перлюстрация E-mail
- Проигрывание записи сетевых пакетов
- Модификация перехваченных сетевых пакетов
- Просмотр сетевого трафика
- Методы социальной инженерии
- Атаки по сети
- Подмена сетевых адресов
- Перехват сессий

Существует огромное количество разнообразных методов осуществления атак. На слайде наиболее часто встречающиеся.

Рассмотрим по отдельности

- Угрозы
- Мотивы
- Методы
- Уязвимости и их причины



Что такое уязвимость?

Уязвимость (слабость) –
любая характеристика или свойство
информационной системы,
использование
которой нарушителем может
привести к реализации угрозы

«Трещины в
крепостной
стене»

- Ошибки проектирования
(продукты не имеют встроенных
защитных механизмов)
- Ошибки реализации
(программы содержат ошибки)
- Ошибки при эксплуатации (многие бреши
не могут быть закрыты с помощью
технологии)

Комплекс защитных мер



Комплекс защитных мер Предупреждение

Предупреждение

- Предотвращение проблем до их проявления
- Проактивный подход к работе над проблемами
- Защита от атак (нарушений), которые можно предсказать
- Технологии (средства защиты) наиболее полезны на данном этапе защиты
- **Пример: Пользователь должен пользоваться магнитной карточкой чтобы попасть в офис**

Комплекс защитных мер

Обнаружение

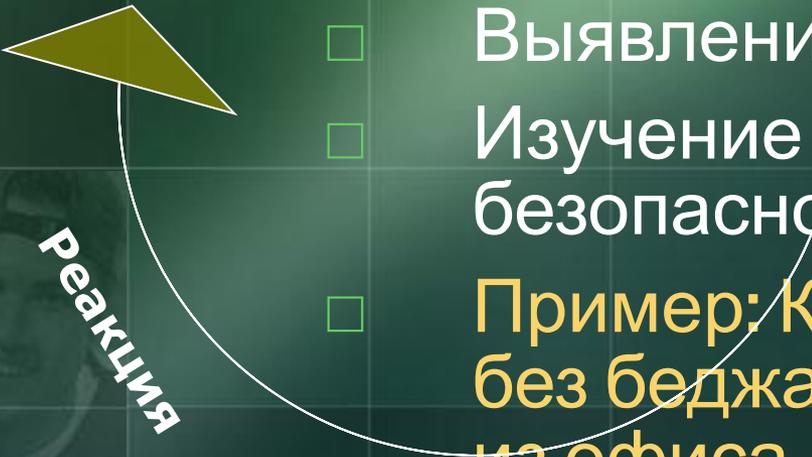
- Обнаружить атаки через бреши в защите, которые не смогли заранее перекрыть
- Оценка известных и неизвестных проблем и брешей в безопасности
- Может работать как реакция на событие или быть проактивной Технологии обнаружения атак могут сильно помочь, но этот этап требует повышенного интеллектуального потенциала
- Важно документировать все действия, чтобы в дальнейшем обоснованно привлекать к ответственности
- **Пример: Сотрудники должны носить бейдж с фотографией поверх одежды все время, пока они находятся в офисе**

Обнаружение

Комплекс защитных мер

Реакция

- Обнаружение без реагирования не имеет смысла!
- Пресечение нарушения
- Восстановление данных и/или сервисов в штатный режим
- Выявление и наказание виновного
- Изучение опыта и улучшение безопасности
- Пример: Каждого, кого обнаружат без бейджа в офисе охрана выводит из офиса для выяснения личности и т.п.



Реакция

Как планировать риски

- Для каждой системы
- Для каждого фактора/мотива и метода
- Разработка планов предотвращения, обнаружения и реагирования
- Анализ результатов для повышения уровня безопасности

Стратегия безопасности

Методология для определения политики безопасности и контроля

→ Анализ рисков и возможностей атак

↳ Для каждого типа угроз (на прим. умышленная атака)

↳ Для каждого метода атак (на прим. Вирусная)

