Файлы под контролем

Иногда функции контроля стоит отделить от функций управления – так будет безопаснее и надежнее. Примером такой разделенной системы может служить решение на базе продукта IBM Tivoli Compliance Insight Manager, внедренное в компании «Энергопром Менеджмент» .

Управлять информационными активами должен отдел информационных технологий, а контроль лучше доверить службе информационной безопасности. Тогда в случае возникновения ошибки в администрировании или несанкционированных действий со стороны "всесильных" системных администраторов, эти нарушения будут зафиксированы службой ИБ, которая будет решать возникшую проблему уже организационными мерами. Для построения такой разделенной системы логично использовать разные продукты: один будет использоваться службой ИТ для управления, а другой – сотрудниками безопасности для контроля. Примером такой разделенной системы может служить внедрение в компании "Энергопром Менеджмент" продукта IBM Tivoli Compliance Insight Manager (ITCIM).

Компания "Энергопром Менеджмент" занимается производством углеграфитовых изделий. Хотя в качестве сырья используется уголь и кокс, производство относится к металлургической промышленности. В России компания является фактическим монополистом в своей отрасли. Такое положение компании удалось заслужить благодаря рецептам изготовления углеграфитовых изделий, которые были разработаны в середине прошлого века и по сей день остаются актуальными.

Одна из задач, стоящих перед службой ИБ состоит в том, что бы осущевствлять контроль правил доступа пользователей к файлам – в "Энергопром Менеджмент" формализована политика безопасности и строго структурирована файловая система. В результате сотрудникам службы ИБ достаточно знать, кто к каким файлам получал доступ, чтобы вовремя предотвратить утечку промышленных секретов. "Сотрудники отдела информационной безопасности не раз просили нас предоставить информацию о том, кто и к каким файлам получал доступ, а у нас не было инструмента, чтобы зафиксировать эту информацию", - пояснил Александр Дидух, директор по ИТ "Энергопром Менеджмент".

Для предоставления таких данных пришлось внедрять систему обработки событий информационной безопасности на базе продукта ITCIM. Внедрение системы осуществила компания CompuTel, которая до этого уже успешно внедрила для «Энергопром Менеджмента» систему сбора и обработки событийной информации на основе продуктов IBM Tivoli. Предполагалось, что создание подобной системы контроля позволит компании защититься от утечек секретной информации и воровства данных в случае увольнения сотрудника, а кроме того, даст возможность проанализировать деятельность сотрудников и произвести в случае необходимости расследование инцидентов. Впрочем, разработчики ITCIM ставили своей целью решение более общей задачи – обработки потока событий, который генерируют различные компоненты информационной системы, и сохранения их для дальнейше-го анализа и расследования инцидентов. Продукт также позволяет архивировать сообщения о происходящих в системе событиях и готовить отчеты о работе защитных механизмов. На определенные события можно настроить немедленную реакцию, чтобы сотрудники службы ИБ могли оперативно принять меры организационного порядка.

В основном продукт предназначен для проверки соответствия реальной информационной системы тем требованиям, которые накладывают международные, отраслевые или корпоративные стандарты. Внедрение ITCIM помогает компании в прохождении процедуры сертификации по некоторым стандартам. В частности, для этого продукта разработаны два дополнительных модуля: по стандарту ISO27001: 2005 и по требованиям PCI DSS. Использование этих модулей упрощает процедуру получения сертификатов на соответствие этим стандартам – оба стандарта требуют наличия системы внутреннего аудита, а именно эту задачу и призван решать ITCIM.

Однако в «Энергопром Менеджмен-те» используется только та часть продукта, которая позволяет следить за досту пом приложений к определенным файлам. Продукт должен контролировать соблюдение требований корпоративного стандарта на правила доступа, которые зафиксированы в политике безопасности. Требования к обработке событий были сформулированы самой компанией: в «Энергопром Менеджменте» есть принятая и утвержденна я политика безопасности. Однако проконтролировать ее соблюдение до внедрения ITCIM было непросто. При этом на предприятии одновременно работают с приложениями около 150 человек, и их работа приводила к тому, что системный журнал, куда записываются все операции с файлами, мог за день пополниться на 5—20 Гбайт информации.

В процессе внедрения сотрудники службы ИТ установили на все используемые в компании приложения специальные агенты, которые фиксируют обращение этих приложений к файловой системе. Такие агенты были установлены на Lotus Domino, файл-сервера Windows и MS SQL Server, всего около двух десятков агентов. Этого оказалось достаточно, чтобы система могла контролировать события в центральном офисе компании и во всех ее филиалах. Собранные данные сохраняются на выделенном сервере компании HP с двумя дисками по 750 Гбайт, объема которых по расчетам службы ИТ должно хватить на запись данных в течение года.

Для анализа событий продукт снабжен Web-интерфейсом, с помощью которого служба информационной безопасности может настроить собственные правила контроля доступа к файлам, формировать отчеты и настраивать сигналы тревоги.

В основе ITCIM лежит ролевая модель для определения правил работы с учетными записями. Впрочем, продукт не дает возможности реально управлять правами доступа пользователей – эти функции возложены на ИТ-службу, которая пользуется для этих целей Active Directory. Наличие двух разных продуктов для управления и контроля делает систему более безопасной: служба ИБ контролирует корректность прав доступа пользователей, но сама не может на них повлиять.

Построенная на основе ITCIM система контроля доступа к файлам позволила службе информационной безопасности фиксировать факт доступа пользователей к секретной информации и оперативно применять меры организационного воздействия. Наличие системы контроля за деятельностью сотрудников оказывает в том числе и дисциплинирующее воздействие на людей.

Несмотря на то что ITCIM является более общим продуктом, использование его для контроля операций с файлами позволило «Энергопром Менеджменту» предоставить службе информационной безопасности необходимые данные для выявления случаев неавторизованного доступа к секретам предприятия. Хотя в компании установлена система защиты шлюза, которая контролирует канал подключения к Internet, данные из нее не передаются в ITCIM, в этом нет необ-ходимости. Иначе говоря, незадействованными остаются наиболее интеллектуальные функции продукта, такие как корреляционный анализ. Тем не менее ITCIM эффективно решает поставленную перед ним задачу, являясь первым крупным внедрением этой технологии в российской компании.

По материалам журнала "Инновации в технологиях и бизнесе", 2.2009