Удобство и безопасность: как совместить несовместимое

Алексей Лукацкий

Консультант по безопасности

Удобство & безопасность

Зачем нужна система ИБ?

- Для защиты
  - Информации
  - Информационных систем
  - Оборудования
- Для обеспечения
  - Конфиденциальности
  - Целостности
  - Доступности
- … (множество других определений)

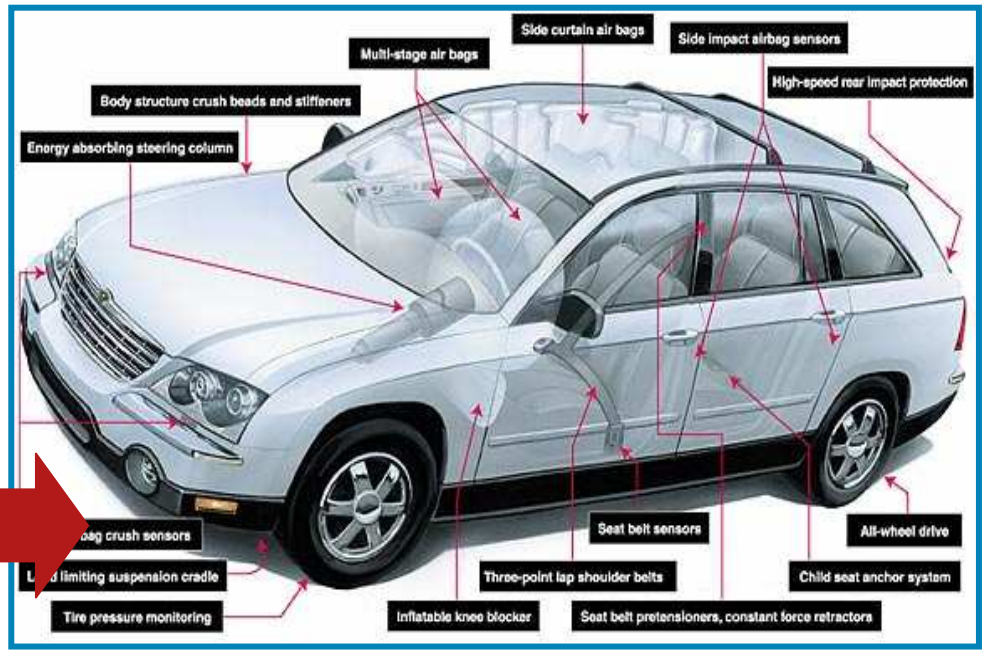
Безопасность, как самоцель

- Многие руководящие документы, стандарты, требования по ИБ рассматривают безопасность, как самоцель