→ Проактивная стратегия

→ Анализ возможного ущерба

→ Определение уязвимостей

→ Минимизация уязвимостей

↳ Реализация плана и разработка политик безопасности и контроля

→ Создания плана работ

→ Стратегия реагирования

→ Оценка ущерба

→ Определение причины ущерба

→ Восстановление

↳ Рализация плана и разработка политик безопасности и контроля

→ Документирование и изучение

→ Создание плана работ

→ Обзор результатов/Симуляция

→ Обзор эффективности политик

→ Изменения в политиках по результатам

Эшелонированная оборона

- Всегда планируйте как минимум два уровня защиты
- Защита должна работать последовательно, а не параллельно; атакующий должен преодолеть А и В – а не А или В

Пример
:

Безопасность коммуникаций



К банковской системе нельзя подключиться по Интернет/модему

Физическая безопасность



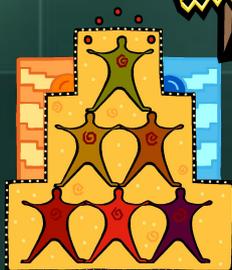
Система требует ключа/смарт-карты для работы

Безопасность логики



Список доступа ограничивает кто может переводить деньги

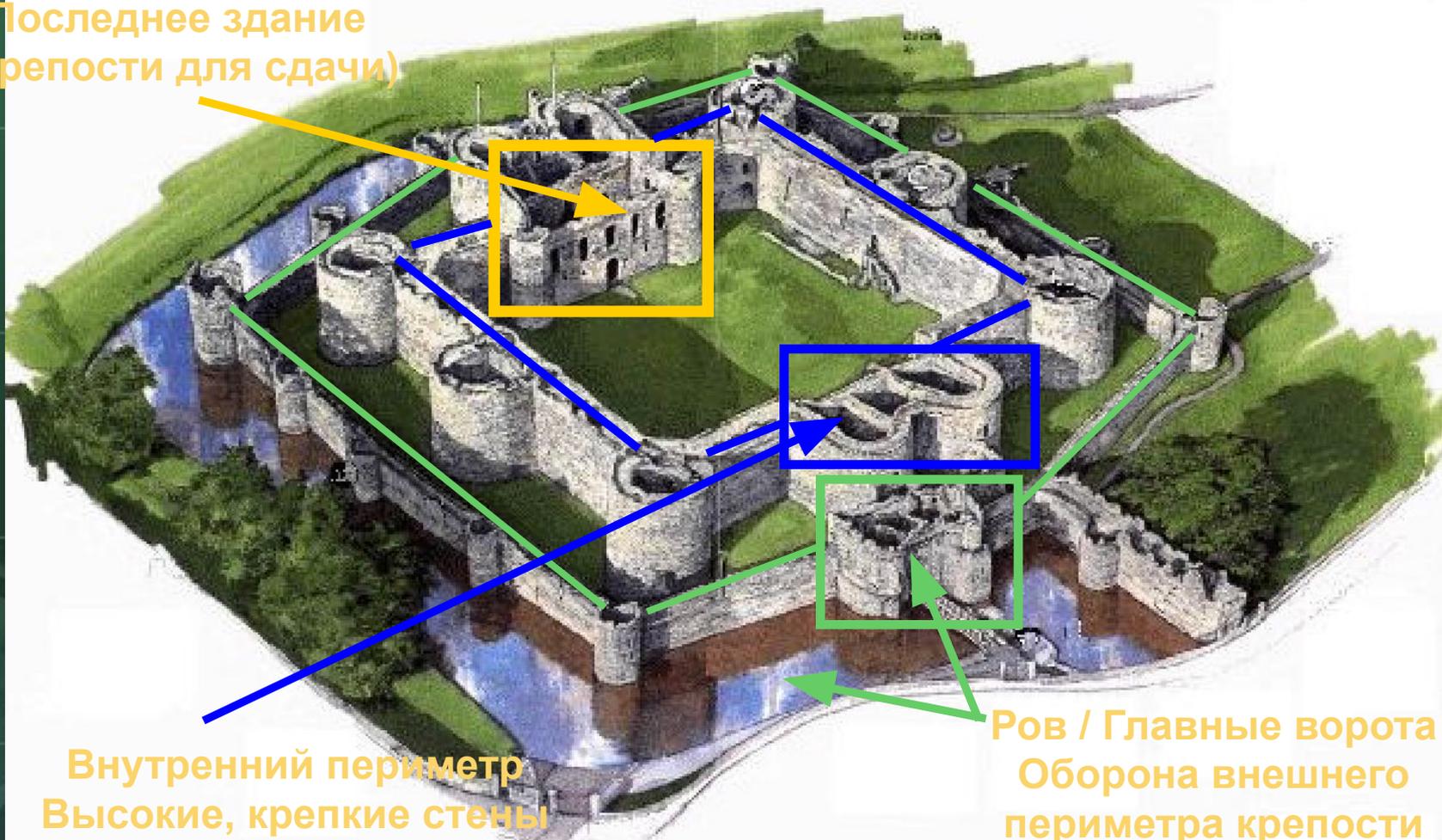
Организационная безопасность



Все переводы более 100000 рублей должны подтверждаться менеджером

Оборона Крепости

Арсенал
(Последнее здание
в крепости для сдачи)



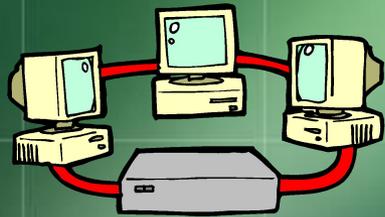
Внутренний периметр
Высокие, крепкие стены
создают дополнительную
зону защиты крепости

Ров / Главные ворота
Оборона внешнего
периметра крепости

Противодействие

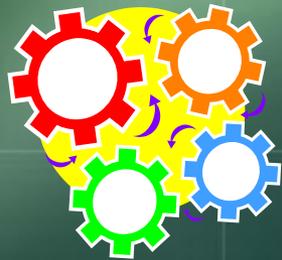
- Применяйте все способы противодействия – технологические, организационные, человеческий фактор

