V. F. Govorun. S. M. Babashev

S. Toraighyrov Pavlodar State University, Pavlodar.

Development of wind energetics in Kazakhstan

Material received on 15.12.2015.

Мақалада жел энергетикасы экологиялық зиянсыз энергия өндіру ғана емес, сонымен қатар әлеуметтік-экономикалық даму, энергетикалық қауіпсіздікті қамтамасыз ету және электр энергиясына баганы төмендету қарастырылған.

The research considers wind energetics not only as environmentally friendly energy production, but as the subject of maintaining social and economic development, ensuring energy security and reduction of electricity prices.

УДК 004.056

А. Ю. Гречанная, А. Д. Тастенов
Павлодарский государственный университет имени С. Торайгырова, г. Павлодар

DLP-СИСТЕМЫ И ИХ РОЛЬ В ЗАЩИТЕ ОТ УТЕЧЕК КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

В данной статье приведены сведения об эффективности использования DLP-систем в защите от утечек конфиденциальной информации.

Ключевые слова: DLP – системы, информационная безопасность, конфиденциальность, утечка информации, право доступа.

Эффективность бизнеса во многих случаях зависит от сохранения конфиденциальности, целостности и доступности информации. В настоящее время одной из наиболее актуальных угроз в области информационной безопасности является утечка конфиденциальных данных от несанкционированных действий пользователей.

Это обусловлено тем, что большая часть традиционных средств защиты, таких как антивирусы, межсетевые экраны и системы аутентификации не способны обеспечить эффективную защиту от внутренних нарушителей. Целью такого рода нарушителей (инсайдеров) является передача информации за пределы компании с целью её последующего несанкционированного использования – продажи, опубликования её в открытом доступе и так далее.

В последнее время активно разрабатывались технологии, позволяющие предотвратить утечку конфиденциальной информации. последнихнесколькихл етиспользоваласьобширнаятерминология: Information Leakage Protection (ILP), Information Leak Protection (ILP), Information Leakage Detection & Prevention (ILDP), Content Monitoring and Filtering (CMF), Extrusion PreventionSystem (EPS) и другие. Но окончательным и наиболее точным термином принято считать аббревиатуру DLP (DataLeakPrevention), предложенную агентством Forrester в 2005 году. В качестве русского аналога принято словосочетание «системы

защиты конфиденциальных данных от внутренних угроз». При этом под внутренними угрозами подразумевают как умышленные, так и непреднамеренные злоупотребления сотрудниками своими правами доступа к данным [1].

Системы защиты от утечек конфиденциальной информации предназначены для отслеживания и блокирования попыток несанкционированной передачи данных за пределы корпоративной сети. Помимо предотвращения утечек информации DLP-система может выполнять функции по отслеживанию действий пользователей, записи и анализу их коммуникаций через e-mail, социальные сети, чаты и так далее. Основная задача систем DLP – обеспечение выполнения принятой в организации политики конфиденциальности (защита информации от утечки).

Использование DLP системы наиболее актуально для организаций, где риск утечки конфиденциальной информации повлечет серьезный финансовый или репутационный ущерб, а также для организаций, которые настороженно относятся к лояльности своих сотрудников. Решения класса DLP по предотвращению утечек информации обеспечивают защиту такой конфиденциальной информации, как условия тендеров, заказы на услуги и решения, номера пластиковых карт, сведения о счетах клиентов, персональные данные сотрудников и клиентов, финансовые данные и так далее.

