ИНСТРУМЕНТЫ БЕЗОПАСНОСТИ

Кастомизируй это: Преумножаем возможности DLP с помощью интеграции с другими программами

Современная DLP-система – это не монолит. Под запрос клиента ее можно интегрировать со сторонними сервисами для полезного обмена информацией. Это существенно увеличивает как функционал DLP, так и сторонних приложений. Начальник отдела информационной безопасности «СёрчИнформ» Алексей Дрозд рассказывает, какие возможности пользователи систем упускают из виду.

Совмещая свой функционал с возможностями другого ПО, DLP может выступать в двух ролях: как источник информации и как процессор, который перерабатывает данные из других систем. Последнее очень важно, так как DLP по сути становится единым мозговым центром, без которого приложения работают автономно и данными не обмениваются.

Некоторые интеграции DLP со сторонними программами стали настолько привычными, что «шов» уже и незаметен. Мало кто вспоминает: а разве было когда-то иначе? Это можно сказать об интеграции с OCR-модулем (никто не усомнится, что DLP-система обязана уметь распознавать текст с картинки) или с SIEM-системой.

Но есть и менее очевидные способы сдружить системы. Ниже перечень программ и систем, из которых собирает данные «СёрчИнформ КИБ». Но он неполный, так как через API систему можно интегрировать практически с любой другой программой.

- системы управления доступом (IMD);
- SIEM-системы;
- системы расчета зарплаты;
- BI-системы;
- системы мониторинга технического состояния (например, zabbix);
- DCAP-системы;
- СКУД;
- оперативные центры SOC;
- DAM-системы.

Проще всего показать, как работает эффект синергии на примере интеграции DLP + СКУД.

На этапе тестирования «СёрчИнформ КИБ» в компании вскрыли схему, по которой сотрудники «прикрывали» отсутствие коллег на рабочем месте. Судя по данным из СКУД, они были на рабочем месте. Однако модуль DLP по контролю рабочего времени (Program Controller) не фиксировал никакой или крайне низкую активность за ПК. Тогда подключили камеры и выяснили, что сотрудники даже не появлялись на рабочих местах. В начале и конце рабочего дня в СКУД сотрудник отмечался не только своей карточкой, но и карточками коллег.

Активность за ПК при том, что сотрудник не прошел через проходную, тоже должна быть алертом, настроенным в политиках безопасности DLP. Эта сработка может указать на то, что сотрудник получил удаленный доступ к компьютеру в обход правил. Или что кто-то использует его учетку.

Еще один полезный вариант интеграции – это обмен информацией DLP с бухгалтерскими системами начисления зарплат (т. н. payroll). Заказчики давно интересовались такой возможностью. Особенно активно интеграцию стали применять во время массовой удаленки – это оказалось хорошим способом сделать расчет быстрее и объективнее.

Мы обычно предостерегаем клиентов от чрезмерного увлечения таким методом (чтобы не «кошмарить» сотрудников поминутным контролем – все это приносит больше вреда). Но для расчета зарплаты некоторых сотрудников, где критерии начисления однозначны, подход оказывается оправданным. Например, это возможно для сотрудников техподдержки или колл-центра.

Защищено, еще защищеннее

Интеграция с DCAP* – и DAM** – системами – это пока еще редкая комбинация, но востребованная. DCAP позволяет наводить и поддерживать порядок

DLP видит, если сотрудник начал пересылать информацию, выгруженную из БД, но сам момент обращения не фиксирует. Это сделает DAM-система

в файловой системе: выявлять, какие документы содержат критичную для бизнеса информацию, где они находятся, кто к ним обращается. DAM-системы позволяют полноценно и удобно защищать базы данных: выявлять внесение критичных изменений для мошенничества или саботажа, удаление, слив и копирование информации.

Эти возможности ПО ценны сами по себе. Но в связке DLP+DCAP+DAM дают полноценную защиту на всех уровнях IT-инфраструктуры, позволяют сократить время выявления инцидента, найти первопричины и показать его полную картину.

Как правило, DLP-системы (в частности наша «СёрчИнформ КИБ») обладают механизмом eDiscovery для работы с данными в покое. Но задача eDiscovery – просто найти конфиденциальное содержимое, тогда как ИБ-специалистам нужно еще и выявить всех сотрудников, которые имеют доступ к файлам, определить, какие были внесены последние изменения, какие редакции критичных файлов сохранены и т. п. И здесь в дело должна вступать DCAP.

Также, DLP-система видит, если сотрудник начал пересылать информацию, выгруженную из БД, но сам момент обращения не фиксирует. Так теряется ценное время на предотвращение инцидента.

Как на практике

Разберем схему расследования инцидентов с использованием комбинации инструментов. Вот реальный пример.

Кейс

Нарушитель – экономист регионального отделения крупного федерального банка. В программе для работы с платежными картами клиентов он несколько раз увеличивал лимит по собственной карте, а потом по карте своего знакомого – подельника. Сначала суммы были небольшие, потом выросли – до 25,9 млн рублей.

В судебной практике немало подобных мошенничеств, хотя это по масштабу, пожалуй, самое заметное. Расследование такого нарушения провести сложно, так как сотрудник формально действует в рамках своих полномочий. Кроме того, нет потерпевшего клиента, который бы заявил об ущербе, и банк обнаруживает подобные проблемы только в результате регулярного мониторинга. Или если повезет, и кто-то из сотрудников заподозрит неладное, поделится этим со службой безопасности.

Но если единственные зацепки – это цифровые следы, нужны системы мониторинга.

Вариант 1 – в компании стоит DLP-система. Она зафиксирует цифровые следы преступления – это очень важно для того, чтобы ретроспективно расследовать инцидент, собрать доказательства вины, которые примет суд. Ими станет отчет об активности в конкретной программе + запись с монитора о конкретных действиях. Но так как перемещения документов нет, ИБ-специалист не сможет остановить инцидент в режиме реального времени.

Вариант 2 – когда DLP работает в связке с системой мониторинга баз данных.

В DAM-системе сработает сложная политика безопасности, что: 1) пользователь обращается к БД, задавая условия («изменить лимит») + 2) значение этого лимита выше заданной сумму (например, больше 50 тысяч рублей). Оба действия легитимные, но сочетание их – опасное и с большой долей вероятности укажет на мошенничество.

DLP же позволит собрать доказательства инцидента: кто был за компьютером (данные авторизации + фото человека перед монитором), его активность в программах, а также конкретные действия в ней.

Заключение

Все описанные возможности интеграции реализованы в DLP «СёрчИнформ КИБ», в том числе с собственными DCAP-системой (FileAuditor) и недавно вышедшей в релиз DAM-системой (DataBase Monitor). Все их можно поставить на тест одновременно, чтобы оценить эффективность каждой и работу в связке. Пилотные версии доступны бесплатно и в полном функционале. Запросите их на сайте searchinform.ru. ●

* DCAP (Data-Centric Audit and Protection) – класс решений, задача которого автоматизированный аудит данных в файловой системе, поиска нарушений прав доступа и отслеживания изменений в критичных документах.
**DAM (Database Activity Monitoring) – класс решений, задача которого – автоматический мониторинг и аудит операций с базами данных.