ЗАЩИТА ПРЕДПРИЯТИЯ ОТ УТЕЧКИ ИНФОРМАЦИИ И ВНУТРЕННИХ УГРОЗ ПУТЁМ ВНЕДРЕНИЯ DLP-СИСТЕМ

Шустов А. Ю.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Мельниченко Д. А. – к. т. н, доц.

По данным международного исследования компании EY в области информационной безопасности и компании InfoWatch, в организациях различных сфер бизнеса количество внутренних атак превышает количество внешних. Собственные сотрудники оказываются серьёзной угрозой и способны нанести огромный ущерб вследствие кражи корпоративной информации или её утечки по неосторожности, а также коррупции, мошенничества, сговоров, воровства и саботажа. В условиях жесткой конкурентной обстановки особенно актуальной является задача по сохранению конфиденциальности данных и минимизации рисков внутренних угроз ИБ (информационной безопасности), или, иными словами, по защите корпоративной информации от инсайдеров.

DLP (англ. Data Leak Prevention) – технологии, а также технические устройства (программные или программно-аппаратные) для предотвращения утечек информации. DLP-продукты – самостоятельная, быстроразвивающаяся отрасль информационной безопасности.

Кроме непосредственной задачи обнаружения и блокировки утечек DLP позволяет решать множество задач: заблаговременно выявлять нелояльных сотрудников и потенциально опасные каналы коммуникаций, вести архив корпоративной электронной почты, распечатываемых документов и других данных. Также DLP используется для приведения системы внутреннего контроля в соответствии с требованиями законов «Об информации, информатизации и защите информации», «О регистре населения», PCI DSS, SOX, других отраслевых стандартов и нормативно-правовых актов, а также для повышения привлекательности организации в глазах клиентов, партнёров, инвесторов и СМИ.

Не меньшее значение, чем функциональность ядра, имеют уровни контроля, на которых работает DLP-система. Их два:

- уровень сети, когда контролируется сетевой трафик в информационной системе;

- уровень хоста, когда контролируется информация на рабочих станциях.

Применение DLP в Беларуси пока ограничивается, зачастую, контролем внешних USB-носителей и принтеров. Только сравнительно немногие организации строят полноценный «защитный контур», перекрывающий все потенциальные каналы утечки конфиденциальной информации.

Несмотря на то, что белорусское законодательство содержит в себе нормы, позволяющие наказывать распространителей корпоративных секретов, подавляющее большинство организаций, использующих DLP-системы, предпочитают ограничиваться внутренними разбирательствами и дисциплинарными взысканиями, в крайнем случае увольняя провинившихся в особо крупных размерах сотрудников.

Список использованных источников:

1. InfoWatch / Сайт группы компаний-разработчиков программных продуктов и решений для обеспечения информационной безопасности организаций, противодействия внешним и внутренним угрозам [Электронный ресурс] – Режим доступа: http://www.infowatch.ru
2. ИТ-защита / Сайт-проект «ИТ-защита» [Электронный ресурс] – Режим доступа: http://itzashita.ru.
3. Компьютерные вести / Обзор DLP-систем [Электронный ресурс] – Режим доступа: http://www.kv.by/content/obzor-dlp-sistem.