Елубаев Н.Р. - магистрант,
Казахский университет технологий и бизнеса,
г. Астана, Казахстан

СИСТЕМЫ ПРЕДОТВРАЩЕНИЯ ПОПЫТОК УТЕЧКИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Статья содержит обзор проблемы защиты и безопасности информации, назначения, режимов, технологий обнаружения утечек DLP (DataLossPrevention) –системы предотвращения утечек конфиденциальной информации изнутри организации.

This article contains an overview of the problems of protection and security of information, destination, mode, leak detection technology DLP (Date LossPrevention)-system to prevent leaks of confidential information within the organization.

Проблеме защиты и безопасности информации сегодня уделяют пристальное внимание. Этот вопрос все актуальнее встает перед организациями, ведь потеря маркетинговой информации ослабляет их позиции на рынке и делает их менее конкурентоспособными. От оптимальности выбора средств защиты информации зависит построение любой системы защиты информации.

Важно, чтобы средства защиты не только выполняли свои функции и обеспечивали ожидаемый уровень защиты, но и не увеличивали риск функционирования информационной системы (ИС) в конфликте с некоторыми другими средствами защиты. Каждый способ должен сначала быть проверенным, чтобы гарантировать, что он обеспечивает ожидаемую степень защиты.

Выбор любой корпоративной системы информационной безопасности зачастую является настолько же трудоёмким, насколько внедрение и последующая эксплуатация. DLP-системы лишь подтверждают это: на рынке сейчас существует несколько десятков различных продуктов с более чем сотней различных параметров, усложняющих выбор.

Основное назначение DLP (DataLossPrevention) — предотвращение утечек конфиденциальной информации изнутри организации. Классические DLP с помощью специальных технологий тщательно анализируют всю информацию, отсылаемую и выносимую сотрудниками за пределы организации, и принимают решение о разрешении или запрете их передачи. В некоторых продуктах все данные дополнительно архивируются.

В реальности далеко не все DLP способны в одиночку противостоять утечкам. Большинство DLP контролирует лишь часть потенциальных каналов утечки и использует ограниченное число технологий обнаружения несанкционированной передачи данных. Выбор еще больше осложняется тем, что многие разработчики архивов или систем контентной фильтрации относят свои продукты к классу DLP, хотя в большинстве случаев такие решения не могут ни заблокировать утечку, ни даже обнаружить передачу защищаемых данных. Ниже приведены вопросы, с помощью которых департамент информационных технологий сделал общий свод требований и выбор подходящей для организаций группы компаний АО НК «КазМунайГаз» DLP-системы.

Кроме непосредственной задачи обнаружения и блокировки утечек DLP позволяет решать множество задач: заблаговременно выявлять нелояльных сотрудников и потенциально опасные каналы коммуникаций, вести архив корпоративной электронной почты, распечатываемых документов и других данных. Также DLP может использоваться для повышения привлекательности организации в глазах клиентов, партнёров инвесторов и СМИ.

Как у любых ИТ-решений, у всех DLP есть свои плюсы и минусы, поэтому правильное определение приоритетности решаемых задач — важный шаг к выбору наиболее подходящего продукта.

Объём данных влияет на выбор типа DLP и сценария работы. Обычно при внедрении DLP встаёт вопрос выбора между активным и пассивным режимом работы. В первом случае DLP ставится “в разрыв” всех проходящих через границы сети данных и активно блокирует неразрешенную передачу информации, во втором система работает строго в уведомительном режиме, т. е. не блокирует передачу, а лишь сообщает о подозрительных инцидентах, занося всю информацию о каждом в журнал событий.