Технологии



На почтовых серверах и клиентах установлено антивирусное ПО. На клиентах реализован запрет запуска исполняемых файлов-вложений и доступ к адресной книге

Процессы



Библиотеки антивирусного ПО постоянно обновляются. Трафик и производительность постоянно анализируются

Люди



Сотрудники обучены безопасной работе с почтовыми клиентами и уведомлены о риске, связанном с открытием вложенных файлов

Стратегия Microsoft

в области обеспечения
безопасности информационных
систем

Microsoft и безопасность – слухи и мифы

- IIS «полон дыр в безопасности»
- Microsoft не занимается безопасностью
- Другие платформы лучше

Поэтому:

- Если мы уйдем от IIS, все проблемы с безопасностью решаться сами собой

Garther First Take, 9/19/01, John Pescatore
“Enterprises ...should start to investigate less-vulnerable Web server products.”



Microsoft и безопасность – реальность

- IIS (сам сервер) не более уязвим чем любая другая платформа ОС или веб-сервер
 - CERT advisories for 2001
 - DataReturn “proof point”
- Microsoft занимается безопасностью
 - Ничего не скрывает
 - Поправки выпускаются максимально быстро
- Другие не обязательно лучше
 - Почитаем прессу: кто помнит “sadmin” или CARKO? Недавний вирус под Apache показал, что на 75% серверов под UNIX не были установлены поправки, Два известных брандмауэра и такой продукт как OpenView имели проблемы с безопасностью
- Это системная, а не «платформенная» проблема
 - И это то, на что нацелена программа Программа Стратегической Защиты Технологий

