INFORMATION PROTECTION AND CONTROL

Information Protection and Control (IPC) — технология защиты конфиденциальной информации от внутренних угроз. Решения класса IPC предназначены для защиты информации от внутренних угроз, предотвращения различных видов утечек информации, корпоративного шпионажа и бизнес-разведки.

Термин IPC соединяет в себе две основные технологии: шифрование носителей информации на всех точках сети и контроль технических каналов утечки информации с помощью технологий Data Loss Prevention (DLP). Контроль доступа к сети, приложениям и данным является возможной третьей технологией в системах класса IPC. IPC включает в себя решения класса Data Loss Prevention (DLP), системы шифрования корпоративной информации и контроля доступа к ней. Термин IPC одним из первых использовал аналитик IDC Brian Burke в своём отчёте «Information Protection and Control Survey: Data Loss Prevention and Encryption Trends».

Технология IPC является логическим продолжением технологии DLP и позволяет защищать данные не только от утечек по техническим каналам, то есть инсайдеров, но и от несанкционированного доступа пользователей к сети, информации, приложениям и в тех случаях, когда непосредственный носитель информации попадает в руки третьих лиц. Это позволяет не допускать утечки и в тех случаях, когда инсайдер или не имеющий легального доступа к данным человек получает доступ к непосредственному носителю информации. Например, достав жесткий диск из персонального компьютера, инсайдер не сможет прочитать имеющуюся на нем информацию. Это позволяет не допустить компрометацию конфиденциальных данных даже в случае потери, кражи или изъятия (например, при организации оперативных мероприятий специалистами спецслужб, недобросовестными конкурентами или рейдерами).

Основной задачей IPC-систем является предотвращение передачи конфиденциальной информации за пределы корпоративной информационной системы. Такая передача (утечка) может быть намеренной или ненамеренной. Практика показывает, что большая часть (более 75 %) утечек происходит не по злому умыслу, а из-за ошибок, невнимательности, безалаберности, небрежности работников — выявлять подобные случае намного проще. Остальная часть связана со злым умыслом операторов и пользователей информационных систем предприятия, в частности промышленным шпионажем, конкурентной разведкой. Очевидно, что злонамеренные инсайдеры, как правило, стараются обмануть анализаторы IPC и прочие системы контроля.

Технология DLP в IPC поддерживает контроль следующих технических каналов утечки конфиденциальной информации:

- корпоративная электронная почта,
- веб-почта,
- социальные сети и блоги,
- файлообменные сети,
- форумы и другие интернет-ресурсы, в том числе выполненные на AJAX-технологии,
- средства мгновенного обмена сообщениями (ICQ, Mail.Ru Агент, Skype, AOL AIM, Google Talk, Yahoo Messenger, MSN Messenger и прочее),
- p2p-клиенты,
- периферийные устройства (USB, LPT, COM, WiFi, Bluetooth и прочее),
- локальные и сетевые принтеры.

Технологии DLP в IPC поддерживают контроль в том числе следующих протоколов обмена данными:

- FTP,
- FTP-over-HTTP,
- FTPS,
- HTTP,
- HTTPS (SSL),
- NNTP,
- POP3,
- SMTP.

Сигнатуры:

Самый простой метод контроля — поиск в потоке данных некоторой последовательности символов.

Иногда запрещенную последовательность символов называют **«стоп-выражением»**, но в более общем случае она может быть представлена не словом, а произвольным набором символов, например, определенной меткой. Если система настроена только на одно слово, то результат её работы — определение 100%-го совпадения, т.е. метод можно отнести к детерминистским. Однако чаще поиск определенной последовательности символов все же применяют при анализе текста. В подавляющем большинстве случаев сигнатурные системы настроены на поиск нескольких

Цифровые отпечатки (Digital Fingerprints):

