Внедрение DLP-решений для КВО

Барановский Александр, директор ООО «НПТ»

Справка ТБ

Барановский Александр Валерьевич, окончил БГУИР, ФИТУ в 2000 г. После службы в пограничных войсках РБ занимал руководящие должности в ряде коммерческих организаций. С 2009 г. — директор компании «НПТ», эксперт по информационной безопасности. Автор ряда публикаций и исследований.

Сегодня мы поговорим о DLP-системах. Это класс программного обеспечения, имеющий наибольшую важность для обеспечения информационной безопасности. Сегодня многие компании и государственные организации приобретают DLP-системы для защиты своих данных. К сожалению, далеко не все специалисты по безопасности знакомы с DLP-системами, поэтому необходимо рассказать о них вкратце, прежде чем переходить к практике.

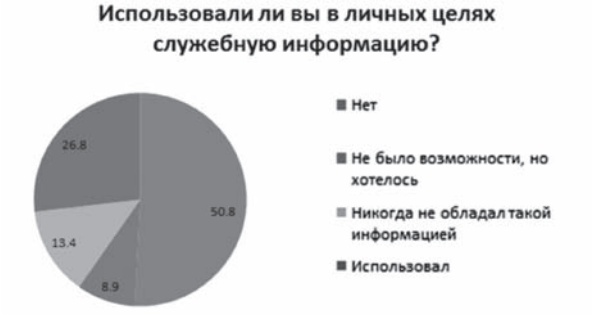
Согласно нашему исследованию, около 9-10% рабочего времени в коммерческих организациях и банках сотрудники тратят на занятия, не связанные с работой (социальные сети, «аська», просмотр фильмов и т.п.). В государственных предприятиях — уже около 19%. Лидером являются проектные организации — там такой вид активности занимает 36% рабочего времени.

Еще одна проблема заключается в том, что сотрудники используют ресурсы предприятия, дорогой лицензионный софт, плоттеры и т.п., делают «левые» проекты, что несет за собой финансовый ущерб для организации. Понятно, что мириться с этим нельзя, однако и на этом сложности не заканчиваются. Следует отметить также проблему передачи сотрудниками конфиденциальной информации за пределы организации (утечка информации). На сегодня существует много каналов потери информации. В первую очередь, это:

1) электронная почта;

2) клиенты для мгновенного обмена сообщениями (ICQ, MSN Messenger, QIP, Jabber);

3) Skype, который считается наиболее защищенным, и в основном все непубличные беседы происходят именно в нем;



Опрос пользователей

4) информация в виде файлов может быть передана по FTP-протоколу;

5) запись на съемный носитель (USB-флешку или CD/DVD диски);

6) распечатка на принтере.

Зачастую компании выбирают методологию запрета каких-то определенных способов, минимизируют количество каналов потенциальной утечки информации. Например, запрещают использовать флэшки, ICQ и т.д. Создается иллюзия безопасности, на самом же деле это недостаточно эффективное решение. Дело в том, что при подобных запретах сотрудник теряет мобильность. Чтобы передать необходимые документы на USB-носителе, сотруднику необходимо обратиться в службу безопасности, которая откроет порт и даст добро на запись документов. Это потеря рабочего времени, и в масштабах организации потери будут достаточно заметными.

Использование рабочего времени сотрудниками в банках

Гораздо эффективнее позволить сотруднику пользоваться привычными и удобными для него способами передачи информации, при этом контролировать данный процесс. Перехват информации никакой сложности сегодня не представляет, для этого существует ряд бесплатных программ. Но производить поиск в больших объемах весьма проблематично, для этого нужен качественный аналитический модуль. Причем из-за необходимости обработки неструктурированной информации простой «поиск по словам» не подходит, иногда нужен поиск похожего, возможность поменять слова местами. В таком случае необходимо обратиться в компании, хорошо зарекомендовавшие себя на рынке корпоративного поиска.

Очень важным аспектом анализа перехваченных данных являются *синонимические ряды*. Можно по общению двух людей понять, о чем идет речь, даже если говорят они иносказательно. Например, с силовыми структурами мы разработали синонимический ряд по получению взятки.

DLP-системы как раз и отличаются от обычных перехватчиков данных (снифферов) тем, что позволяют не только перехватывать, но и анализировать перехваченную информацию. Впрочем, этим их возможности не ограничиваются. Рассмотрим подробнее. Все они в полной мере реализованы в предлагаемом нашей компанией решении — «Контуре информационной безопасности SearchInform».

Интеграция с доменной структурой Windows. С ее помощью достаточно легко определить пользователя, который отправил почту, сообщение, можно определить, какой пользователь и в какое время, с какой рабочей станции, какие ресурсы использовал для отправки любого рода информации. Часто сотрудники пытаются обойти подобные системы. Архивируя почту, ставят на нее пароль, передают информацию в графическом виде. Однако **полноценная DLP-система позволяет отследить этот процесс** и выявить злоумышленника. **DLP-системы дают возможность определить группу риска.** Например, из 10 тысяч сотрудников выбрать 500, которые уже были замечены в нарушениях инфор-

Использование рабочего времени сотрудниками в гос.предприятиях

мационной безопасности. В случае проведения внутреннего расследования легко получить информацию по конкретному сотруднику, посмотреть его активность за заданный промежуток времени.