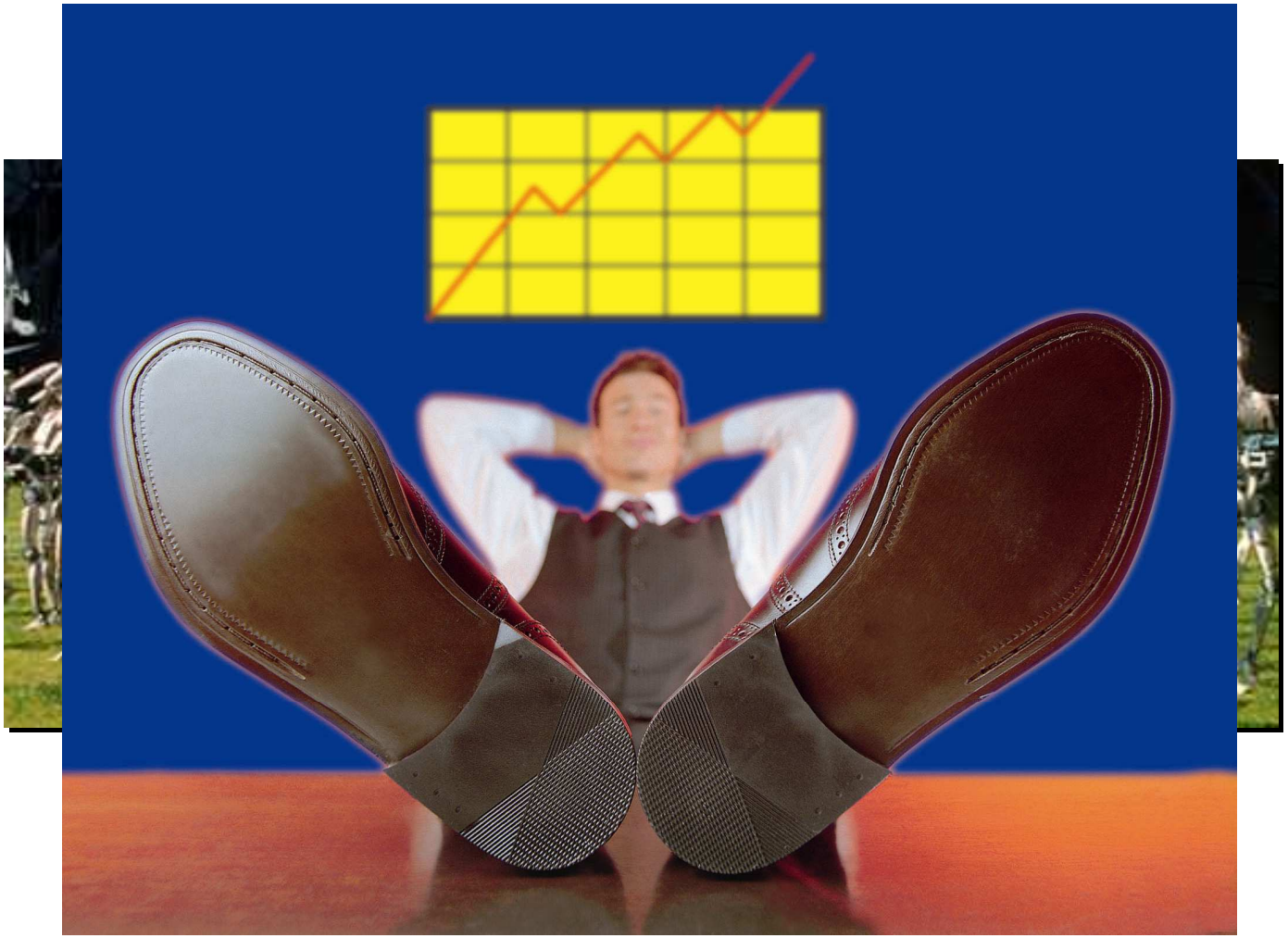
Безопасность, как самоцель

Правильная безопасность

- Информационная безопасность - это рычаг для генерации большего бизнеса и увеличения гибкости предприятия, которая позволит ему работать в тех областях, которые слишком опасны без реализации адекватной программы ИБ



Кто генерит бизнес?



Безопасность или удобство?

Психологическая приемлемость

Психологическая приемлемость

- Очень важно, чтобы интерфейс взаимодействия с пользователем был удобным в использовании; чтобы пользователи запросто и «на автомате» использовали механизмы защиты правильным образом. Если образ защиты в уме пользователя будут соответствовать тем механизмам, которые он использует на практике, то ошибки будут минимизированы. Если же пользователь должен переводить представляемый им образ на совершенно иной «язык», он обязательно будет делать ошибки

  Джером Зальтцер и Майкл Шредер, 1975 (!) год

Пароли: что плохого?

- Выбирайте пароли длиной свыше 8 символов
  - А как их запомнить?
- Используйте системы автоматической генерации паролей (8HguJ7hY)
  - А как их запомнить?
- Пусть пароль выбирает пользователь
  - Тривиальные и легко угадываемые пароли

Почему это происходит?

