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

Наталья Касперская: DLP –больше, чем защита от утечек

17/09/2012, Cnews
Василий Прозоровский

В ожидании очередной, пятой по счету отраслевой конференции DLP-Russia, CNews беседует с Натальей Касперской, руководителем InfoWatch. Компания Натальи стояла у истоков направления DLP (защита от утечек информации) в России. Потому мы не могли не поинтересоваться ее видением перспектив рынка DLP в нашей стране и за рубежом. Что такое настоящее DLP-решение и почему их выделили из массива информационной безопасности? Как продавать защиту от утечек и почему она стоит своих денег?

CNews: Что сейчас происходит на рынке DLP? Какие можно выделить тенденции?

Наталья Касперская: Рынок DLP образовался недавно. Всего 6 лет назад IDC выделило его в отдельную категорию. Но до сих пор на рынке нет единого мнения, что такое DLP. Под DLP многие клиенты и производители решений иногда понимают то, что DLP не является – скажем, систему защиты и блокировки портов. Есть устойчивое мнение, что DLP – это только софт, что тоже в корне неверно. DLP – это целый комплекс организационных и технических мер. Не случайно наиболее дальновидные производители DLP стремятся выйти за рамки систем защиты от утечек в смежные области, нарастить функционал. На мой взгляд, это одна из наиболее заметных тенденций.

CNews: Чем сейчас живет компания в контексте рынка? Какие последние достижения?

Наталья Касперская: Мы диверсифицировали свой бизнес. В 2010 году InfoWatch вместе с компанией "Ашманов и партнеры" создала дочернее предприятие "Крибрум", разрабатывающее сервис для мониторинга и анализа репутации компаний, брендов, персон в интернет-пространстве. В 2011 с приобретением немецкой компании cynapspro GmbH (позднее преобразована в EgoSecure), которая разрабатывает продукты в области Endpoint protection, InfoWatch превратилась в холдинг. Кроме того, компания вложилась в стартап по разработке программного обеспечения для контроля приложений. Развиваем несколько новых проектов в области ИБ.

Наталья Касперская: Наиболее дальновидные производители DLP стремятся выйти за рамки систем защиты от утечек в смежные области

Что касается продуктов, InfoWatch занимается модернизацией своего флагманского DLP продукта InfoWatch Traffic Monitor. Мы движемся в сторону развития функциональности с одной стороны, и большей гибкости системы с другой. Первое – это ответ на все возрастающие требования заказчиков к продукту – организации хотят контролировать информационные потоки максимально полно, включая "экзотику" - шифрованный Skype, оборот отсканированных копий документов и пр. Второе, то есть большая гибкость – задел на будущее. Это возможность быстрой интеграции с другими решениями и технологиями, не обязательно "защитными".

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

CNews: Может ли современное предприятие обойтись без DLP-систем? Что в таком случае будет происходить с конфиденциальной информацией компании?

Наталья Касперская: Любая крупная организация без DLP обойтись не может. Ценность информации постоянно растет, а ее структурированность, наоборот, понижается. На сегодняшний день в России налицо весьма плачевная ситуация с защитой информации, ежегодно регистрируется огромное число утечек конфиденциальных данных. Сведения о гражданах свободно циркулируют в соцсетях. Потащив за одну ниточку, о человеке можно узнать все.

Если предприятие никак не защищает конфиденциальную информацию, персональные данные собственных сотрудников и клиентов, если нет понимания, что именно конфиденциально, а что нет, с большой вероятностью это приведет как минимум к постоянной утечке ценных информационных активов компании. А как максимум, к взысканиям со стороны регулирующих органов, денежным и репутационным потерям.

CNews: Как у вас построена работа с заказчиком?

Наталья Касперская: Поначалу мы, подобно нашим конкурентам, рассматривали DLP как программный продукт. Но жизнь внесла коррективы, оказалось, что невозможно продавать DLP-решения как пирожки. DLP-проект – дело сложное, это очень много консалтинга, совместной работы с заказчиком, и совсем чуть-чуть собственно внедрения, адаптации системы под инфраструктуру конкретной компании.

