

Чтобы облака не протекали

Computerworld Россия, Валерий Коржов, 10.11.2011

На конференции DLP-Russia обсуждали перспективы рынка средств защиты от утечки данных

IV МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ

DLP-Russia

Protect your inner space

Характеризуя современное состояние рынка средств защиты от утечки данных (Data Leak Protection) на состоявшейся 28 октября четвертой ежегодной конференции DLP-Russia, Эрик Домаж, менеджер IDC в области информационной безопасности по Западной Европе, отметил, что в связи с размыванием

границ организации возникают проблемы с классическими сенсорами для перехвата информации.

«За одним пользователем может быть закреплено несколько устройств, каждое со своим собственным IP-адресом, — отмечает Домаж. — Поэтому простой контроль потока сообщений по IP не всегда позволяет установить пользователя, который передает данные. Это затрудняет составление правил фильтрации». Такое «размывание» происходит не только с идентификацией, но и с периметром сети: не всегда по IP-адресу получателя можно отличить, куда направляется пакет — наружу или внутрь сети.

Российский рынок DLP, по данным портала Anti-malware.ru, составляет 15 млн долл. в год в ценах для конечных заказчиков. Защитой от утечек интересуется все больше компаний, в том числе и из сегмента SMB. Для них необходимо упростить архитектуру защиты и удешевить само решение. Сейчас же, по данным Домажа, на 1 долл. лицензии на ПО требуется 7 долл. на внедрение. Всем без исключения компаниям требуется защитить персональные данные своих сотрудников и финансовую информацию, в остальном «набор секретов» зависит от отрасли, и, возможно, для каждой из них стоило бы выпустить свой типовой пакет защиты от утечек, но пока производители этого не сделали.

Технологии DLP развиваются в основном экстенсивно — добавлением новых каналов перехвата сообщений и контролируемых протоколов.



«Я в последнее время не видела ни одной принципиально новой технологии защиты», — отметила Наталья Касперская, генеральный директор одного из ведущих разработчиков таких систем, компании InfoWatch. Однако простым увеличением количества «перехватчиков» уже не обойтись. Как указал Домаж, основной проблемой является не сам по себе объем потоков данных, а значительное увеличение типов критически важных данных, которые средства DLP должны защитить. Между тем существующие технологии устроены так, чтобы защищать не очень большой объем строго определенной информации. По данным InfoWatch, более 90% утечек в настоящее время связано с персональными данными — именно их и нужно защищать в первую очередь, но объем их может

оказаться достаточно велик.

Остроту проблемы защиты от утечек критически важных данных резко обостряют облачные вычисления и распространением модели предоставления программ и платформ в качестве сервиса. Основным активом, который нужно защищать при использовании облачных технологий, являются именно данные. «DLP в облаках — это наше будущее, — считает Домаж. — Средства защиты от утечки данных должны стать частью облака». Впрочем, пока же, как он утверждает, вопреки распространенному мнению, клиентов интересует не безопасность, а лишь стоимость облачных сервисов.



С одной стороны, DLP контролирует коммуникации компании с внешним миром, и здесь облачные технологии вполне уместны. Но с другой — компании не будут безоговорочно доверять облачным провайдерам защиту собственных секретов, дескать, что охраняешь, то и имеешь. Поэтому компании хотели бы рассчитывать на то, что в облачной среде уже есть встроенное DLP-решение, которое и будет контролировать утечку критических для них данных. Для того чтобы рынок облачных сервисов состоялся, нужно убедить клиентов, что это для них безопасно, для этого и может пригодиться инструментарий DLP.

Производители стараются реализовать в своих продуктах возможность не только контролировать потоки информации, но и блокировать утечки. «Клиенты часто требуют возможности перехватывать сообщения, — объясняет Касперская, — однако используют эту возможность очень редко: по нашим оценкам, всего в 5% случаев». Проблема в том, что перехват сообщений требует компьютерных ресурсов и дополнительных расходов на покупку лицензий. Скорее всего, эта функциональность в дальнейшем развиваться не будет.

Оригинал публикации: <http://www.osp.ru/news/articles/2011/11/13011308/>