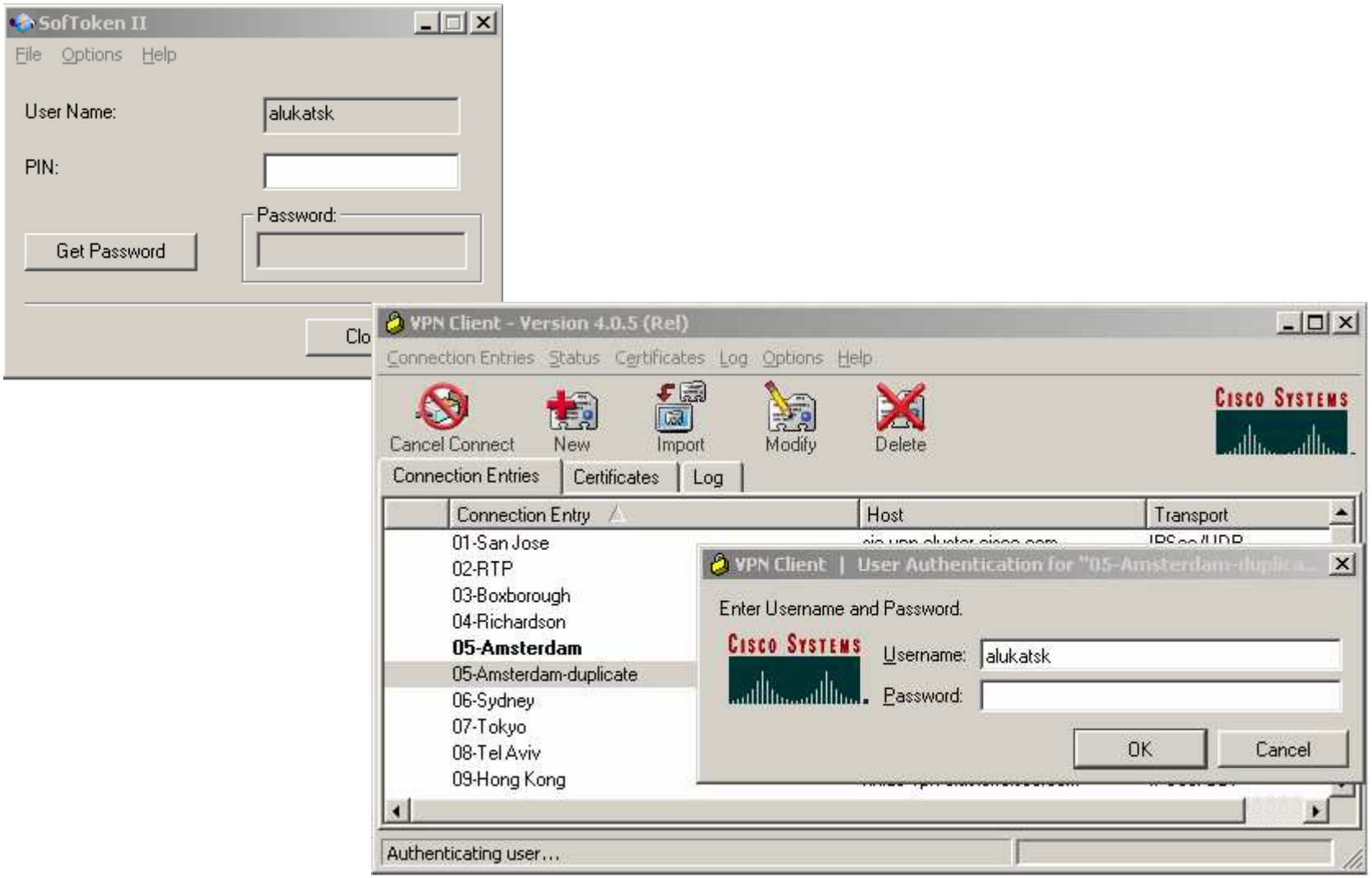
- Продукт разрабатывается с точки зрения разработчика, а не потребителя
- Если потребители и опрашиваются, то только с точки зрения функций защиты
- Тестирование проводится на предмет ошибок и дыр, но не юзабилити
- Продукт выпускается в условиях жесткой конкуренции со стороны других разработчиков
- В России практически никто не обращается к услугам специалистов по эргономике

Хорошие и плохие примеры

Пароли: как улучшить?

- Графические пароли
- Токены, смарт-карты, биометрия

Пароли: хочется сэкономить?



