

Как песок сквозь пальцы

MskIT.ru, 31.10.11

28 октября 2011 года в Москве прошла IV Международная конференция DLP-Russia, посвященная вопросам контроля информационных потоков и защиты конфиденциальной информации от внутренних угроз. Конференция проводится по инициативе Совета «DLP-Эксперт» с 2008 года.

IV МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ

DLP-Russia

Protect your inner space

людям; NHS потеряли ноутбук, содержащий 8 млн 300 тыс. записей, большая часть которых принадлежала онкологическим больным. Месяцем ранее двое бывших сотрудников сотового оператора T-Mobile совершили кражу персональных данных клиентов компании; в Гонконге публично были обвинены четыре банка в несанкционированной передаче персональных данных и так далее.

Анализ показывает, что персональные данные – самый уязвимый вид данных, именно он составляет 90% утечек всех данных. Генеральный директор InfoWatch Наталья Касперская уточнила, что утечки практически равномерно распределяются по различным каналам. Для DLP-вендоров это означает, что защищать надо все каналы, что, несомненно, сложнее. То есть, уже невозможно сегодня «закрыть» что-то одно и на этом успокоиться.

Совет «DLP-Эксперт» констатирует, что на рынке сегодня, на первый взгляд, существует достаточно разнообразных решений, относимых к классу DLP. Но в реальности, большинство из них решает лишь отдельные проблемы, перекрывая максимум 1-2 канала утечки информации из корпоративной сети. Это означает, что отсутствует комплексный подход к решению данной проблемы.

Больше всего информации «утекает» из больших корпораций – 47,7%, из них 30% - намеренно, в государственных учреждениях утечек меньше – 18,9%, из них намеренно – 6,10%. В образовательных учреждениях утечки составляют 30,4% (намеренных – порядка 11%). Стоимость потерь компаний от утечек год от года растет.

Одна из серьезных проблем защиты, по словам Натальи Касперской, то, что в основной своей массе информация неструктурированная. В хорошо развитых крупных компаниях структурированная информация составляет не более 20%. При этом 10% информации изменяется ежедневно, 10% - создается заново. Однако обилие неструктурированной информации – не единственная проблема.

В DLP-решениях лишь 20-30% занимает собственно программное обеспечение. Остальное – это совместная работа вендора или партнера с заказчиком. «Но клиенты, как показывает практика, сами делать ничего не хотят», - отмечает Наталья Касперская. Между тем, лишь клиент может оценить

Согласно данным, собранным из открытых источников, в первом полугодии текущего года в мире было выявлено 560 утечек конфиденциальных данных. Для сравнения: за весь 2010 год – 794 утечки. Вот только некоторые, сообщения о которых приведены на сайте DLP-Эксперт: в июле личные данные около 60 300 клиентов компании Telstra (Австралия) были отправлены посторонним



степень важности информации, и в зависимости от этого выбрать способ защиты. Компании как будто в растерянности – не знают, по какой дороге двигаться.

Что касается рынка DLP, то за 2011 год рост его замедлился, выросло количество игроков (многие из них питают иллюзию, что DLP – это легко). Наметился сильный крен в сторону предприятий СМБ, в континентальной Европе появился интерес к такого рода системам. Углубилось противоречие: клиенты хотят, чтобы решение стоило дешево, внедрялось быстро, и было надежно, но такое невозможно.

«Рынок DLP сейчас переживает кризис доверия со стороны клиентов», - сказала Наталья Касперская. Технологии перехвата и мониторинг не дают гарантию полной защиты. Рост неструктурированных данных, возникновение новых каналов утечек требуют новых технологий, но при слабой заинтересованности рынка такие технологии не возникают.

Но как бы то ни было, отрасль DLP развивается по следующим направлениям: ведется работа над расширением функциональности продуктов, расширяются сферы влияния DLP, происходит развитие DLP-технологий в другие области. В частности, **InfoWatch** в своих решениях увеличивает число перехватчиков, усложняет технологии перехвата, проводится усложнение политик и интеграция с другими технологиями.



Эрик Домаж, менеджер по исследованиям и консалтингу в области информационной безопасности в Западной Европе, IDC EMEA Software Group

Эрик Домаж, менеджер по исследованиям и консалтингу в области информационной безопасности в Западной Европе, IDC EMEA Software Group, отметил, что развитие мобильного Интернета привело к практически полной потере контроля над действиями пользователя. Человек сам выбирает себе мобильное устройство и подключается к Сети в любой точке города, страны и мира. Собственно

поэтому DLP должно присутствовать везде. Однако повсеместному распространению систем перехвата могут препятствовать местные законы. Действовать, не нарушая эти законы – одна из непростых задач, решаемых в ходе DLP-проектов. При этом все равно нужно учитывать, что хакеры обойдут любой закон.


Среди современных проблем защиты информации Эрик Домаж назвал разнородность сетей, бурное развитие сетей социальных. «Основная сложность заключается именно в сложности сетей, поэтому нужно идти от технологии к управлению», - отметил он.

Также существует проблема «больших данных». К 2020 году прогнозируется, что в мире будет создано 35 ZB данных, основная часть которых, как мы уже сказали выше, неструктурированные данные. Чтобы по возможности обеспечить безопасность информации, всем компаниям и организациям следует регулярно анализировать, какая информация нуждается в защите, и в защите какой степени. Это нужно для оптимизации затрат на безопасность. Постепенно в мир приходит Cloud computing. Сегодня уже имеется технология шифрования в «облаке», некоторые операторы предлагают DLP как сервис.

Эрик Домаж подчеркнул, что система безопасности – это много составляющих, а также – это не нечто решенное раз и навсегда, это постоянный процесс.

Владимир Денежкин, генеральный директор ООО «Трафика», напомнил участникам конференции законодательные нормы, которыми следует руководствоваться при использовании





средств DLP. Об организации защиты данных рассказали представители Банка Москвы, банка «Возрождение», а также представители компаний МТС, «ВымпелКом» и других. Специалисты компаний-разработчиков средств защиты представили на конференции свои решения.

Оригинал публикации: <http://www.mskit.ru/news/n108417/>