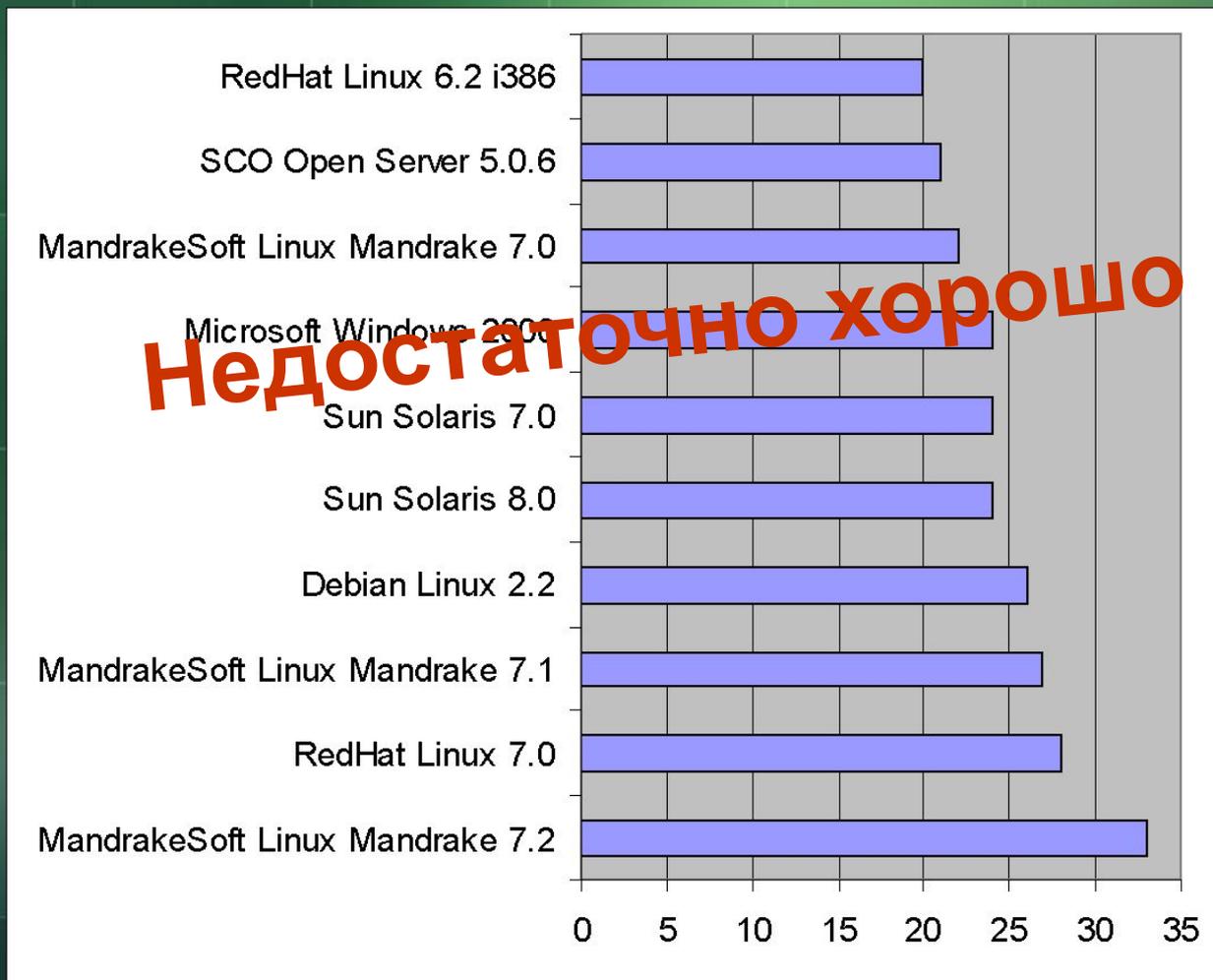
“CERT-ифицированные” факты

- CERT Advisories*
 - Больше уязвимостей в UNIX-серверах чем в IIS
 - Две уязвимости в брандмауэрах
- Выдержки из списка ошибок Bugtraq в 2001
 - Mandrake Linux 7.2 – 33 (v7.1 еще 27)
 - Red Hat Linux 7.0 – 28
 - Sun Solaris 8.0 – 24 (v7.0 еще 24)
 - Windows 2000 – 24
- Отчет Netcraft uptime

*For more info/details see <http://cert.org>

** (as of 10/01)

Уязвимости в разных ОС



Почему вопросы безопасности так важны для Microsoft?

- Атаки становятся все более частыми
- Простои и потери данных обходятся все дороже
 - Microsoft играет важную роль в электронной коммерции (более 50% сайтов с SSL в Интернет), а это требует инвестиций и действий
- Microsoft хочет быть лидером
 - “Code Red” и “Nimda” дорого обошлись заказчикам, которые не были к ним готовы
 - Заказчики ждут руководства к действию от Microsoft
- Установка из коробки нацелена на удобство использования, а не на высокую безопасность
 - Это уязвимость номер один
 - Важно донести эту идею до заказчиков и помочь им исправить положение