Основные функции DLP-систем:

– контроль передачи информации через Internet с использованием электронной почты e-mail, протоколов HTTP(HyperTextTransferProtocol– Протокол передачи гипертекста), HTTPS (HyperTextTransferProtocolSecure – Расширение протокола HTTP, поддерживающее шифрование), FTP (FileTransferProtocol– Протокол передачи файлов), Skype, служба мгновенного обмена сообщениями сети Internet ICQ и других приложений и протоколов;

– контроль сохранения информации на внешние носители – CD, DVD, flash-диски, мобильные телефоны и прочее;

– защита информации от утечки путем контроля вывода данных на печать через принтерные (LPT) порты, а также утечка через модемные (COM) порты;

– блокирование попыток пересылки/сохранения конфиденциальных данных, информирование администраторов ИБ об инцидентах, создание теневых копий, использование карантинной папки;

– поиск конфиденциальной информации на рабочих станциях и файловых серверах по ключевым словам, меткам документов, атрибутам файлов и цифровым отпечаткам;

– предотвращение утечек информации путем контроля жизненного цикла и движения конфиденциальных сведений.

Обычно система класса DLP включает следующие компоненты:

– центр управления и мониторинга;

– агенты на рабочих станциях пользователей;

– сетевой шлюз DLP, устанавливаемый на Internet-периметр.

Результат применения решения:

– предотвращение утечек и несанкционированной передачи конфиденциальной информации;

– минимизация рисков финансового и репутационного ущерба;

– повышение дисциплины пользователей;

– материал для расследования инцидентов и их последствий;

– ликвидация угроз безопасности персональных данных, соответствие требованиям по защите персональных данных [2].

Сегодня на рынке существует довольно много продуктов, позволяющих детектировать и предотвращать утечку конфиденциальной информации по тем или иным каналам. Однако комплексных решений, покрывающих все существующие каналы, значительно меньше. В этих условиях чрезвычайно важным становится выбор технологии, обеспечивающей защиту от утечек конфиденциальной информации с максимальной эффективностью и минимальным количеством ложных срабатываний.

Все чаще и чаще возникающие утечки важной документации стали причиной беспокойства многих руководителей компаний, и этим обуславливается востребованность и актуальность систем DLP в настоящее время.

Так почему же системы DLP становятся популярными только сейчас? Ведь подобные технологии у многих вендоров существовали уже давно. Раньше задачи, которые должна была решать система DLP, считались неразрешимыми с помощью технических средств, а сами системы были слишком сложными для внедрения. Теперь же продукты полностью отвечают всем требованиям.

Популярность DLP-систем растет естественным путем, она не является маркетинговым ходом. От угроз извне большинство компаний защитилось уже давно и всеми возможными способами. А вот актуальность угроз изнутри растет с каждым годом. Конечно, как и любая другая, технология DLP еще будет совершенствоваться, но уже сегодня эффективность систем защиты данных очень высока. Особенно это касается исполнения первоочередной задачи, поставленной разработчиками для DLP – сократить количество ложных срабатываний для случаев утечки информации, спровоцированных по халатности, неумышленно.

В DLP-системах обычно используются три метода идентификации: вероятностный, детерминистский и комбинированный. Системы, основанные на первом методе, по большей части используют лингвистический анализ контента и «цифровые отпечатки» данных. Такие системы просты в реализации, но недостаточно эффективны и характеризуются высоким уровнем ложных срабатываний. Системы, использующие детерминированный подход (метки файлов), очень надежны, но им не хватает гибкости. Комбинированный подход сочетает оба метода с аудитом среды хранения и обработки данных, что дает возможность достичь оптимального решения проблемы защиты конфиденциальности информации.

Есть два основных подхода анализа контента. Первый подход базируется на фильтрации контента, то есть содержательного наполнения информации. Это означает, например, что при проверке на секретность стандартных офисных документов в формате .doc система сначала переведет их в текстовый формат, а затем, используя заранее подготовленные данные, вынесет по этому тексту

вердикт. Контекстная фильтрация использует принципиально другую схему: система проверяет контекст, в котором передается информация: извлекает метки файла, смотрит на его размер или анализирует поведение пользователя.

