BECAUSE YOUR DATA IS YOUR BUSINESS

INFORMATION
WATCH
TECHNOLOGIES

INFOWATCH

Универсальные средства защиты от угроз – нужны ли они?

Наталья Касперская

Генеральный директор «InfoWatch»,

Председатель совета директоров
Группы компаний Kaspersky Lab

6 ноября 2008

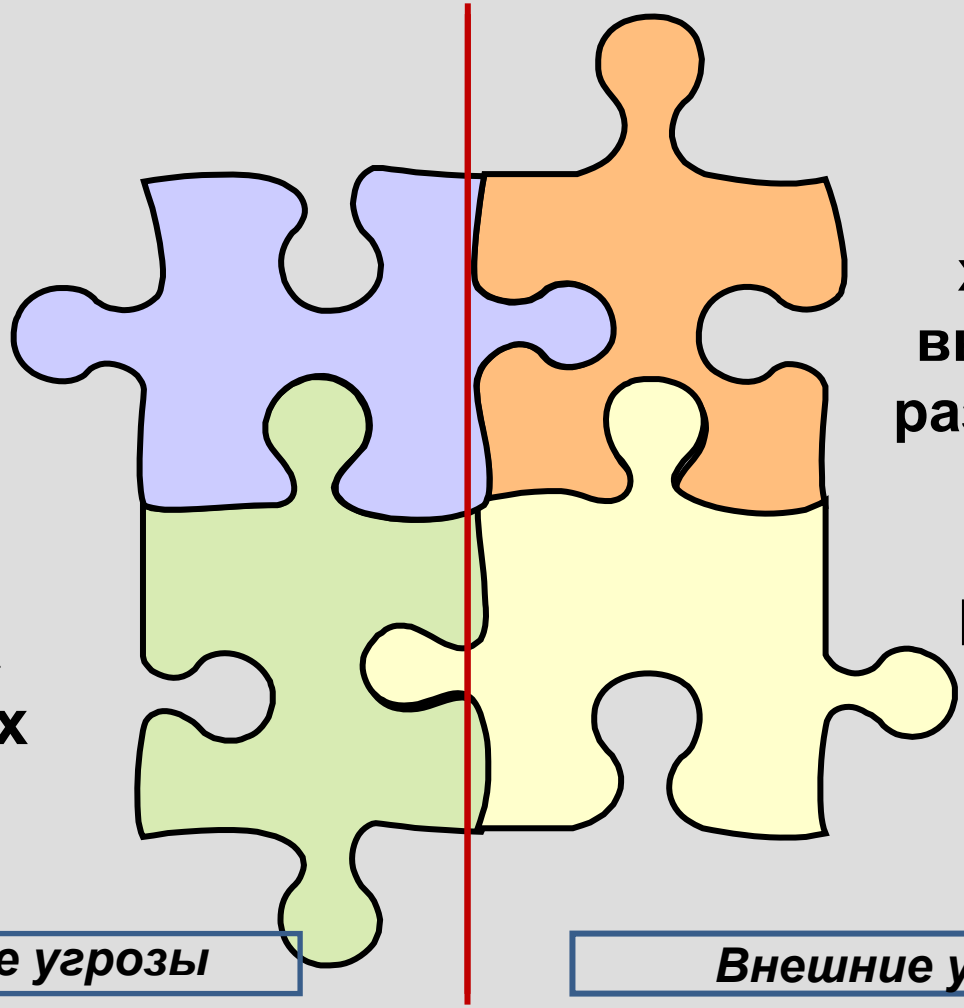
Повестка презентации

- Определение внешних и внутренних угроз
- Возможные решения
- Тренды
- Что такое DLP?
- Универсальное решение – есть ли оно?

Угрозы информационным активам компании

Несанкцио-нированный доступ к внутренним ресурсам

Утечка данных



Вирусы, хакеры, спам, вымогательство, разл. Троянцы, пр.

Кража /утеря носителей

Внутренние угрозы

Внешние угрозы

Виды ИТ-угроз

- **Внешние:**
  - Вирусы
  - Троянские и различные шпионские программы
  - Хакерские атаки
  - Программы двойного назначения
  - Спам
- **Внутренние:**
  - Умышленные действия – воровство информации сотрудниками, занесение программ-шпионов в локальную сеть
  - Халатность - потеря сотрудниками носителей с данными, случайная пересылка информации
  - Несанкционированный доступ к информации

Каковы решения по защите сегодня?

- **От внешних угроз**
  - Продукты защиты от вредоносных программ – антивирусы, антишпионы и т.п.
  - Сетевые экраны
- **От внутренних угроз**
  - Системы защиты от утечек (DLP)
  - Программы шифрования данных
  - Системы защиты от несанкционированного доступа

Необходимые элементы DLP решения

- контроль нескольких каналов передачи данных за пределы компании
- централизованные инструменты настройки и управления
- предотвращение несанкционированного использования данных внутри компании
- защита от утери /кражи данных
- архивация и хранение данных
- защита новых документов (проактивность)

Необходимые элементы решения по защите от внешних угроз (антивирус)

- контроль всех каналов поступления информации
- централизованные инструменты настройки и управления
- защита от уже существующих внешних угроз (вирусы, троянские программы и т.п.)
- защита от новых типов внешних угроз (проактивность)
- защита от несанкционированного доступа к информационным ресурсам компании извне (хакерство)

Общие элементы для обоих систем

- Одни и те же защищаемые каналы
- Централизованное управление и определение политик
- Необходимость проактивной защиты

Выводы:

1.Налицо явный тренд на интеграцию

2.Системы решают *разные задачи*, требующие разных знаний и компетенций

Плюсы и минусы интегрированного решения

Плюсы	Минусы
Меньше число настраиваемых параметров по сравнению с настройкой отдельных компонент	Высокие требования к знаниям специалистов, обслуживающих систему
Многоуровневость, комплексность защиты	Сложность в создании правильных настроек
Защита всех каналов поступления и пересылки данных	Снижение качества по каким-то из каналов
	Необходимость модернизации текущей инфраструктуры безопасности

Тренд

- **Интегрированное решение, обеспечивающее комплексную защиту от угроз**
  - централизованное управление
  - единые политики
  - модульность
- **Система анализа инцидентов информационной безопасности, изменяющая поведение корпоративной ИТ - системы в зависимости от наличия в ней угроз**

Выводы

- **Нет единой рекомендации**
  - выбор модулей должен осуществляться в зависимости от потребностей
  - необходимость настройки правил и политик
- **При выборе подхода нужно учитывать интеграцию с уже существующими системами**
- **DLP решение является базисом интегрированной платформы, т.к. оно перекрывает почти все каналы**

Спасибо!

Задавайте вопросы.

Узнайте о нас больше:
http://www.infowatch.ru