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

Интервью с Константином Левиным, директором по продажам InfoWatch

Anti-Malware.ru, Александр Панасенко, 21.12.2011

На вопросы Anti-Malware.ru любезно согласился ответить Константин Левин, директор по продажам компании InfoWatch. Это интервью продолжает цикл публикаций "Индустрия в лицах".

- На прошедшей недавно конференции DLP-Russia 2011 было много разговоров о поиске новых трактовок аббревиатуры DLP. Что Вы вкладываете в это понятие?

- Есть теоретический подход – то, как понимают DLP западные аналитики (IDC, Gartner и пр.), и есть подход, который работает на практике. В терминах теоретиков DLP – это защита информации при перемещении, использовании, хранении – in motion, in use, at rest. Я же понимаю под DLP нечто иное. Есть конфиденциальная информация, по идее, в каждой компании она должна классифицироваться, кое-где есть даже списки КИ, но процесс классификации часто носит декоративный характер. Корпоративная политика ИБ не пересекается с теми документами, которые нужно защищать. Информационную безопасность рассматривают как защиту инфраструктуры, но не данных.

Константин Левин

Окончил МИРЭА в 2005 году. Работу в компании **InfoWatch** начал в 2007 году в должности продавца.

Имеет обширный опыт в сфере консалтинга, PR и маркетинга. Лично участвовал в сделках с крупнейшими клиентами **InfoWatch**, такими как РусГидро, Банк Москвы, Райффайзенбанк, Банк Возрождение, РосЕвроБанк, ВТБ и другими. С 2010 года является руководителем отдела продаж.

Поэтому первое, что мы делаем, когда приходим к клиенту – пытаемся определить, какую информацию будем защищать. Мы помогаем определить, какие категории данных для него критичны. По опыту проектов 60-70% информации нельзя назвать уникальной – форматы повторяются в рамках отдельных вертикалей, отраслей. Возьмем любую ИТ-компанию – кроме ноу-хау, методик, базы клиентов у нее есть бухгалтерские документы, договоры – это одинаковые, условно говоря, данные. Здесь основа для типизации вертикалей, отраслевой специфики. Логично, что под каждую вертикаль можно создать некий перечень, универсальную классификацию, свой словарь ключевых слов, базу контентной фильтрации. Оставшиеся 30% - специфика конкретной организации.

Проводя на начальном этапе проекта аудит данных компании-заказчика, мы в автоматическом режиме сортируем по категориям типовой слой данных, уникальная информация категоризируется вручную, а далее остается лишь привязать к отдельным категориям владельцев информации. Дальше включается проактивный компонент системы – он работает с сырыми данными, входящей информацией. Организуется хранение, интеграция с бизнес-приложениями, настраивается система управления, проверяются правила и политики. Собственно, все – DLP готова. Если формализовать все сказанное, DLP – это автоматизированная система контроля движения категоризированной информации в рамках модели угроз компании.

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

- В бизнес-среде есть устойчивое представление, что защищать нужно всю информацию компании. Есть ли универсальный рецепт от практика – желательно в процентах – что нужно защищать, а что нет?

- Все идет от бизнеса. Прикладная ИБ всегда идет от модели угроз, где расписаны бизнес-процессы, документы в разрезе бизнес-процессов и владельцев. К примеру, доля конфиденциальной информации в крупной компании может составлять 1 процентов, но есть клиринговые центры, процессинг, коллекторские компании – там доля чувствительной информации стремится к 90%.

- А для вертикалей? Например, для банков?

- Нет универсального рецепта и не будет – банки разные…

- Но модель угроз для тех же банков может быть типовой…

Если мы говорим о СТО БР, банки обычно адаптируют типовую модель под себя, появляется некий набор категорий информации. Наверное, можно говорить о 60-70% - такова в среднем доля «непубличной» информации в банке, но это все, повторюсь, условно.

- Тем не менее, есть типовые модели, типовая информация – возможна ли типовая DLP?

- DLP из коробки, так, чтоб все работало, да еще и стоило недорого – тема точно не для крупных компаний. Реализовать такое для СМБ мешает специфика процессов каждой компании – если перестроить все процессы под коробку, что останется от конкурентных преимуществ компаний?

- Если не коробка, почему не типовое внедрение?

- Уже есть. Устав проекта, описания, схемы внедрения - это такие стандартные вещи. В общем, методология понятна, типовой проект внедрения существует. Правда, в каждом случае нашим партнерам приходится «натягивать» типовую схему на организацию – а там, допустим, не четыре исходящих потока, а пять. Не было еще на моей памяти двух проектов, которые были бы похожи. Типовой проект хорош в плане взаимодействия внедренца и заказчика, у нас все прописано – как идет проект, как оказываем техподдержку, типовые документы… Доходит до анекдотов – заказчики просят наших западных конкурентов работать по нашей модели внедрения, поскольку им она понятна, удобна. Есть ряд проектов, где мы стоим параллельно с другими системами, и западные коллеги учатся работать на российском рынке, используя нашу методологию.

- Хорошо ли это – отсутствие стандартизации? Отрасль меняется стремительно – новые каналы, облачные сервисы.. Те же мобильные устройства – никто до сих пор не знает, как их контролировать.

- Знают, просто никто это пока не сделал.

- И тем не менее… Возможно, такая нестабильность в DLP и связана с появлением все новых и новых технологий? Те же каналы утечки – можно ли сегодня выделить какие-то главные, наиболее важные каналы, которые нужно контролировать в обязательном порядке?

