Защита от профессионалов

Сформулирована концепция защиты от утечек, вызванных вредоносным программным обеспечением

ВАЛЕРИЙ КОРЖОВ
Computerworld Россия

Инструменты защиты от утечки данных (Data Leakage Protection, DLP) существуют довольно давно. Их концепция оформилась после принятия в 2002 году в США закона Сарбейнса-Оксли, который, в частности, обязал компании фиксировать утечки конфиденциальных данных и сообщать о них клиентам. Для реализации этих требований и появился класс программных продуктов, контролирующих передачу данных и фиксирующих случаи передачи вовне конфиденциальных сведений, таких как персональные данные, номера кредитных карт, пароли и др. В России первым специализированным поставщиком решений этого класса продуктов стала образованная в 2004 году компания InfoWatch. Несколько позже сформировалось профессиональное объединение DLP Expert, ежегодно оно проводит конференцию DLP-Russia, посвященную проблемам защиты от утечек конфиденциальной информации.

14-15 октября состоялась третья конференция, и на ней были сформулированы новые принципы построения DLP. Тарик Мустафа, директор и основатель компании nexTier Network, описал новый тип защиты, которую он назвал Malicious Data Leak Prevention (MDLP), то есть «защита от воровства данных посредством вредоносных программ». Дело в том, что классические продукты DLP защищают в основном от утечек по открытым каналам, таким как электронная почта, протокол HTTP, флэшки и др. Для корректной работы такого инструмента важно, чтобы он мог разобрать, какие именно данные передаются по каналу. Утечки такого рода вызваны в основном нарушениями в работе с конфиденциальной информацией.

В то же время профессиональные утечки, как правило, организуются с помощью специализированных программных средств, которые предназначены для организации скрытых каналов передачи данных. Они не позволяют сенсорам классического DLP-инструментария прочитать содержимое, используя для этого шифрование и необычные протоколы. Как результат доступные на рынке инструменты DLP не могут защитить от атак с помощью подобного типа троянских программ. Для защиты от подобных приложений, по мнению Мустафы, нужно использовать специальные методы определения утечек и защиты от них.

ТАРИК МУСТАФА объяснил, чем MDLP отличается от классической системы DLP

Технологическую концепцию построения MDLP сформулировал Джо Стюарт, директор по исследованиям вредоносных программ компании SecureWorks. Он считает, что от утечек, вызванных троянскими программами, можно защититься многоуровневой обороной, которая состоит из системы управления обновлениями, антивируса, межсетевого экрана, URL-фильтра, системы предотвращения вторжений (Intrusion Prevention System, IPS) и HIPS, а также системы контроля приложений. Пикантность ситуации в том, что именно такую систему защиты требует построить ФСТЭК для защиты персональных данных от утечек. И чиновников часто обвиняли в том, что их система защиты не контролирует собственно содержание открытых каналов, по которым данные также могут утечь. Впрочем, похожесть методов, скорее всего, связана с одинаковой моделью угроз: и ФСТЭК, и идеологи MDLP рассматривают в основном угрозы со стороны внешних нарушителей, а классические DLP защищают от внутренних угроз.

Следует отметить, что стек перечисленных Стюартом технологий уже реализован во многих продуктах класса Internet Security, это антивирусный комбайн, включающий в себя самые различные защитные механизмы. Фактически это означает, что антивирусные продукты уже сейчас готовы взять на себя роль MDLP: все компоненты для этого уже есть, однако нужно, чтобы разработчики антивирусного программного обеспечения могли с помощью своих продуктов блокировать скрытые каналы утечек, организованных троянцами. «Лаборатория Касперского» уже создала в Новосибирске лабораторию защиты информации от внутренних угроз, и в ней, похоже, работают над решением указанной задачи. Важно только понимать, что MDLP является не противопоставлением классическому варианту DLP, а его продолжением. Лишь комплексное решение позволит защититься от утечек различных типов.