Модуль электронной почты позволяет происходить перехвату всех протоколов электронной почты, в том числе через Web-интерфейс. Все блоги, форумы, куда сотрудник может написать информацию, также легко контролируются и перехватываются.

FTP-протокол предназначен для передачи данных больших объемов (чертежи, финансовая информация и т.д.). По нему могут происходить наиболее опасные для организации утечки информации, поэтому данный канал необходимо контролировать не менее тщательно, чем ту же электронную почту.

Мы являемся первой компанией на территории СНГ, которая начала перехватывать **Skype**: текстовые сообщения, пересылаемые файлы и голосовые сообщения.

Также поддерживается и стандартный для современных DLP-систем **перехват Интернет-месенджеров и печати**. Есть возможность перевода графической информации в текстовый вид с последующим полнотекстовым поиском. Все, что пишется на съемные устройства, перехватывается, складывается и хранится определенное время.

Модуль **MonitorSniffer** позволяет в режиме реального времени отслеживать одновременно до 16 рабочих столов пользователей. Кроме того, позволяет делать снимки с определенным интервалом времени, своеобразный скриншот. Параллельно безопасник может отслеживать загруженные процессы.

FileSniffer обеспечивает эффективный и оперативный контроль того, кто и каким образом использует хранящуюся на файл-серверах конфиденциальную информацию.

Индексация рабочих станций позволяет отследить появление конфиденциальной информации на компьютерах пользователей, а также любые действия над ней.

ReportCenter позволяет отследить связи между сотрудниками как внутри организации, так и вне ее. Кроме того, позволяет собирать статистику по активности пользователей и инцидентам, связанным с нарушениями политики безопасности, представляя ее в виде отчетов.

В организациях есть сотрудники, которые часто ездят в командировки и берут с собой ноутбук. Опасности подвергается информация, которая в нем находится. **EndpointSniffer** позволяет отследить все те же информационные потоки, которые я перечислял, но уже локально, на отключенной от сети рабочей станции. При подключении обратно в сеть этой рабочей станции происходит пересылка информации в общую базу данных. Также данный модуль позволяет контролировать внешние устройства, перехватывать шифрованные протоколы и Skype.

«Контур информационной безопасности SearchInform» позволяет предупреждать не только заранее спланированные, но и случаные утечки. Например, в банковской сфере часто существует такая проблема. Сотрудник имеет какой-то план работы за день, скажем, оформление 20 заявок на получение кредита. За день он успевает сделать 15, премия же выплачивается при норме 20. Пять оставшихся заявок сотрудник скидывает на свой электронный ящик, без какого-либо злого умысла, дома спокойно завершает работу, утром приносит отчет за предыдущий день. Он не думает о том, что эти заявки могут пройти через несколько бесплатных ресурсов и быть кем угодно перехвачены, либо же утечка может произойти при взломе бесплатного ящика сотрудника. С нашим решением можно отследить такие действия и сотрудников, подобным образом нарушающих должностные инструкции.

Преимущества Контура информационной безопасности:

1. **Простота и скорость внедрения.** Среднее время развертывания системы — около 2-х часов.
2. **Возможность контроля всех каналов передачи информации**, которые существуют на предприятии.
3. **Функция «поиск похожих».** Уникальная функция, которая позволяет искать текст, похожий по смыслу на задаваемый в параметрах. Также отслеживаются случаи перестановки слов или целых абзацев в тексте.
4. **Полная идентификация пользователя.**

Использование рабочего времени сотрудниками в проектных организациях

Вопросы:

– Сейчас развиваются корпоративные сети на основе ноутбуков, нетбуков, беспроводных сетей. Каким образом адаптируются DLP-системы в таких корпоративных сетях?

– На самом деле, для нас нет разницы, по какому принципу построена сеть. Существует как вариант установки через контроль зеркалируемого трафика, так и вариант, когда устанавливается программа-агент на рабочую станцию.

– Как ваша DLP-система будет согласовываться с системой обнаружения/вторжения?

– В случае установки агента необходимо в большинстве случаев наш «Контур» добавлять в доверительные приложения антивирусов, после чего никаких уведомлений появляться не будет.

– Контроль передачи голосовых сообщений Skype и контроль монитора предполагает наличие клиентской части. В случае использования клиентом технологии «Tor» ваш шлюз зафиксирует, какие ресурсы пользователь посещает?

– В этом случае будет зафиксирована передаваемая информация и указано, кем реализовано действие. Какие ресурсы посещались, мы не отслеживаем, нам важна информация, которая передается, в том числе и по технологии TOP. Кстати, наше решение является единственным из DLP, которое позволяет полноценно контролировать информационные потоки при использовании терминальных решений.

– Авторизация в Skype происходит…

– По имени. Есть привязка — какой пользователь, с какого компьютера и в какое время авторизировался.

– Под какой платформой вы работаете?

– Под Windows.

– Какова стоимость системы?

– Весь комплект модулей — из расчета 4 млн за 1 рабочее место. Но ненужные для организации модули можно убрать, что значительно сократит стоимость.

ООО «НПТ»
220012, г. Минск, ул. К.Чорного, 5А, пом.5а
Тел.: (029) 649-77-79
E-mail: ab@searchinform.ru
Сайт: www.searchinform.ru