INFOWATCH®
BECAUSE YOUR DATA IS YOUR BUSINESS

т./ф.: (+7 495) 22-900-22

Россия, 123022, Москва
2-ая Звенигородская ул., д. 13, стр. 41

www.infowatch.ru

DLP. В точке перегиба

Татьяна Белей, директор по маркетингу InfoWatch, Anti-Malware.ru, 9.11.11

Тема защиты информации от утечек с помощью специализированных решений (класса DLP - Data Leakage Prevention) давно не воспринимается как откровение. Системы DLP существуют не первый год, проблема инсайда, иных внутренних угроз с завидной периодичностью дискутируется на профильных ИБ-конференциях, встречах отраслевых «безопасников». Но сам рынок DLP, цитируя классика, страшно далек от стабильности и предсказуемости. В этом могли убедиться участники IV конференции DLP-Russia. Наиболее точно ситуацию описала Наталья Касперская, генеральный директор **InfoWatch**. Рынок DLP переживает кризис доверия: инфраструктура заказчиков усложняется, объем корпоративной информации растет по экспоненте, требуются все более совершенные технологии перехвата... но платить за это клиент не готов. Разработчики серьезных DLP-систем предлагают клиенту сложные решения с длительным циклом внедрения, клиент же наоборот стремится «закрыть» проблему с минимальными потерями. Акционеры и высшее руководство компаний не видят смысла во внедрении дорогостоящего продукта без стопроцентной гарантии защиты внутренней информации. Здесь, по выражению Алексея Лукацкого, менеджера по развитию бизнеса Cisco, не работают ни «страшилки» об утечках данных в компаниях различных отраслей, ни юридические риски как следствие невыполнения требований российских законодательных актов. Бизнес понимает только один язык - финансовый, и только тогда, когда цепочка событий «инцидент - прямые убытки» укладывается в простую логическую схему «причина - следствие». Евгений Климов, вице-президент ассоциации профессионалов в области информационной безопасности RISSPA подчеркивает: до сих пор среди руководителей бизнеса преобладает мнение, что в компании защищать нужно все, без классификации информации и расчета эффективности средств защиты. С другой стороны, заказчик редко задается вопросом, что будет, если корпоративные секреты станут общедоступными. Парадоксально, но факт: бизнес не представляет последствий утечек, а ИБ-подразделение в большинстве случаев не может определиться с тем, что именно нужно защищать. 80% корпоративной информации не структурировано, нет ясного представления о том, что называть конфиденциальной информацией, нет внятных методик для определения реальной ценности информации... Но в этом, по мнению экспертов, один из возможных источников роста рынка. Ответив на вопрос, сколько стоит информация и как правильно построить ее защиту, вендор DLP превращается из разработчика софта в поставщика экспертизы, лучших практик в организации процессов жизненного цикла информации. Не случайно именно сейчас, когда рост DLP-рынка ощутимо замедлился, тема организационных аспектов защиты информации вышла на первый план. Бизнес, как мы уже отмечали, не мыслит в терминах угроз, конфиденциальности, целостности или доступности информации, если за этими терминами не стоят реальные суммы финансовых потерь. Но стоит объяснить, что DLP-система - это, кроме всего прочего, инструмент для проведения расследований внутренних утечек, сбора доказательной базы с целью дальнейшего привлечения злоумышленников к ответственности, то ситуация предстает в ином свете. На это обратил внимание участников конференции Петр Стельмах, руководитель направления информационной безопасности компании «Антивирусные решения». Подход к внедрению систем противодействия утечкам корпоративной информации сродни проекту внедрения ERP, и факторы успеха сходны до неразличимости. Александр Малявкин, руководитель отдела консалтинга компании **Leta**, прямо заявил - без поддержки руководства компании-заказчика, понимания, что DLP-проект - это надолго, деятельного участия всех бизнес-подразделений заказчика и классификации информации никакая система защиты не заработает. Одна из причин - внедрение DLP предполагает автоматизацию процессов, которые, зачастую, у заказчика лишь прописаны на бумаге, но в реальной жизни не выполняются -

INFOWATCH®
BECAUSE YOUR DATA
IS YOUR BUSINESS

т./ф.: (+7 495) 22-900-22

Россия, 123022, Москва
2-ая Звенигородская ул., д. 13, стр. 41

www.infowatch.ru

еще одна отсылка к ERP. Заказчик ждет от разработчиков и внедренцев DLP-решений реальной помощи, необходима методология определения стоимости информационных активов, методики оценки рисков, масштабируемые практики применения ИБ-решений. Одним словом, заказчику DLP нужен качественный ИБ-консалтинг. Не исключаю, что именно консалтинг в области организационных мер защиты информации поможет сблизить позиции вендора и заказчика. По крайней мере, мы услышали этот сигнал от рынка. Сложно сказать, пойдет ли компания по пути аккумулирования компетенций и передачи лучших практик заказчикам напрямую, по примеру крупных вендоров ERP, или же изберет стратегию взаимодействия с партнерами. Но то, что рынку DLP для дальнейшего развития не хватает авторитетного источника не технической, а организационной, методологической экспертизы, для меня совершенно очевидно.

Оригинал публикации: http://www.anti-malware.ru/node/4891