Computerworld Россия 2008 № 31

Поисковая разведка

18.09.2008 Валерий Коржов

- Ключевые слова :
- Предприятие

Сохранять конфиденциальную информацию при подключении к Internet становится все труднее. Иногда ценная информация может попасть в общий доступ случайно или по злому умыслу внутренних недоброжелателей. При неправильной настройке Web-сервера или прав доступа к корпоративной сети ценная информация о компании может оказаться доступной из Internet для всех желающих.

Сохранять конфиденциальную информацию при подключении к Internet становится все труднее. Иногда ценная информация может попасть в общий доступ случайно или по злому умыслу внутренних недоброжелателей. При неправильной настройке Web-сервера или прав доступа к корпоративной сети ценная информация о компании может оказаться доступной из Internet для всех желающих. Исключить подобную угрозу можно, только отключившись от Internet полностью, однако в современных условиях это практически нереально.

Чтобы обезопасить свою компанию от такого рода неприятностей, сотрудникам, отвечающим за информационную безопасность предприятия, стоит контролировать наличие в общем доступе ценной для компании информации. Методике проведения подобных исследований был посвящен семинар компании «ДиалогНаука», названный «Практические аспекты проведения аудита утечек конфиденциальной информации в сети Интернет на основе технологий конкурентной разведки».

Термин «конкурентная разведка» Андрей **Масалович**, руководитель одноименного направления компании «ДиалогНаука», определил как шпионаж с использованием только легальных способов получения информации. Наиболее ценным источником конфиденциальных сведений сейчас является Internet. Поэтому большинство задач конкурентной разведки можно решить с помощью Сети. В частности, Internet позволяет проводить разовый поиск информации о партнерах, поставщиках или клиентах, проводить мониторинг информационной активности контрагентов, анализировать популярность ресурсов и их эмоциональную окраску, выявлять информационные атаки, их направление и авторство, а также контролировать утечки собственных конфиденциальных данных.

Поиск информации в Internet можно выполнять с помощью общедоступных поисковых машин или специализированных инструментов, таких как метапоисковые машины или персональные средства Internet-поиска. Для разового поиска можно пользоваться общедоступными поисковыми системами, например Google или «Яндексом». Однако результаты этих поисковиков сильно зашумлены «поисковым спамом», и для получения нужной информации приходится пользоваться различными приемами: расширенным языком самого поисковика или правильным подбором слова для составления запроса. Масалович утверждает, что есть около 15 ключевых слов, которые позволяют существенно улучшить качество результатов определенных поисковых запросов.

Однако эффективный контроль за утечками конфиденциальной информации должен быть не разовым, а постоянным. Это позволит вовремя обнаружить утечку, оперативно найти ее причину и ограничить распространение опасной для компании информации. Открытых инструментов для мониторинга информационного пространства Internet нет, поэтому приходится использовать специализированные инструменты. Впрочем, по заверениям Масаловича, для конкретной компании достаточно проверять информацию, которая публикуется всего на 50 сайтах: «Этого, как правило, достаточно, чтобы быть в курсе всех новостей по определенной теме: если событие не заметили ключевые средства массовой информации, то его не заметит никто».

Со своей стороны, в «ДиалогНауке» собираются представить осенью этого года вторую версию специализированного инструментария Avalanche. Он предназначен для постоянного мониторинга ключевых сайтов Internet и обнаружения на них конфиденциальных сведений. Для использования этого инструмента аналитик должен определить ключевые сайты и их тематическую направленность — это приходится делать с помощью открытой поисковой машины. Однако, когда эти сайты определены, аналитик может ежедневно просматривать новости по заданным им темам.

Продукт Avalanche 2.0 существует только в персональной версии, однако аналитики могут образовать коллектив и обмениваться результатами работы при условии, что у всех определены одинаковые структуры каталогов. Формирование подобных корпоративных аналитических центров берет на себя и «ДиалогНаука». Для таких проектов компания может настроить Avalanche так, что он будет искать и документы, которые по тем или иным причинам невидимы для других поисковых машин. Впрочем, клиенты могут заказать у «ДиалогНауки» и специальную услугу по аудиту утечек конфиденциальной информации, которую проводят сами сотрудники компании. На основе анализа Internet они определяют, какие данные о компании распространены в Internet и как можно обнаруженную информацию удалить. Проведение подобного аудита помогает компании определить наличие ценной информации в общем доступе и перекрыть с помощью специальных систем все каналы утечки.