Постепенно сложилась концепция трех стадий взаимодействия с клиентом в DLP-проекте: pre-DLP, DLP и post-DLP. На первом этапе команда вендора, интегратора и заказчика совместно разбираются с объектами защиты, выясняют, какую именно конфиденциальную информацию мы будем отслеживать в компании. Это во многом консалтинговая работа, хотя мы даже создали автоматический инструмент для помощи компании в категоризации информации. Он позволяет в полуавтоматическом режиме разнести информацию по категориям. В дальнейшем, при анализе исходящего трафика, система определяет, к какой категории или категориям относится исходящий документ, сопоставляет его с уже имеющимися образцами (сравниваются векторы документов, построенные в многомерном пространстве. Измерения этого пространства - термины). Если вектор нашего документа близок к вектору эталонного конфиденциального документа, система сообщает об этом или блокирует отправку (в зависимости от настроек). В общем, сложная гибридная лингвистика в действии. Так вот на этапе pre-DLP важно подготовить такую классификацию, чтобы у системы в процессе работы не возникало ни сомнений, ни ложных срабатываний.

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

Наталья Касперская: DLP-проект – дело сложное, это очень много консалтинга, совместной работы с заказчиком, и совсем чуть-чуть собственно внедрения, адаптации системы под инфраструктуру конкретной компании

Далее мы с совершенно спокойной душой приходим к DLP-стадии, собственно к внедрению. Внедрение – это простая часть, обычно она занимает от одного до нескольких дней. По сути это просто развертывание софта на всю компанию. Если там сложная, большая разветвленная инфраструктура, это будет подольше.

Стадия post-DLP предполагает работу с системой, когда инцидент уже произошел. Наша система одна из немногих архивирующих весь объем исходящего трафика. Причем не скидывает все в кучу, а аккуратно раскладывает по полкам. Данный компонент называется Forensic Storage. В итоге в любое время можно достать из системы все логи, документы, выяснить, кто и что отправил. При соблюдении в компании ряда процедур данные системы могут использоваться в качестве доказательства в суде (в случае преследования нарушителя за несоблюдение режима коммерческой тайны, например).

CNews: Кто ваши основные заказчики?

Наталья Касперская:Защита от утечек – довольно непростая тема. Учитывая сложность внедрения DLP, а также дороговизну, компании долго решают, нужно ли им подобное. И покупают лишь тогда, когда точно знают, зачем им эта система.

Среди наших клиентов много представителей нефтегазового сектора, потому что их основные активы — информация о месторождениях и людях. Специалистов мало, и они боятся их потерять. Второй по размеру сегмент — это банковский сектор. У них много требований со стороны регуляторов, на них давит ЦБ со своими инструкциями, закон о защите персональных данных, они практически все под него попадают. Третья категория – компании телекоммуникационного сектора. Они просто обязаны иметь систему защиты от утечек, в том числе и персональных данных абонентов.

Наталья Касперская: В России плачевная ситуация с защитой информации, ежегодно регистрируется огромное число утечек конфиденциальных данных

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

Есть еще производители товаров, им надо защищать схемы, графики, инструкции, описание технологий, то есть то, из чего состоит ноу-хау. Но там только DLP в его нынешнем виде недостаточно, нужна интеграция технологий, и мы даже выделяем это в отдельный сегмент. В частности, нужно распознавать изображения, потому что документы могут быть очень объемными, и отследить их только с помощью лингвистики невозможно.

CNews: Вы назвали 4 больших категории, вместе с тем на витрине у вас лежит, образно говоря, один товар. Не было идей сделать отраслевые варианты?

Наталья Касперская:Они у нас есть. Например, решение для банковского сектора. Основное отличие - библиотека фильтрации контента, по-другому "онтология". Это список категорий, который может быть в компании. На основе этих категорий работает лингвистический анализатор.

У банков есть предписания ЦБ, PCI DSS, Basel. Некоторые попадают под европейских регуляторов. Соответственно, у нас в продукте сделаны специальные опции, которые позволяют компании соответствовать этим параметрам.

Вообще мы выделяем 13 вертикалей, соответственно – 13 кастомизированных решений, но на особом счету решения для компаний-производителей. Как я уже сказала, любой производитель уникального продукта, помимо прочего, как никто заинтересован в защите своей интеллектуальной собственности, секретов производства. Но есть сложность, поскольку производственные компании могут принадлежать к совершенно разным отраслям. Потому и "онтологии" должны быть разными. У производителей самолетов одни термины, у производителей штанов – другие, танков – третьи. Но тем интереснее…

Оригинал публикации: http://safe.cnews.ru/reviews/index.shtml?2012/09/17/503241_2