Различного типа хеш-функции образцов конфиденциальных документов позиционируются западными разработчиками DLP-систем как новое слово на рынке защиты от утечек, хотя сама технология существует с 70-х годов. На Западе этот метод иногда называется «digital fingerprints». Суть всех методов одна и та же, хотя конкретные алгоритмы у каждого производителя могут отличаться. Некоторые алгоритмы даже патентуются, что помогает в продвижении «новой патентованной технологии DG». Общий сценарий действия такой: набирается база образцов конфиденциальных документов. Суть работы DG довольно проста и часто этим и привлекает: DLP/IPC-системе передается некий стандартный документ-шаблон, из него создается цифровой отпечаток и записывается в базу данных DF. Далее в правилах контентной фильтрации настраивается процентное соответствие шаблону из базы. Например, если настроить 75 % соответствие «цифровому отпечатку» договору поставки, то при контентной фильтрации DLP обнаружит практически все договоры этой формы. Иногда, к этой технологии относят и системы вроде «Антиплагиата», однако последняя работает только с текстовой информацией, в то время как технология «цифровых отпечатков»,

в зависимости от реализации, может работать и различным медийным контентом и применяться для защиты авторских прав и препятствию случайному или намеренному нарушению законов и нормативов информационной безопасности.

Метки:

Суть этого метода заключается в расстановке специальных «меток» внутри файлов, содержащих конфиденциальную информацию. С одной стороны, такой метод дает стабильные и максимально точные сведения для DLP-системы, с другой стороны требуется много довольно сильных изменений в инфраструктуре сети. У лидеров DLP- и IPC-рынка реализация данного метода не встречается, поэтому рассматривать её подробно не имеет особого смысла. Можно лишь заметить, что, несмотря на явное *достоинство* «меток» — качество детектирования, есть множество существенных *недостатков*: от необходимости значительной перестройки инфраструктуры внутри сети до введения множества новых правил и форматов файлов для пользователей. Фактически внедрение такой технологии превращается во внедрение упрощенной системы документооборота.

Регулярные выражения:

Поиск по регулярным выражениям («маскам) является также давно известным способом детектирования необходимого содержимого, однако в DLP стал применяться относительно недавно. Часто этот метод называют «текстовыми идентификаторами». Регулярные выражения позволяют находить совпадения по форме данных, в нем нельзя точно указать точное значение данных, в отличие от «сигнатур». Такой метод детектирования эффективен для поиска:

- ИНН,
- КПП,
- номеров счетов,
- номеров кредитных карт,
- номеров телефонов,

- номеров паспортов,

- клиентских номеров.

- Поиск по «маскам» позволяет DLP- или IPC-системе обеспечивать соответствие требованиям все более популярного стандарта PCI DSS, разработанного международными платежными системами Visa и MasterCard для финансовых организаций.

Лингвистические методы (морфология, стемминг):

Самым распространенным на сегодняшний день методом анализа в DLP/IPC-системах является лингвистический анализ текста. Он настолько популярен, что часто именно он в просторечье именуется «контентной фильтрацией», то есть несет на себе характеристику всего класса методов анализа содержимого. Лингвистика как наука состоит из многих дисциплин — от морфологии до семантики, и лингвистические методы анализа различаются между собой. Есть технологии, использующие лишь «стоп-выражения», вводящиеся только на уровне корней, а сама система уже составляет полный словарь; есть базирующиеся на расставлении весов встречающихся в тексте терминов. Есть в лингвистических методах и свои отпечатки, базирующиеся на статистике; например, берется документ, считаются пятьдесят самых употребляемых слов, затем выбирается по 10 самых употребляемых из них в каждом абзаце. Такой «словарь» представляет собой практически уникальную характеристику текста и позволяет находить в «клонах» значащие цитаты. Разбор всех тонкостей лингвистического анализа не входит в рамки этой статьи, однако необходимо заметить ширину возможностей данной технологии в рамках IPC-систем.

Ручное детектирование («Карантин»):

Ручная проверка конфиденциальной информации иногда называется «Карантином». Любая информация, которая попадает под правила ручной проверки, например, в ней встречается слово «ключ», попадает в консоль специалиста информационной безопасности. Последний по очереди вручную просматривает такую информацию и принимает решение о пропуске,

блокировке или задержке данных. Если данные блокируются или задерживаются, отправителю посылается соответствующее сообщение.