SOLAR SECURITY

ИБ на результат

От теории к практике применения DLP

Анна Попова
Руководитель департамента анализа активности пользователей (DLP)
Infosecurity a Softline Company

МОСКВА, 2018

INFOSECURITY

Компания Infosecurity специализируется на выполнении комплексных проектов в информационной безопасности с 2010 года. За эти годы нашими клиентами стали представители ТОП-5 компаний различных отраслей экономики:

- Банковский сектор (ПАО Банк «ФК Открытие», ПАО Банк «ТРАСТ», ПАО «РГС Банк»);
- Инвестиционный бизнес (АО «Открытие Брокер», SOVA CAPITAL LIMITED);
- Страховой бизнес (СК Росгосстрах, АО «СК Опора»);
- Негосударственные Пенсионные Фонды (НПФ «ЛУКОЙЛ-ГАРАНТ», АО «НПФ электроэнергетики»);
- Промышленность (АО Архангельскгеолдобыча, SEGEZHA GROUP).

Ключевые сервисы «Инфосекьюрити» — реагирование на инциденты информационной безопасности (Security Operations Center), предотвращение утечки данных, защита от угроз нулевого дня, поддержка IT-инфраструктуры.

В состав «Инфосекьюрити» входит Лаборатория компьютерной криминалистики, специалисты которой участвуют в раскрытии киберпреступлений, проводят тесты на проникновение и исследования различных цифровых объектов.

В начале 2018 года Infosecurity вошла в состав Группы Softline.


mailarchiva
2010
начало формирования команды аналитиков
для работы с почтовым архивом

Как мы пришли к DLP?

Трейдер уходит в тюрьму

Суд Лондона приговорил похитившего у «Открытия» $150 млн трейдера Урумова к 12 годам

Семен Михайлов 27.01.2017, 18:08

Королевский суд в Лондоне вынес приговор экс-сотруднику корпорации «Открытие» Джорджу Урумову и бывшему брокеру Threadneedle Asset Management Владимиру Герсамия. За похищение у «Открытия» более $150 млн Урумов получил 12 лет тюремного заключения, Герсамия — семь. Ранее они были признаны присяжными виновными в мошенничестве и отмывании средств. Из зала суда оба отправятся в одну из лондонских тюрем.

Предпосылки

- Сбор доказательной базы для предоставления в суд
- Работа с большим объемом накопленных данных
- Поиск и анализ информации в сжатые сроки
- Контроль действий сотрудников с целью недопущения повторения истории с Урумовым
- Мониторинг коммуникаций в условиях постоянной интеграции бизнесов

Критерии первоначального выбора DLP (2011-2012)

- Наиболее полный перехват каналов
- Масштабируемое решение
- Удобство поиска и выгрузки данных
- Готовность вендора к сотрудничеству
- VIP-поддержка

DLP-система, которую мы тогда выбрали

SEARCHINFORM
INFORMATION SECURITY

Вехи истории (2012 – 2017)

- Постоянное увеличение объемов информации за счет Регулярного расширения бизнеса ключевых клиентов
- Появление новых отраслей бизнеса клиентов
- Увеличение штата инженеров и аналитиков для работы с системой (штат аналитиков увеличился с 3 до 15 человек)
- Модификация задач, поставленных перед DLP-системой
- Подбор DLP-решения на замену текущему

Разделение компетенций аналитиков системы. I этап

БАНКОВСКИЙ СЕКТОР

Открытие, Траст, Росгосстрах Банк

БЛОК НЕБАНКОВСКИХ ОРГАНИЗАЦИЙ

Брокеры, Страховые компании, НПФ

Разделение компетенций аналитиков системы. II этап

Настройка системы
В том числе аналитики политик безопасности

- Обработка событий и инцидентов
- Поиск и анализ информации
- Профилирование сотрудников

Изменение вектора общения с текущим вендором

Смещение акцентов с техподдержки на доработку

Совместный с вендором roadmap

Ведение changelog по релизам и доработкам

Разделение компетенций аналитиков системы. III этап

- Аналитика инцидентов ИБ, определение легитимности действий сотрудников
- Контроль процесса обработки, передачи и хранения конфиденциальной информации

- Мультиканальный контроль за действиями сотрудников
- Выявление признаков недобросовестности сотрудника (предупреждение фактов потенциального нарушения и создания конфликтных ситуаций
- Оценка эффективности работы сотрудников

- Расследование возможных утечек клиентских данных (ретроспективный анализ)
- Анализ внутренних и внешних связей сотрудников для предупреждения репутационных и финансовых рисков
- Анализ распространения информации (файлов, значимой информации, отдельных частей конфиденциальных документов)

Кейсы применения DLP

Выдача «плохих» кредитов

На момент проверки заявки по выдаче крупного кредита под залог земельных участков, выяснилось, что они уже **находились в залоге** у нескольких несвязанных кредитных организаций, а полученные кредитные средства планировалось инвестировать в **собственность за рубежом**.

Сопровождение значимых проектов

При проведении тендера на закупку дорогостоящего оборудования, в результате анализа коммуникаций, IT-директор был замечен в **лоббировании** определенного **поставщика**.

Кейсы применения DLP

Обналичивание денежных средств

В результате анализа поисковых запросов, у некоторых сотрудников был выявлен интерес к Интернет-ресурсам по тематике **«серых схем».** В ходе дальнейшего разбирательства, было установлено, что они, используя свое служебное положение, открывали счета, для дальнейшего обналичивания денежных средств. Таким образом, за полгода ими было обналичено более **150 млн. руб**. В результате проведенного расследования, сотрудники были уволены, счета заблокированы, материалы переданы в правоохранительные органы для **возбуждения уголовного дела.**

Контроль ключевых сотрудников

Инвестиционному консультанту на личный электронный адрес поступило предложение о **переходе в компанию-конкурент**, при этом одним из условий было, помимо действующих клиентов, **переманить всю команду**.