Стратегия Microsoft

по обеспечению безопасности

Защищенные
информационные системы

Стратегическая программа
защиты технологий

Инициатива «обеспечение
безопасности Windows»

Secure Windows Initiative

Strategic Technology
Protection Program

Trustworthy Computing

Обязательство Microsoft перед заказчиками:

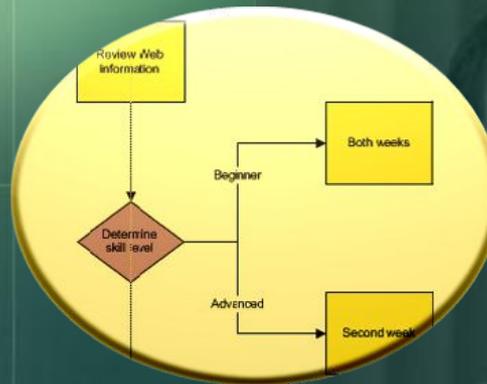
Делать все возможное, чтобы быть уверенными, что каждый заказчик может безопасно работать и обмениваться информацией через Интернет

Инициатива «обеспечение безопасности Windows»

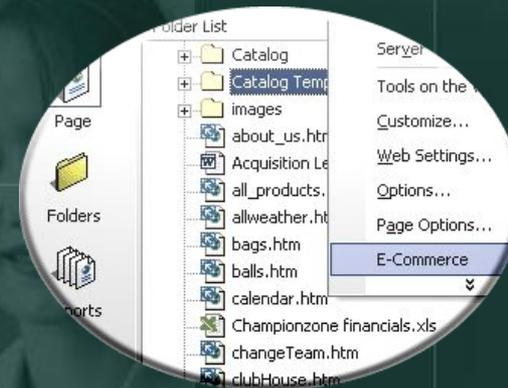
“Создано с мыслью о безопасности”
Цель: Устранить уязвимости системы до начала продаж продукта



Люди



Процесс



Технологии

Инициатива «обеспечение безопасности Windows»

Люди

Курсы повышения квалификации в области безопасности для каждого разработчика, тестера и менеджера для создания более безопасных продуктов

Выделение проблем безопасности в качестве критического фактора при разработке, кодировании и тестировании любого продукта Microsoft

Просмотр кода и дизайна другими людьми

Анализ угроз по каждой спецификации на разработку

Специальная «Красная Команда» тестирует код

Не только поиск переполнения буферов

Цикл работы над ошибками и подписания кода

Изучение кода и тестирование сторонними консультантами

Разработка автоматизированных инструментов для улучшения качества кода там, где это возможно

Гарантированное обнаружение переполнение буферов

Новые компиляторы и отладчики

Стресс-тесты

Процесс

Технологии

Инициатива «обеспечение безопасности Windows»

Сертификация безопасности

- Испытания по FIPS 140-1 для подсистемы криптографии Cryptographic Service Provider (CSP) – *Завершены*
 - *Реализация базовых крипто алгоритмов в Windows проверено государственными органами США*
- Международная сертификация Common Criteria – *Завершена!*
 - *Исследование исходного кода Windows по международным критериям безопасности кода для получения международного сертификата*
- Передача ключевых компонент третьим лицам для исследования, изучения
- Исходные коды лицензированы более чем для 80 университетов, лабораторий и правительственных агентств

Инициатива «обеспечение безопасности Windows»

Сертификация Windows 2000 по Common Criteria for Information Technology Security Evaluation (ISO-IEC 15408)

- Сертификацией Windows 2000 занималась специализирующаяся в области тестирования независимая компания **Science Applications International Corporation (SAIC)**
- Соответствие по профилю защиты **Controlled Access Protection Profile** уровню **Evaluation Assurance Level 4 (EAL4) + ALC FLR 3 (Systematic Flaw Remediation)**
- В России стандарт ГОСТ Р ИСО/МЭК 15408–2002

Government Security Program

- 14 января 2003 года корпорация Microsoft объявила новую программу GSP (Government Security Program)
 - Задача программы – повышения доверия к технологиям Microsoft с точки зрения информационной безопасности
 - Программа адресована национальным правительствам и международным организациям
- В рамках программы GSP Microsoft предоставляет доступ к исходному коду Windows и другой технической информации, необходимой для создания защищенных систем на платформе Microsoft Windows