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

- Относительно новых каналов - так будет всегда, и, слава Богу, мы успеваем идти в ногу со временем и адаптировать наш продукт к изменениям инфраструктуры. К тому же старые технологии также меняют протоколы взаимодействия. Когда мы разрабатывали снифер для почты, понятия SSL не применялось в принципе. Адаптировали. Появились ICAP, P2P и так далее, и это хорошо – значит, бизнес не закончится никогда. Рынок насыщается, потолок близко, но в итоге победит тот, кто накопил больше опыта, имеет экспертизу. Наш продукт стоит во множестве компаний – всевозможные сетевые конфигурации, гетерогенные среды, мы выдерживаем самый высокий уровень техподдержки по ИБ - решение проблем в течение двух часов это серьезный показатель. Плюс методологическая подложка - и в рамках законодательства, и в рамках технологий. Мы не просто даем безопаснику инструмент – мы даем конкретную инструкцию, через бизнес-задачи объясняем, как и что нужно делать офицеру по безопасности, администратору, владельцу информации.

Что касается приоритета каналов – утечки действительно распределяются почти равномерно, но наиболее важными были и остаются почта, интернет, съемные носители, печать – это 20% затрат и 80% эффекта. Почти все остальное можно «зарезать» организационными мерами. ICQ, Skype, P2P, FTP режутся на уровне прокси-серверов и сетевых экранов. Крайне редко тот же FTP действительно является протоколом взаимодействия – у нас лишь один клиент, где 4 тыс. сотрудников используют FTP. Я к тому, что ради одного-двух человек поднимать защиту FTP экономически невыгодно, проще просто запретить организационно.

- На уровень выше – как правильно обосновать внедрение для бизнеса? Эффективность самой системы DLP, возврат инвестиций можно посчитать – по предотвращенному ущербу, например, а вот если внедрения еще не было, как тогда?

- Действительно, лучше всего работают пилотные внедрения, когда владелец информации воочию убеждается, сколько и какой информации уходит из компании. И главное – может сам оценить, сколько же это стоит в случае успешной утечки, каков ущерб. Тут и непреднамеренные утечки, и инсайд… А вот до внедрения… На уровне здравого смысла – есть владельцы информации, у них есть задачи, KPI. Ведь наши функциональные заказчики – это не только гендиректора, но и руководители продаж, HR, R&D.

Скажем, для HR удержание работника – KPI. Был случай, когда Traffic Monitor отреагировал на передачу персональных данных и отследил письмо с резюме работника одной нефтяной компании в адрес компании-конкурента. А у них специалисты на вес золота. Вовремя сделанный контрофер позволил удержать работника. Для компании экономия – не нужно тратиться на обучение и адаптацию нового сотрудника, для HR – выполнение KPI. В продажах еще проще – если у меня сидит инсайдер и сливает информацию конкурентам, страдает не только компания, но и я лично. Ведь это мое подразделение. Все это легко перевести на язык рисков. То или иное негативное событие – потерянные деньги. А про деньги бизнес очень хорошо понимает.

- А может система приносить прибыль?

- Как посмотреть. Если оценивать сэкономленное, сохраненное как заработанное. Но корректнее так – сэкономленные активы – первый шаг к прибыли.

- Наверное, Вы уже устали от вопросов про дыры в системе. И все же, – подготовленный инсайдер обойдет DLP?

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

- Система DLP снижает риски. Так же, как организационные меры, нормативка, физическая безопасность. Все вкупе дает эффект. Подготовленный инсайдер вынесет информацию - факт, но давай смотреть глубже – доказано, что тренированный человек может запомнить 20-30 экранов, есть камеры мобильных телефонов, не везде контролируют печать. Но если утечка идет по каналу связи – почта, интернет – в DLP-системе останутся следы. Как доказать вину сотрудника, собрать доказательную базу и открыть дело – история другая, для этого специализированные организации существуют. DLP же, повторюсь – это снижение рисков, ни в коем случае не панацея, не волшебная таблетка.

*- Куда пойдет **InfoWatch** в обозримом будущем? Если не коробочный DLP, то что?*

- Анализ рисков, качественные эндпойнты… те же мобильные устройства – есть решение, но оно имеет ряд ограничений… Кроме того, DLP система давно рассматривается не как отдельное решение, но как часть ИБ –системы, Traffic Monitor поставляет данные в ситуационные центры компаний в виде событий или показателя уровня безопасности, на данных DLP работает многофакторный анализ. Скажем, документ пошел на печать, а пользователь, отправивший его на принтер, по данным системы физической безопасности сегодня даже на работу не пришел. Это сразу сигнал офицеру безопасности, сразу расследование. Пока мы не рассматриваем системы корреляции событий как отдельное направление R&D, но в рамках проектов в банках и операторах связи, например, мы активно интегрируемся с такими системами.

- Облачная DLP?

А облако можно реализовать уже сейчас, есть даже готовый кейс, когда профильтрованный трафик приходит к заказчику от его же «дочки» – поставщика ИТ и ИБ услуг. У заказчика распределенная структура, у «дочки» тоже, наружу заказчик выходит только через инфраструктуру «дочек». Внутри – те же эндпойнты. То же делают многие интеграторы, фильтруя трафик для небольших компаний. Вообще же безопасность как сервис – тема следующих интервью.

Оригинал публикации: http://www.anti-malware.ru/node/5069