



INFOWATCH

Внутренние угрозы 2.0

Машины против людей?

- 6 лет на рынке
- Лидер DLP-рынка России (IDC 2009)
- Фокус на внутренних угрозах компаний
- Создатель экспертного совета DLP-Expert (> 50 членов)
- Международные конференции DLP-Russia 2008, 2009
- Более 80 корпоративных заказчиков в России
 - естественные монополии Газпром, Транснефть, РЖД
 - 5 из 7 нефтяных компаний
 - 2 из 3 федеральных мобильных оператора
 - 3 из 5 крупнейших банков
 - 4 федеральных министерства

- Высокая текучесть кадров
- Недостаток ресурсов для защиты
- Усиление конкуренции
- «Персональные данные» (ФЗ 152, «проблема 01.01.10»)

Причины

- Увольнения и сокращение оплаты труда
- Увеличение конкуренции
- Борьба за выживание

Влияние

- Вынос данных уволенными
- Поиск доп. заработка
- Кража чужих секретов

Последствия

- Снижение доходов
- Потеря репутации
- Потеря доли рынка
- Уход с рынка

- Использование корпоративных ресурсов в личных целях
- Хищение информации
- Правонарушения с использованием корпоративной инфраструктуры
- Злоупотребление служебным положением
- Установка нелицензионного и потенциально опасного ПО
- Нарушение требований регуляторов

Криминальные действия сотрудников

- Шантаж, мошенничество, нарушения авторских прав и т.д.

Нежелательные действия сотрудников

- Распространение нежелательной информации от лица компании.
- Несанкционированное взаимодействие с прессой.

- Временные сотрудники (стажеры, переводчики и др.)
- Сотрудники компаний аутсорсеров (дата – центры, колл – центры, транспортные компании и т.д.)
- Сотрудники компаний, имеющих доступ к вашей информации (консультанты, аудиторы, контролеры и т.д.)

- Финансовые прямые и косвенные
- Снижение репутации
- Потеря интеллектуальной собственности
- Потеря конкурентных преимуществ => потеря доли рынка
- Потеря персональных данных

- Октябрь 2008, Deutsche Telekom (Германия), сотрудники контактного центра продавали персональные сведения 30 млн. клиентов.
- Декабрь 2008, Heartland Payment System (США), банковский провайдер для 250 000 организаций, злоумышленникам удалось получить доступ к информации о картах клиентов.
- Февраль 2008, LGT банк (Лихтенштейн), инсайдер Хайнрих Кибер подставил целое государство, продав базу данных банка сначала немецким, а потом и английским спецслужбам, получив за это \$6,5 млн.
- Январь 2008, сотрудник LG Electronics передал китайцам секретные данные о заводе по производству плазменных дисплеев, потери оцениваются в размере \$1,4 млрд.
- Сентябрь 2008, Agilent Technologies, производителя измерительного оборудования, в результате кражи незашифрованного ноутбука утекли данные около 51 тыс. человек.
- Январь 2009, Intel, бывший сотрудник похитил более 100 страниц важных документов и 19 чертежей, подозрение в передаче их AMD.

Средний объем ущерба из-за утечки

Заказчик	Канал	Угроза	Ущерб, руб
Банк	Web-mail	Список добросовестных плательщиков	50 млн.
Системный интегратор	ICQ	Переписка злоумышленников	15 млн.
Нефтяная компания	E-mail	Мошенничество при закупках	7 млн.
Нефтяная компания	USB-диск	Коммерческий шпионаж	200 млн.

* по оценке
заказчика

- Признаки и категоризация конфиденциальной информации
- Разработка системы учета, хранения и маршрутизации КИ (политики безопасности)
- Внедрение политик защиты КИ
- Исполнение сотрудниками политик безопасности
- Контроль исполнения



- Лишь 20% информации структурировано
- 10% информации меняется ежедневно
- Точные формальные критерии конфиденциальности информации неизвестны
- В компании нет концентрированной экспертизы для классификации информации
- В самом сообщении не содержится достаточно информации для принятия решения

У вас нет времени и средств защитить каждый документ
Но у вас есть время защитить важные категории документов

Автоматически
определяется
категория
сообщения/документа

Автоматически
определяется
важность инцидента

Автоматически
запускается сценарий
обработки инцидента

В зависимости от задач можно выбрать два режима:

- **Пассивный.** Снятие копий со SPAN-порта, теневых копий печати и копирования на сменные носители, их анализ и обработка инцидентов. Не влияет на работу инфраструктуры
- **Активный.** Разворачивания системы «в разрыв». Блокирование запрещенных операций. Максимальная степень защиты.

Система работает только в случае перемещения информации. В остальное время система не использует вычислительные мощности.

- **Хранение: IBM, EMC, Hitachi, HP**
- **IRM: Microsoft RMS, Oracle IRM, Adobe LifeCycle**
- **UTM: Aladdin eSafe, BlueCoat, Websense**
- **Routers: Cisco, Juniper**
- **Endpoint protection: DeviceLock**

- Опыт в розничных, инвестиционных и универсальных банках
- Пилотные проекты для того, чтобы решить, нужно ли вам это решение
- Рассрочка, если вы используете CAPEX-бюджеты
- Аутсорсинг для использования OPEX-бюджетов
- Экономия: интеграция с уже имеющимися решениями

- **InfoWatch Data Control** – 3000 р. за лицензию, при 100 рабочих станциях
- **InfoWatch Traffic Monitor** – 5500 р. за лицензию, при 500 рабочих станциях
- Аудит действующей системы контроля информации, как правило, входит в общую стоимость проекта



Вопросы?

<http://www.infowatch.com>