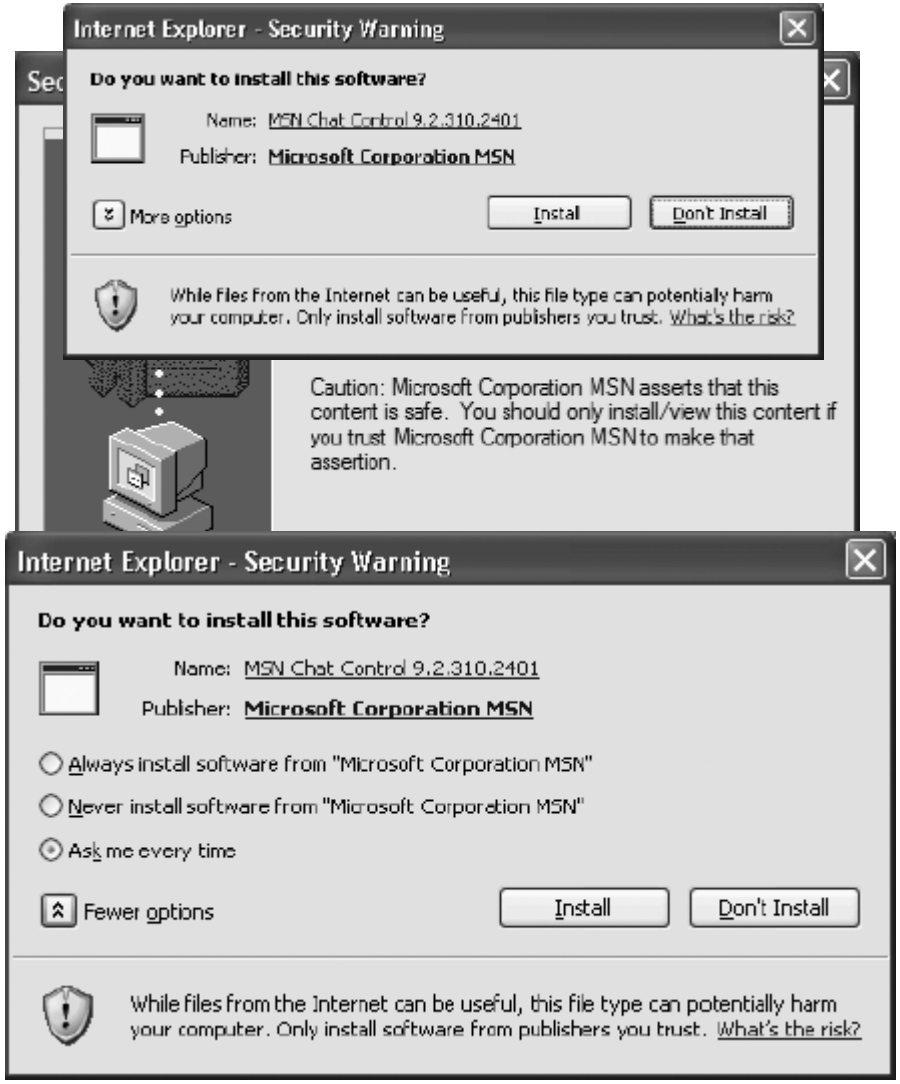
Microsoft

- «Монополист» рынка программного обеспечения
  - За счет удобства для пользователя
- Множество нареканий с точки зрения безопасности
  - Ситуация изменяется

Пример с ОС Windows

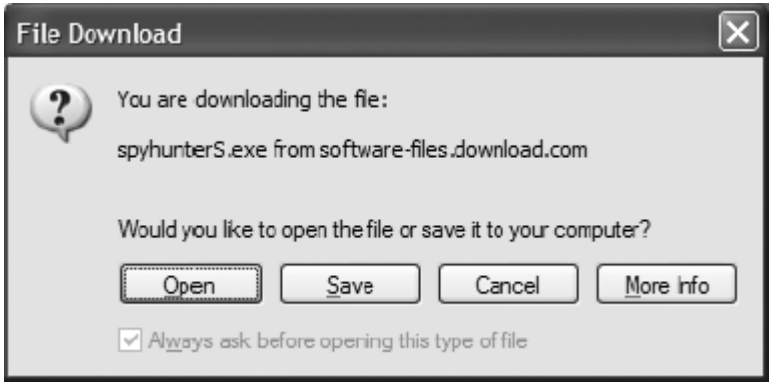
- Что такое «signed»?
- Что такое «Microsoft Code Signing PCA»?
- Всегда доверять этому источнику?

  А если я хочу всегда недоверять этому источнику?
- Что «да» и что «нет»?
- Чем это опасно?