Кейсы применения DLP

Выявление групп рисковых сотрудников

Офицером безопасности в рамках ежедневной активности по выявлению рисковых сотрудников было обнаружено событие в системе DLP, сформированное по настроенной политике, в котором была зафиксирована переписка 2 сотрудников Департамента инвестиций Криволапова М.Г. и Праворучко Н.Д., свидетельствующая о нелояльном отношении к Руководству компании АО «Б».

В ходе анализа переписки указанных сотрудников было установлено, что Криволапов М.Г. и Праворучко Н.Д. собираются покинуть компанию АО «Б» и уже успешно прошли собеседования в компании конкуренте АО «Б». Также, Криволапов М.Г., будучи руководителем Департамента инвестиций, планирует переманить свою команду.

Кейсы применения DLP

Выявление мошеннических схем

Офицером безопасности на дашборде системы DLP было обнаружено сообщение о наличии нетипичной связи у сотрудника компании Нелепхиной И.Т.. В ходе анализа почтовой переписки было установлено, что Нелепхина И.Т. перечисляет внушительные денежные суммы третьему лицу, которому и принадлежит электронный адрес, выявленный в нетипичных связях. Третье лицо, в свою очередь, переводило ровно такие же суммы еще одному сотруднику компании Мурадову М.Г.. Впоследствии было установлено, что Нелепхина И.Т. и Мурадов М.Г. являются сожителями и таким образом переводят денежные средства за откаты.

Кейсы применения DLP

Контроль рабочего времени сотрудников

Офицером безопасности было обнаружено событие в системе DLP, сформированное по настроенной политике, в котором содержалась информация о просмотре сотрудником автомобильного портала в сети интернет.

В ходе анализа активности было установлено, что сотрудник регулярно проводит время на развлекательных ресурсах сети интернет, а также запускает игровые приложения на своем корпоративном компьютере.

Расширение функционала аналитиков

1. Увеличение ресурса на изучение функционала системы
2. Составление чек-листа для подбора «идеальной» DLP-системы
3. Общение с другими вендорами. В том числе Solar Security

На какую DLP-систему поменять

SEARCHINFORM
INFORMATION SECURITY

?

Рассмотренные решения

МФИ СОФТ
ГАРДА ПРЕДПРИЯТИЕ

SOLAR DOZOR

INFOWATCH TRAFFIC MONITOR

SecureTower™ ZECURION STAFFCOP

FORCEPOINT
POWERED BY Raytheon

TOP-3 DLP-решений

Почему Dozor?

- Полуавтоматическое ведение "досье" на каждого работника, учитывающее должность, предстоящее увольнение, наличие внешних рабочих контактов, наличие фактов нарушения в прошлом (репутация) и прочее

- Система разграничения функционала аналитиков ИБ

  Обнаружение -> обработка события -> контроль нагрузки и эффективности работы

  Удобный формат взаимодействия аналитиков

- Группировка событий по информационным объектам
  Например, всё, что происходило с определённым документом, в дополнение к классическому варианту с группировкой по сотрудникам

Почему Dozor?

- Хорошие возможности по предотвращению утечки информации (продемонстрировано на демонстрационном стенде):
  - ✓ Возможность запретить передачу
  - ✓ Уведомление о возможном нарушении правил ИБ
  - ✓ Возможность разрешать передачу информации только после согласования сотрудника ИБ (при истечении срока, отведенного на реакцию, передача информации может быть разрешена/запрещена автоматически)
  - ✓ Возможность запрашивать согласование на отправку информации у руководителя сотрудника
  - ✓ Лучший показатель по возможности реализации требований в блоке "анализ"
- Возможность получения информации из стороннего ПО (например, списки увольняемых)
- Качественная презентация с демонстрацией функционала, демо-стендом и кратким обучающим курсом

Новейшая история. 2017- 2018

- Увеличение пула потенциальных клиентов за счет присоединения к группе Softline
- Дальнейшее наращивание компетенции по работе с DLP-системами
- Выбор вендоров для стратегического партнерства - Solar Security
- Обсуждение вариантов совместных продуктов Solar Security и Infosecurity

Советы. Как избежать ошибок

- Формирование своего чек-листа
- Больше разных мнений о системе от тех, кого вы знаете и кому доверяете
- Правильный вектор взаимодействия с вендором
- Брать на пилот только то, что вам подходит по чек-листу
- Осознать, что вы хотите получить от системы не только после внедрения, но и в ходе дальнейшей ее эксплуатации

Советы. Какие задачи можно решать

- Предотвращение утечек информации
- Соблюдение требований законов и подзаконных актов
- Контроль движения информации в компании
- Контроль за коммуникациями сотрудников
- Поиск внутренних злоумышленников

Для кого будет польза от DLP

Собственники бизнеса

ТОП-менеджмент

Функциональные руководители

Служба безопасности

HR

Чем могут помочь Solar Security и Infosecurity

- Аудит существующих процессов обеспечения экономической безопасности
- Разработка контрольных процедур для выявления внутреннего мошенничества
- Выбор и адаптация инструментальных средств: настройка и адаптация политик безопасности DLP
- Выстраивание процессов мониторинга и реагирования на инциденты безопасности
- Своевременное выявление инцидентов информационной безопасности

Спасибо за внимание!

Анна Попова
Руководитель Департамента анализа активности пользователей (DLP)

Anna.Popova@softline.com
popova@infosecservice.ru