О способах контроля информационных потоков компании

Минин Виктор
Советник Председателя МОО
«Ассоциация защиты информации»

Ассоциация

Защиты

Информации

Наша цель: Создание благоприятных условий для реализации потребностей граждан, бизнеса и органов госвласти в продуктах и технологиях защиты информации.

Председатель Совета

Емельянов Г.В.

Член-корреспондент Академии криптографии РФ

Член-корреспондент Российской инженерной академии

- **Межрегиональная общественная организация «Ассоциация защиты информации» (АЗИ) образована в 2002 году по инициативе ФАПСИ и Гостехкомиссии России.**
- **АЗИ активно взаимодействует с аппаратом Совета Безопасности РФ, ФСБ России, Федеральной службой технического и экспортного контроля (ФСТЭК), Федеральным агентством по информационным технологиям (ФАИТ), другими министерствами и ведомствами, а также со многими финансово-экономическими структурами.**
- **Устав АЗИ дает право осуществлять международные связи, разрешает вступать в международные общественные объединения, а также осуществлять внешнеэкономическую деятельность.**

- **Ассоциация готова оказывать содействие в налаживании деловых контактов и связей с целью реализации продуктов и технологий защиты информации, обмена деловой информацией, осуществления совместных разработок и промышленного производства, проведения симпозиумов, конференций, выставок, семинаров, организации обучения специалистов в области информационной безопасности.**

Основные направления деятельности АЗИ

определяются возможностями предприятий АЗИ:

- **Комплексная защита информационных ресурсов корпоративных систем**
- **Применение криптографических средств**
- **Защита информации от утечки по техническим каналам**
- **Поставка комплексных систем и средств ИБ**
- **Поставка защищенных средств вычислительной техники**
- **Независимый аудит ИБ объектов информатизации**
- **Проведение НИОКР**
- **Обеспечение экспортных поставок**
- **Подготовка кадров**

АЗИ входит в оргкомитет Национальной премии по безопасности «За укрепление безопасности России»

Одно интересных явлений рынка в области DLP В 2005 году - это появление на рынке продукта компании «Смарт лайт инк.» DEVICE LOCK

Это единственный продукт частично реализующий функционал DLP-систем, который получил высокую оценку золотую медаль и был выдвинут экспертами премии на получение ЗУБРа.

Членами АЗИ являются физические лица - руководители ведущих предприятий отрасли РФ

Первыми Членами Ассоциации являлись компании разработчики российских криптографических средств.

В Ассоциации представлена компания, которая является одним из первых разработчиков российского прообраза DLP-системы – это продукты ФОРПОСТ и УРЯДНИК, которые до настоящего времени стоят на вооружении некоторых ОГВ.

Данный продукт явился основой для первого российского продукта DLP-системы АВАНТПОСТ, который стоит на вооружении одной из служб ИБ крупнейшего коммерческого банка России.

Западные вендоры DLP-систем 2005 год

- InfoWatch
- Tizor
- Proofpoint
- Tablus
- Hackstrike
- Oakley Networks
- PacketMotion, Inc.
- WebSense и др.

Российские вендоры DLP-систем

- Инфосистемы Джет
- РНТ
- Инфовотч
- Софтинформ
- Смарт Лайн инк.
- Периметрикс и др.

Требования в DLP-системам

формируются запросами рынка и развитием новых технологий

- Информация может быть переписана на локальный компьютер, где может подвергаться несанкционированным правкам.
- Может быть отправлена по почтовым протоколам, в том числе зашифрованное.
- Сообщение, отправленное посредством клиентов, для мгновенного обмена сообщениями (ICQ, SKYPE, MSN Messenger и другие).
- Данные могут быть переписаны на съёмный носитель (например USB-носитель или CD/DVD диски).
- Могут быть распечатаны на принтере.
- Данные могут быть отправлены через альтернативные каналы IrDA-порты, Bluetooth, FireWire, Wi-Fi, 4G

Требования в DLP-системам

Существует распространённое решение проблемы утечки информации за пределы компании – блокировка каналов возможного хищения. Является ил этот вариант оптимальным. Можно блокировать возможность доступа к локальным дискам компьютера и к электронной почте. А также блокировка ICQ,SKYPE, USB-портов или доступа к записывающим CD/DVD устройствам и принтеру не даёт работать полноценно сотруднику.

Современные информационные системы должны позволять сотрудникам в рамках своей деятельности использовать все возможные каналы для передачи информации, при этом система должна иметь возможность контролировать и анализировать информационные потоки, идущие по этим каналам.

Кто не управляет информацией, тот не управляет компанией

Самое слабое звено практически всех реализованных **DLP-**проектов - человек, имеющий доступ к администрированию сети.

Способы контроля информационных потоков:

- Административный
- Организационный
- Технологический (DLP - системы и DLP - подобные системы), в том числе позволяющий контролировать действия все привелигированных пользователей
- Проверка на лояльность сисадминов

Бизнес и Государство: чем они могут быть полезны друг другу?

Бизнес- создание эффективных инструментов контроля, позволяющих реализовать требования регуляторов в части мониторинга доступа к персональным данным.

Государство - разработало механизм проверки таких продуктов на лояльность, а именно сертификация на отсутствие недекларированных возможностей, и это оправдано т.к. эти продукты обрабатывают и вырабатывают чувствительную информацию, в том числе различную по грифу.

СПАСИБО ЗА ВНИМАНИЕ

Минин Виктор

Председатель Общественного консультативного совета по научно-технологическим вопросам информационной безопасности Комиссии по информационной безопасности при Координационном совете государств-участников СНГ по информатизации при РСС,

Советник Председателя Ассоциация защиты информации

Член Правления Союза ИТ-директоров России,
Сопредседатель комитета по информационной безопасности