Существует и смешанный режим, когда DLP ставится “в разрыв”, но политики настраиваются таким образом, что предотвращаются только самые явные нарушения, а остальной трафик пропускается без какой-либо модификации. Кроме того, в активном режиме у большинства систем имеется возможность ручной проверки, т. е. подозрительные данные помещаются в “карантин” и ожидают ручной проверки сотрудником безопасности. Сценарий внедрения влияет на совокупную стоимость владения — в долгосрочной перспективе пассивный режим требует больших трудозатрат на анализ трафика и расследование, в то время как в активном режиме DLP автоматически блокирует большую часть утечек. При этом требования к оборудованию для всех сценариев примерно одинаковые — как минимум один производительный сервер, хотя при небольшой нагрузке можно установить DLP прямо на прокси-, почтовый или любой другой действующий сервер.

Структура и перечень защищаемых данных в первую очередь влияют на набор технологий обнаружения утечек, которым должна обладать DLP-система. Общий перечень возможных технологий включает в себя сигнатурный и лингвистический анализ, поиск по базам регулярных выражений и “цифровых отпечатков”, OCR (обнаружение текста на пересылаемых изображениях) и самообучающиеся технологии. К сожалению, пока далеко не каждая DLP-система предлагает хотя бы половину из приведенных технологий.

Каждая технология оптимальна лишь для определенного типа данных. “Цифровые отпечатки”— одна из наиболее популярных и простых в применении технологий, однако она эффективна для обнаружения довольно объёмных документов, редко подвергающихся изменениям. “Регулярные выражения” идеальны для обнаружения передачи персональных данных и информации с типовой структурой – номеров счетов, телефонов, адресов и т. д.

Лингвистические технологии (морфология и стемминг) хорошо работают с большинством типов данных, однако их эффективность зависит от тщательности настройки, которую, как правило, могут обеспечить лишь профессиональные лингвисты.

Несмотря на то что под защитой от утечек в большинстве организаций по-прежнему подразумевают лишь контроль внешних устройств, принтеров и электронной почты, полноценные DLP-системы также должны контролировать и другие каналы коммуникаций. В первую очередь сюда относится интернет-трафик: интернет-пейджеры, веб-почта, социальные сети, блоги, форумы, файлообменники, FTP, пиринговые сети, сервисы отправки SMS/MMS и т. д.

Далеко не все решения умеют контролировать весь перечень потенциальных каналов утечки. Так, у большей части западных DLP-решений контроль популярных в России и СНГ каналов коммуникаций пока вызывает серьезные проблемы. Например, передаваемые через интернет-пейджеры ICQ и Mail.Ru Агент данные могут анализировать лишь несколько DLP-решений на рынке.

Расследование инцидентов — важная часть любой системы защиты от утечек данных. Зачастую на практике необходимо не только обнаруживать и блокировать утечки, но и проводить служебное расследование по каждому инциденту. Такое расследование может включать в себя

как анализ непосредственно обнаруженных конфиденциальных данных, так и ретроспективный анализ активности пользователя или группы пользователей. К сожалению, многие DLP не только не позволяют произвольно архивировать перехватываемые данные, но и не сохраняют заблокированную информацию. В таком случае невозможно понять, что на самом деле было заблокировано, ведь даже самая технологичная DLP-система может ошибиться.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Андрончик А.Н. Защита информации в компьютерных сетях. – УГТУ-УПИ, 2008 – 248 с.
2. Анисимов А.А. Менеджмент в сфере информационной безопасности. – Изд-во: Интернет-университет информационных технологий, 2009. – 176 с.
3. Безбогов А.А., Яковлев А.В., Шамкин В.Н. Методы и средства защиты компьютерной информации: учебное пособие – Тамбов: Изд-во Тамб. гос. техн. ун-та, 2006. – 196 с.
4. Белов Е.Б. Основы информационной безопасности. - Москва: Горячая линия - Телеком, 2006. – 544 с.
5. Блинов А.М. Информационная безопасность: Учебное пособие. Часть 1. – Санкт-Петербург: Изд-во СПбГУЭФ, 2010. – 96 с.
6. Бойцев О.М. Защити свой компьютер на 100% от вирусов и хакеров. – Санкт-Петербург: Питер, 2008. – 288 с.