Пример с ОС Windows

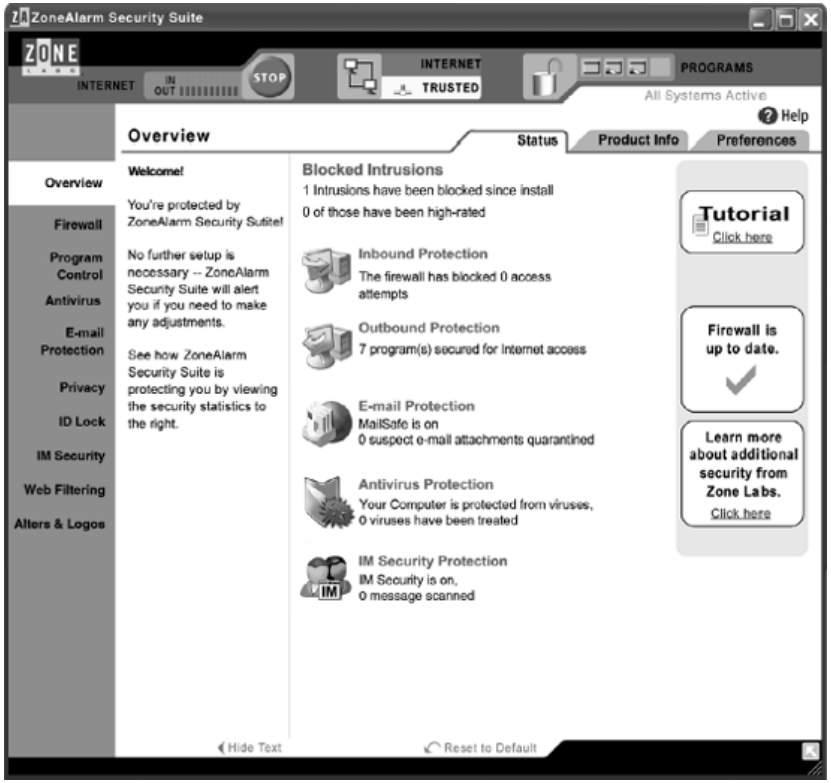
- Как можно открыть exe-файл?
- Чем это опасно?
- Какие действия осуществляются по умолчанию?



Заключение

ZoneAlarm

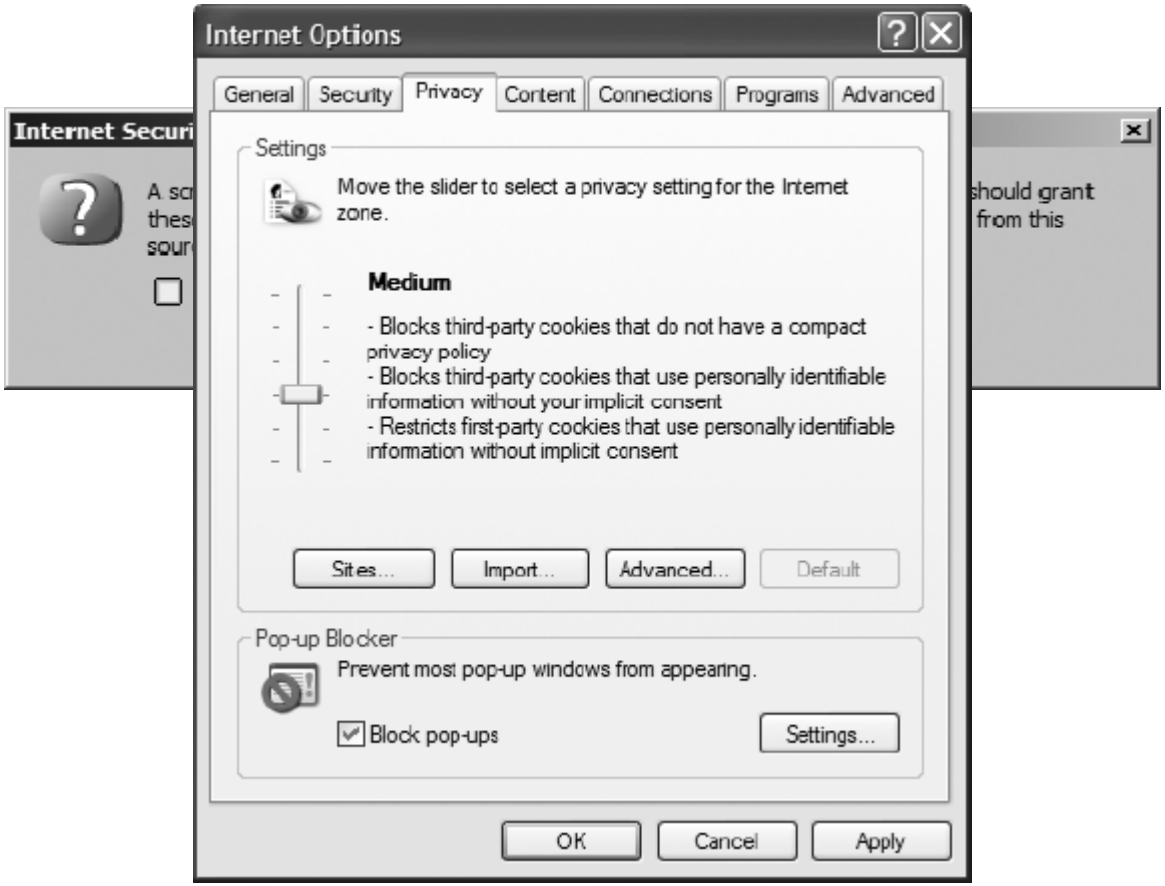
- 1 миллион загрузок с сайта за первые 10 недель
- Один из самых популярных продуктов для персональной Интернет-безопасности
- «…чтобы даже мама могла использовать»