Программа GSP в России

- Россия – первая страна, в которой подписано Соглашение в рамках программы GSP
- Программа GSP предполагает долгосрочное сотрудничество в области информационной безопасности
- В Соглашении учтены все требования российской стороны

Инициатива «обеспечение безопасности Windows»

В настоящее время

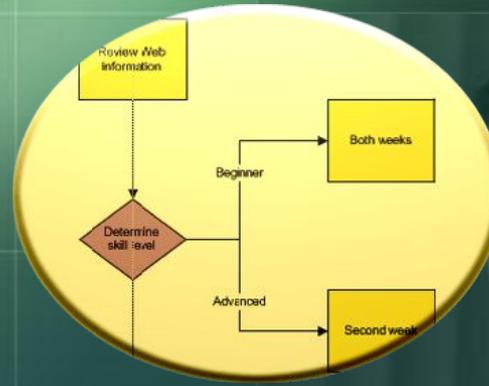
- Фокус на безопасности Windows
 - Мобилизованы ВСЕ
 - Обязательные курсы по безопасности
 - Фокусировка на все источники уязвимостей, снижение возможностей для атак, установка всех параметров по умолчанию и функций в безопасное состояние
 - Первоочередное исправление ошибок и уязвимостей

Стратегическая программа защиты технологий

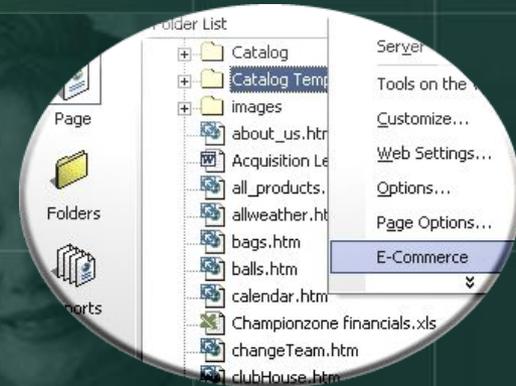
Цель: Помочь заказчикам обезопасить их системы на базе Windows



Люди



Процесс



Технологии

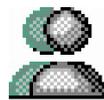
Стратегическая программа защиты технологий – Заказчикам нужна

ПОМОЩЬ

Более 50% пораженных червем Code Red не установили заплатки и пострадали от червя Nimda

- Я не знаю какие заплатки мне нужны
- Я не знаю где взять заплатки
- Я не знаю какие машины латать
- Мы обновили наши «боевые» сервера, но сервера разработки и тестовые были инфицированы

Стратегическая программа защиты технологий



Люди



Процесс



Технологии

Стратегическая программа защиты технологий



Курсы по безопасности
Партнеры, готовые провести аудит



Microsoft Security Toolkit
Материалы по настройке серверов
Новые инструменты и исправления, Windows
Update клиент для Windows 2000



Enterprise Security Tools
Microsoft Baseline Security Analyzer
SMS security patch rollout tool
Windows Update Auto-update client



Защищаем Microsoft Security Toolkit

- Повышает безопасность систем на Windows NT и 2000, даже если они не подключены к Интернет
- Автоматизирует обновление серверов
 - Программы «мастер» для установки одной кнопкой и скрипты для SMS
- Обновления и заплатки
 - Включает **все** Сервис Паки и **критические** исправления для ОС и IIS
- HFNetchk: программа проверки уровня установки заплаток
- IIS Lockdown & URLScan

Стратегическая программа защиты технологий



Windows 2000 Service Pack (SP3)/Windows XP SP1

Устанавливает все исправления с одной перезагрузкой



Corporate Windows Update Program

Позволяет компаниям разместить внутри сервер для Windows Update



Улучшение защиты в продуктах

Все новые продукты, включая Windows 2003 Server имеют гораздо более строгие политики защиты

Защищенные информационные системы (Trustworthy Computing)

Цель: Сделать компьютеры и программное обеспечение столь же надежными, как бытовые электроприборы

Задачи концепции «Защищенные информационные системы»

- В краткосрочном периоде
 - улучшенный дизайн
 - реализация технологий
 - политик безопасности
- Среднесрочная перспектива
 - новые механизмы управления системами
 - новые стратегии предоставления услуг
- В долгосрочном плане
 - десятилетие фундаментальных исследований

Продукты и технологии Microsoft

Для управления безопасностью

Доступные инструменты

(бесплатно!)