Системы DLP необходимы для всех компаний, которые хотят предотвратить утечку критически важной для бизнеса информации. Если говорить более конкретно, то в первую очередь можно упомянуть банки и страховые компании, которые вынуждены выполнять требования регуляторов. Для их бизнеса особенно актуальна утечка конфиденциальных данных, так как она чревата серьезными репутационными рисками.

Приняты четыре критерия оценки программных продуктов, реализующих функциональность DLP, сформулированных компанией ForresterResearch (независимая исследовательская фирма, которая предоставляет объективные данные о рынке новых технологий, а так же осуществляющей профильные консультации):

– многоканальность. Решение DLP не должно быть сосредоточено только на одном канале утечек. Это должно быть комплексное решение, охватывающее максимальное количество каналов: e-mail, Web и IM(Instantmessaging – Система мгновенных сообщений), а также мониторинг файловых операций;

– унифицированный менеджмент. Система должна обладать унифицированными средствами управления всех компонентов, которые она в себя включает. Их, как правило, три: менеджмент-сервер, на котором хранятся политики групп пользователей; устройство, которое отслеживает утечку через сеть; агенты для рабочих станций, серверов, файловых хранилищ. Главное требование второго критерия – возможность управлять этими тремя компонентами с одной консоли;

– активная защита. Система должна не только фиксировать утечку конфиденциальной информации, но и давать возможность ее блокировать;

– классификация информации с учетом, как содержимого, так и контекста. Утечки конфиденциальной информации должны базироваться не только на содержимом пересылаемой информации, но и на контексте, в котором она происходит: какой используется протокол, какое приложение, от какого пользователя, куда и так далее [3].

Сегодня на этом рынке существует не менее 8 крупных производителей, чьи DLP-продукты – результат поглощений: PortAuthority стала частью соответственно Websense; Onigma и Reconnex стали частью McAfee; Tablus – RSA (EMC), Vontu – Symantec, Orchestria – Raytheon, Provilla – Trend Micro, Consul – IBM, IronPort– Cisco.

В странах СНГ представлены такие вендоры как InfoWatch, McAfee, Websense, Symantec.

Современные DLP-системы умеют проверять все документы, отправляемые на печать, и даже подтверждать наличие в офисе того сотрудника, от имени которого сформировано задание печати. Но после того как документ напечатан, его распространение отследить крайне сложно. За физическим перемещением бумажного носителя ныне можно проследить только организационно-правовыми методами, на технику здесь надежды мало.

Создатели DLP-решений сегодня столкнулись с новым вызовом. Понятие защищенного периметра организаций, по сути, ушло в прошлое, потому системы защиты каналов утечки информации должны обеспечить безопасность данных как внутри инфраструктуры компании, так и за ее пределами. Речь идет о необходимости объединить в рамках DLP-систем технологии, позволяющие контролировать каналы утечек информации, а также находить и контролировать принадлежащие компании данные, в том числе на просторах глобальной сети.

СПИСОК ЛИТЕРАТУРЫ

1 Технологии InfoWatch для анализа и защиты. – www.infowatch.ru, 2013.

2 Защита от утечек конфиденциальной информации (DataLossPrevention–DLP) – security-microtest.ru

3 Системы DLP – itglobal.su

Материал поступил в редакцию 15.12.2015.

А. Ю. Гречанная, А. Д. Тастенов

DLP-жүйелері және құпия ақпараттың жайылып кетулерінен қорғаныс

С. Торайғыров атындағы Павлодар мемлекеттік университеті, Павлодар қ.

Материал 15.12.2015 баспаға түсті

A. Grechannaya, A. Tastenov

DLP-systems and their role in protection against leakage of confidential information

S. Toraighyrov Pavlodar State University, Pavlodar.

Material received on 15.12.2015.

Осы мақалада құпия ақпараттың жайылып кетулерінен қорғаныс DLP - жүйесінің пайдалану тиімділігі туралы айтылған.

This research provides information on the effectiveness of DLP-systems in protecting confidential information from leakage.