Принципы дизайна ZoneAlarm

- Знайте вашу аудиторию
- Думайте как ваша аудитория
- Избегайте беспорядка
- Избегайте сложности
- Встаньте на сторону пользователя даже если конкуренты «давят» на вас со сроками
- Обеспечьте обратную связь с пользователем!!!

Обратная связь!!!



Вирус bagle.aa и Cisco Security Agent

- Вирус появился в апреле 2004
- Не было времени на установку патча или обновление антивируса
- Из 38,370 ПК защищенных Cisco Security Agent, около 600 было скомпрометировано – 620 пользователей открыло зараженный файл

  Некоторые пользователи нажали “Yes” на вопрос «Подозрительное приложение пытается получить доступ к электронной почте. Разрешить?»
- Существенное снижение времени и стоимости борьбы

  А также обновление политики безопасности для снижения влияния «человеческого фактора»

Дополнительная информация

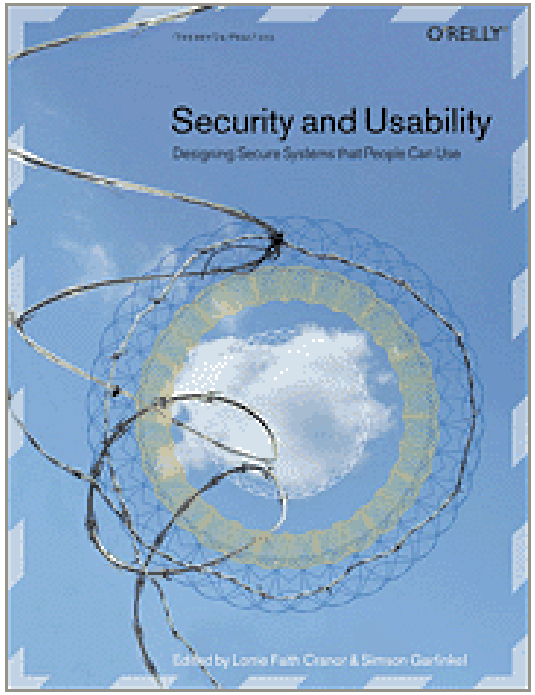
- http://www.ischool.berkeley.edu/~rachna/security_usability.html - множество ссылок на публикации об удобстве и безопасности
- Security and Usability. Lorrie Cranor, Simson Garfinkel

  Publisher: O'Reilly

  Pub Date: August 2005

  ISBN: 0-596-00827-9

  Pages: 738



Вопросы?

Дополнительные вопросы Вы можете задать по электронной почте security-request@cisco.com
или по телефону: (495) 961-1410