Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Макаров М.В. Необходимость использования DLP-систем (Data Loss Prevention) - для защиты данных корпоративных сетей // Академия педагогических идей «Новация». Серия: Студенческий научный вестник. – 2017. – № 06 (июнь). – АРТ 249-эл. – 0,2 п.л. - URL: http: //akademnova.ru/page/875550

РУБРИКА: ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 004.056.53

Макаров Михаил Вениаминович
студент 1 курса, институт заочного и дистанционного образования
ФГБОУ ВО «Московский технологический университет» МИРЭА
г. Москва, Российская Федерация
e-mail: mikhail-makarov@mail.ru

НЕОБХОДИМОСТЬ ИСПОЛЬЗОВАНИЯ DLP-СИСТЕМ (DATA LOSS PREVENTION)- ДЛЯ ЗАЩИТЫ ДАННЫХ КОРПОРАТИВНЫХ СЕТЕЙ

Аннотация: В статье рассмотрена необходимость использования DLP-систем в корпоративных сетях для защиты данных.

Ключевые слова: DLP-система, защита данных, корпоративная сеть.

Makarov Mikhail
1st year student, institute of correspondence and distance education
FGBOU VO «Moscow University of Tehnology» MIREA
Moscow, Russian Federation

THE RELEVANCE OF THE USE OF DLP-SYSTEMS (DATA LOSS PREVENTION) FOR DATA PROTECTION OF CORPORATE NETWORKS

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Abstract: The article considers the relevance of the use of DLP-systems in corporate networks .

Keywords: DLP-system, data protection, corporate network.

Для организаций, которые используют локальные сети или Интернет в качестве основных операционных инструментов их деятельности, потеря или раскрытие критически важных данных может оказаться фатальным.

Бреши в системах безопасности для нас уже являются обычным явлением. Чуть ли не каждую неделю происходят хакерские атаки на сайты и электронные почтовые ящики мелких и крупных организаций,а вместе с этим множество злонамеренных действий сотрудников компании или простые человеческие ошибки могут привести к потере конфиденциальной и важной для стратегии развития и функционирования бизнеса информации.Именно на такие действия приходится до 85% всех утечек критически важной информации.

Поэтому, автоматизация процесса защиты данных в корпоративных сетях даст значительно лучшие результаты, чем просто полагаться на людей,подверженным ошибкам. Для предотвращения инциндентов,которые могут повлечь за собой серьезные последствия,следует внедрять системы защиты данных класса DLP.

DLP (Data Loss Prevention)-система-это готовый программный продукт, созданный для предотвращения утечек важной или конфиденциальной информации за пределы корпоративной сети. Строение этой системы основано на анализе потоков данных как внутри, так и выходящих за пределы корпоративной сети. В случае сработки определенной сигнатуры и обнаружения передачи конфиденциальной

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

информации система либо блокирует такую передачу, либо посылает уведомления администратору по безопасности.

Корпоративная сеть-это сложная система, с большим количеством потенциальных точек утечки данных. Поэтому в стратегии внедрения DLP-системы необходимо принять во внимание множество факторов. Обстоятельства внедрения будут варьироваться от организации к организации в рамках целевого и их оперативного режимов функционирования.Однако,DLP-система может быть внедрена в IT-инфраструктуре любого масштаба и сложности,она легко масштабируется без ущерба функциональным возможностям,а также способна работать в автономном режиме.

Основные возможности DLP-систем включают в себя следующее:

- мониторинг внутренней и Интернет электронной переписки, сетевого трафика, приложений и использование средств массовой информации – с ограничениями и элементами дополнительного контроля;

- проверка и, при необходимости, блокирование потоков информации по электронной почте (внутренней и Интернет), HTTP и HTTPS переходов, доступа к документам через FTP-соединения,публикации документов или информации через Web-интерфейсы;

-инспектирование тем, текстов и вложений исходящих сообщений, для потенциально важных областей;

-установление и осуществление политики безопасности для мониторинга и возможного блокирования передачи документов или информации через Web-мессенджеры и социальные сети;

-установка уровней риска для исходящей электронной почты и сообщений, связанных с ними действий (например, блокировка,оповещение, шифрование);

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

- шифрование сообщений электронной почты для дополнительной безопасности и в соответствии с определенными нормативными требованиями;

-уведомление конечных пользователей и сетевых администраторов, когда возникают вопросы несоблюдения или нарушения корпоративной политики.

Скорейшее принятие организациями и внедрение программных DLP-решений сосредоточено на конечном анализе и мониторинге сетевого трафика ноутбуков, настольных систем, электронной почты, мобильных устройств, USB-дисков и съемных носителей.

На современном IT-рынке существует множество производителей различных DLP-систем в зависимости от функциональных потребностей и масштаба организации .Рассмотрим характеристики основных параметров программных продуктов лидеров отрасли: InfoWatch,Symantec,SearchInform и FalconGaze.

Таблица “Сравнительная характеристика основных параметров DLP-систем”

Параметр	InfoWatch	Symantec	SearchInform	FalconGaze
Модульность системы	Да	Нет	Да	Нет
Роли	Несколько	Любое количество	Любое количество	Администратор системы
Контроль HTTP/HTTPS, FTP	Да	Да	Да	Да
Контроль подключаемых внешних устройств	Да	Да	Да	Нет
Контроль портов	USB,COM,LPT, Wi-Fi, Bluetooth	USB,COM,LPT, Wi-Fi, Bluetooth	USB, LPT	USB, LPT
Блокируемые протоколы	HTTP, HTTPS, FTP, FTP over HTTP, FTPS, SMTP, SMTP/S, ESMTP, POP3, POP3S, IMAP4, IMAP4S	SMTP, HTTP, HTTPS FTP, Yahoo Messenger, MSN Messenger, AIM, AIM Pro Messenger, MSN Messenger,	SMTP, POP3, MAPI, IMAP, HTTP,FTP, ICQ, Jabber	HTTP, HTTPS, FTP, FTTPS, Вся почта и IM

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

		AIM, AIM Pro Messenger, MSN Messenger, AIM, AIM Pro		
Режимы оповещений	Консоль, почта	Консоль, почта, графики	Консоль, почта, графики	Консоль, почта, графики
Возможность тестирования продукта на серверах разработчика	Нет	Да	Нет	На сервере дистрибьютора

Исходя из сравнительных характеристик, DLP-системы позволяют полностью контролировать использование конфиденциальной информации, управлять данными,повысить общий уровень информационной безопасности,а также предотвратить утечку критически важных данных за пределы организации - умышленно или непреднамеренно.

Список использованной литературы:

1. Jessie Russel, Ronald Cohn «Предотвращение утечек информации» Москва, 2013
2. Выбираем DLP-систему для средней организации. — URL: http://habrahabr.ru
3. Understanding DLP. —URL: http://www.infosectoday.com

Дата поступления в редакцию: 14.06.2017 г.
Опубликовано: 17.06.2017 г.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Для заметок