- IIS Lockdown Tool
 - Настраивает параметры IIS 4.0/5.0 на противодействие различным типам атак
 - Выключает ненужные системные сервисы
 - Закрывает доступ к системным командам
- URLscan Tool
 - Фильтр ISAPI, который работает в IIS 4.0/5.0
 - Блокирует потенциально опасные URL
 - Полностью настраивается
- Microsoft Baseline Security Analyzer
 - Проводит комплексный анализ безопасности серверов и рабочих станций в сети
- <http://www.microsoft.com/security>

Демонстрация

IIS Lockdown Tool



MBSA

- Единое приложение для Windows 2000 и Windows XP
- Обеспечивает локальное и удаленное сканирование Windows NT 4, Windows 2000, и Windows XP
- Проверка основных «плохих» конфигураций и не установленных обновлений
 - Windows
 - Internet Information Server 4.0 и Internet Information Server 5.0
 - SQL 7.0 и SQL 2000
 - Настольные приложения
 - Internet Explorer
 - Office
 - Outlook™

MBSA

- Стандартная и консольная версии
- Показывает контрольную карточку-отчет
 - Общая оценка системы
 - Сдан/Не сдан для каждой проверки
 - Пояснения и инструкции по устранению обнаруженных уязвимостей
- Утилита “read-only” – нет возможности удаленного управления компьютером
- Пользователь должен обладать правами local administrator на каждом компьютере

MBSA Сценарий

применения

- Администраторы могут проводить сканирование своей сети на предмет обнаружения уязвимостей OS и приложений с одного компьютера
 - Индивидуальные отчеты с каждого компьютера сохраняются централизованно
- Домашние пользователи могут самостоятельно проверить свои компьютеры
- Администраторы могут использовать консольную версию для регулярных (по расписанию) проверок безопасности компьютеров в организации

Использование консольной версии MBSA



```
C:\WINDOWS\System32\cmd.exe - mbsacli
C:\apps\MBSA>mbsacli
Microsoft BaseLine Security Analyzer
(c) 2002, Microsoft Corporation. All rights reserved.
Developed for Microsoft Corporation by Shavlik Technologies, LLC
www.shavlik.com

Version 1.0
Engine version 3.6.0.3
Hotfix version 3.65.0.0

Attempting to download the CAB from:
http://download.microsoft.com/download/xml/security/1.0/NT5/EN-US/mssecure.cab
File was successfully downloaded.

Attempting to load .\mssecure.xml.
Using XML data version = 1.0.1.235 Last modified on 3/7/2002.
Scan performed Sat Mar 16 16:22:09 2002
Shavlik Network Security Hotfix Checker, Enterprise Edition, 3.70
Using XML data version = 1.0.1.235 Last modified on 3/7/2002.

Scanning...
[      ] 0 of 1 computer scan(s) complete.....
```

Демонстрация

MBSA



MBSA подводя итоги

- MBSA обеспечивает...
 - Самый простой способ проверить один или несколько компьютеров на наличие уязвимостей и не установленные hotfix'ы
 - Легкий в использовании графический интерфейс для помощи как обычным пользователям, так и ИТ-профи
 - Работа из командной строки (mbsacli.exe) – для регулярных проверок безопасности по расписанию

Corporate Update Server

(бесплатно!)

- Клиент автоматического обновления
 - Автоматически сгружает и устанавливает критические заплатки
 - Запатки для: безопасности, особо серьезных ошибок и драйвера для устройств, когда никаких драйверов не установлено для этого устройства
 - Проверяет сайт Windows Update или сервер Corporate Update каждый день
 - Устанавливает обновления по расписанию после загрузки
 - Настройка через политику безопасности
 - Поддерживаются Windows .NET Server, Windows XP и Windows 2000
- Сервер обновлений - Update server
 - Вы можете разместить свой собственный Windows Update Server внутри предприятия
 - Сервер самостоятельно синхронизируется с сервером Windows Update и локально хранит все обновления для тех версий, которые есть на предприятии
 - Простой интерфейс управления через IE
 - Обновления становятся доступны только после разрешения администратора
 - Работает на Windows .NET Server и Windows 2000 Server

