



ИРС: НОВАЯ КОНЦЕПЦИЯ ЗАЩИТЫ ИНФОРМАЦИИ ОТ ВНУТРЕННИХ УГРОЗ

Алексей Раевский
Компания SecurIT





Почему внутренние угрозы?

- Хакеры являются причиной только 1% утечек данных
- Инсайдеры находятся на 1 месте по количеству инцидентов
- 79% IT-директоров сообщили хотя бы об одном инциденте за последний год
- Изнутри сети получить доступ к конфиденциальной информации гораздо проще
- Более высокая актуальность в условиях кризиса (сокращения персонала)



Почему внутренние угрозы?


- Закон о персональных данных
- Необходимость приведения существующих систем в соответствие до 1 января 2010г
- Гражданская ответственность
- Административная ответственность (ст. 13.11 КоАП РФ)
- Уголовная ответственность (ст. 137 УК РФ – злоупотребления и незаконные действия с данными о частной жизни)





DLP: традиционный подход

- Контроль наиболее очевидных каналов утечки:
 - Периферийные устройства (USB-диски и т.д.)
 - Принтеры
 - Электронная почта
 - Веб-трафик и IM
 - Социальные сети
- Контентный анализ
- Архивирование для обеспечения возможности расследования инцидентов



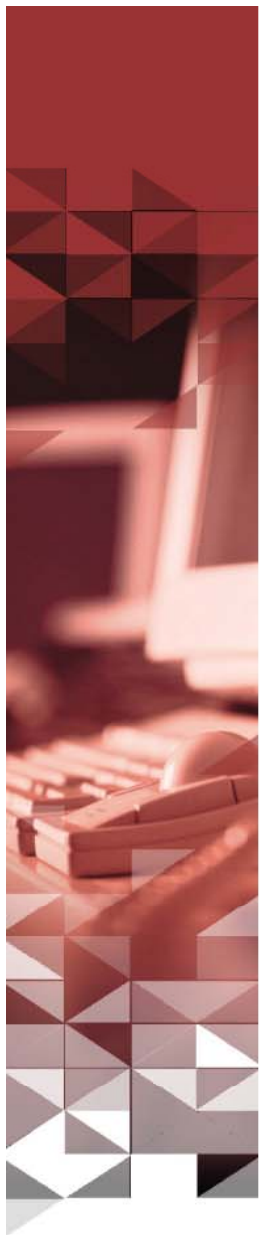
DLP != защита от внутренних угроз

- Физический доступ к носителям
 - Магнитные ленты
 - Жесткие диски и хранилища
 - Ноутбуки
- Аутентификация и идентификация



Физический доступ к носителям

- В ходе рутинных бизнес-процессов часто возникают ситуации, в которых вероятны утечки
 - Потеря магнитных лент
 - Потеря и кража ноутбуков
 - Продажа и ремонт жестких дисков
- Большое количество инцидентов
- Внутренняя угроза



Аутентификация и идентификация

- Проблема доступа в сеть с помощью паролей
 - Необходимость использования сложных паролей
 - Сложность запоминания
 - Необходимость периодической смены
 - Возможность подсмотреть
- Проблема блокировки рабочих станций





IPC: Information Protection and Control

- Защита от утечек с использованием наиболее очевидных каналов – DLP
- Шифрование данных на носителях (data-at-rest)
- Идентификация и аутентификация (identity management)

IPC: прогнозы

- Исследование IDC:
- По мнению 81% опрошенных, IPC – это важная часть в общей стратегии ИБ
- 64% респондентов собираются внедрять новые IPC технологии
- Рынок средств IPC будет расти на 33% в год и в 2011 достигнет суммы в \$3 млрд.





Линейка ИРС продуктов

- Zserver Suite – защита магнитных лент, жестких дисков и хранилищ
- Zdisk – защита данных на ноутбуках
- Zlock – контроль внешних устройств и принтеров
- Zgate – контроль интернет-трафика
- Zlogin – защищенный вход в сеть с использованием электронных ключей и смарткарт
- Централизованное управление из единой консоли



Zserver Suite

- Обеспечивает защиту данных в случае физического доступа к носителю
- Прозрачное шифрование магнитных лент, серверных хранилищ и оптических дисков
- Хранение ключей на смарт-карте
- Кворум ключей шифрования
- Быстрое развертывание и ввод в эксплуатацию



Zlock

- Разграничение доступа к внешним и встроенным устройствам и принтерам
- Огромный спектр поддерживаемых устройств
- Теневое копирование
- Сбор и анализ информации о событиях
- Мониторинг клиентских модулей



Zgate

- Контроль и архивирование электронной почты
- Анализ текста письма и файлов-вложений, в том числе, архивов
- Возможность заблокировать письмо или поместить его в карантин
- Контроль веб-трафика (сервера бесплатной почты, социальные сети)*
- Контроль служб мгновенных сообщений*

* -- середина-конец 2009 года

Zlogin

- Вход в сети и приложения с использованием одного ключа или смарт-карты
- Автоматическая генерация паролей
- Автоматическая блокировка рабочей станции
- Возможность использования карты или ключа в СКД



Вопросы



<http://www.securit.ru>



Z