Источники информации

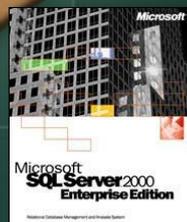
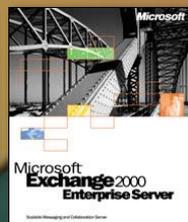
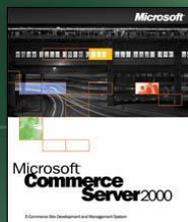
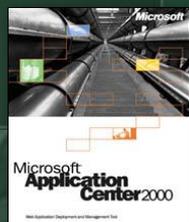
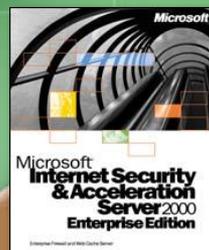
- ❑ Сайт по безопасности
<http://msdn.microsoft.com/security/>
- ❑ Office
<http://office.microsoft.com/>
- ❑ SQL Server
<http://www.microsoft.com/sqlserver/>
- ❑ Exchange Server
<http://www.microsoft.com/exchange/>



Безопасная инфраструктура

Интернет

ISA Server:
Брандмауэр уровня
предприятия и
фильтрация на уровне
приложений



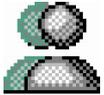
Серверные продукты
работают с безопас-
ностью Windows



Безопасность в Windows:

- Аутентификация
- ACL
- Active Directory

Безопасность это путь... А не конечная станция



Обучение и подготовка персонала

- Пройдите обучение на курсах

Возможность противостоять

- Проанализируйте политики безопасности и измените их для соответствия реалиям сегодняшнего дня
- Изучите и используйте Microsoft Operations Framework



Технологии, чтобы работать проще

- STPP для вас
- Microsoft продолжает инвестировать в свои продукты, а также в разработку новых методик их использования
- Используйте инструменты и новые технологии



Квартальная маркетинговая программа «Безопасность информационных систем»

- Срок действия 1 января – 31 марта
- Раздел на сайте:
<http://www.microsoft.com/rus/promotion/security/>
- Специальные предложения:
 - При покупке ПО по программе MYO – USB карта памяти Verbatim Personal Storage емкостью 64 Мб **в подарок**
 - **SA за полцены** покупателям Windows 2000 Server или Small Business Server 2000

Поиск по сайту



Расширенный поиск | Карта

- Обзор
- Стабильная работа
- Безопасность
- Специальные предложения
- Где купить

Семинары по Microsoft Small Business Server 2000



Перебои в работе?
Вирусы?
Атаки хакеров?
Не в вашей компании.

БЕЗОПАСНОСТЬ
покупателям продукции Microsoft



Лучшие продукты Microsoft в РАССРОЧКУ!
специальное предложение »

Small Business Server
специальное предложение »

Windows 2000 Server
специальное предложение »

Современный бизнес требует от информационной системы решения все более сложных, иногда казалось бы взаимоисключающих задач — поддержка клиентов в режиме 24x7; снижение стоимости эксплуатации, гибкость в управлении; обеспечение доступа к информации сотрудников в любой момент и в любом месте.

Но все эти задачи могут быть успешно решены только в одном случае. Если информационная система обеспечивает бесперебойную работу и защиту информации. Т.е. обладает двумя важнейшими свойствами — надежностью и защищенностью.

Последние версии программных продуктов Microsoft — **Microsoft Windows XP, Microsoft Office XP, Microsoft Windows 2000 Server, Microsoft Small Business Server 2000** — обеспечивают **высокую стабильность работы и защиту ваших данных и информационной системы.** Они идеально подходят для вашей информационной системы.

Ваше мнение

Что Вы думаете об этом предложении?

- интересно, собираюсь воспользоваться
- интересно, но не для меня
- неинтересно

Ваш комментарий к ответу:

Вы работаете в организации, где количество ПК:

- до 20
- от 21 до 50
- от 51 до 100
- более 100

Ваша компания является партнером Microsoft



Вопросы?

Microsoft

<http://www.microsoft.com/rus>

Андрей Крючков

andreykr@microsoft.com

Телефон: (095) 967-8585

