



SecureTower — эффективный инструмент для защиты от внутренних угроз

Компания Falcongaze была основана в 2007 году. Является разработчиком и поставщиком высокопроизводительных решений премиум-класса в области информационной безопасности. Предлагает комплексные решения для контроля утечки и нежелательного распространения конфиденциальной корпоративной информации, адаптированные для мониторинга сетевой деятельности сотрудников.

Почему ваша разработка востребована в банковской сфере?

Банковская сфера является наиболее чувствительной к потере конфиденциальных данных, поскольку цена утечки информации для банка может быть не просто велика, а даже критична.

Специфика работы банков предполагает наличие баз данных, содержащих персональную информацию клиентов и данные по их операциям, огромных массивов электронных документов, финансовой документации. Поэтому, с одной стороны, важно контролировать утечку таких данных, в каком бы формате они ни находились, будь то файлы, электронная переписка или базы данных. С другой стороны не менее важно контролировать как можно большее количество каналов передачи данных. Поскольку практически вся ценная информация хранится в электронном виде, неизбежна ее передача посредством, например, электронной почты, мессенджеров, социальных сетей или путем записи файлов на внешние носители.

В таких условиях невозможно исключить вероятность ни преднамеренной, ни тем более случайной утечки данных. Последствия такой утечки могут быть самыми серьезными: репутационные риски, связанные с потерей доверия клиентов и вкладчиков, судебные иски и штрафные санкции, влекущие за собой прямые финансовые убытки.

Кроме того, доступность современных средств коммуникации при отсутствии должного контроля над ними может способствовать серьезному ухудшению рабочих показателей. Так, чрезмерное общение по мессенджерам или в социальных сетях приводит к неэффективному использованию корпоративных ресурсов и рабочего времени, что приводит к нарушениям производственных процессов сотрудниками и снижает эффективность ведения бизнеса.

Каким образом вы решаете эти проблемы?

Мы обеспечиваем комплексный подход к информационной безопасности,



Александр Акимов,
директор компании
Falcongaze.

Справка ТБ

Акимов Александр Иванович. Директор компании Falcongaze. Образование высшее, в 1992 году закончил БГУИР. Опыт работы в сфере информационной безопасности и систем защиты от утечки информации — с 2007 года.

включающий в себя контроль всевозможных каналов передачи данных и мониторинг сетевой активности персонала. Именно эти составляющие являются жизненно важными для любой компании, работающей в банковской сфере. Без какой-либо из них усилия, предпринимаемые для обеспечения информационной безопасности предприятия, можно считать лишь полумерами.

Такой комплексный подход к решению проблем информационной безопасности и реализован в DLP-системе SecureTower.

SecureTower отслеживает и контролирует всю электронную почту, сообщения мессенджеров, любую активность, которую проявляют сотрудники компании в блогах, форумах, социальных сетях. Особо стоит упомянуть о контроле сообщений и разговоров в программе Skype. Именно ее во многих компаниях принято запрещать, поскольку далеко не каждая DLP-система «умеет» расшифровывать и анализировать трафик, идущий через нее. При этом система предоставляет исчерпывающую информацию о том, когда, каким пользователем, с

какого компьютера в сети и куда была произведена отправка данных.

Вы отдельно упоминали о контроле персонала. Почему это так важно? Какую пользу это приносит компании?

В современных банках многие сотрудники имеют доступ к конфиденциальным документам, будь то финансовые отчеты, банковская нормативная документация или персональные данные клиентов. Да и исключать варианты, что в компании работают нелояльные или нечистые на руку сотрудники, — nepозволительная роскошь.

SecureTower дает возможность не только формировать детальные отчеты о сетевой активности любого сотрудника, но, что гораздо важнее, автоматически отслеживать взаимосвязи персонала как внутри информационного поля компании, так и с внешними абонентами. В результате в руках заказчика находится многоцелевой инструмент для своевременного определения и упреждения возможных утечек информации, а не только для расследования уже случившихся инцидентов.

Были ли в вашей практике конкретные примеры?

Да, например, в одном из банков еще на стадии тестирования SecureTower был выявлен нелояльный сотрудник, основное рабочее время которого, судя по отчетам и снимкам экрана, уходило на посещение развлекательных сайтов и гиперактивное общение в мессенджерах на темы, даже отдаленно не связанные с работой. При более детальном анализе было определено намерение отсылки важных сведений конкурентам и последующего трудоустройства к ним же. С помощью функции графа-анализатора взаимосвязей было установлено, что конкурент контактировал еще с несколькими сотрудниками банка. Это позволило службе безопасности своевременно определить наметившуюся угрозу и без потерь локализовать назревающий инцидент.

Каковы затраты на внедрение вашего продукта?

Наша разработка очень успешно развенчивает миф о том, что DLP-система — это что-то очень сложное в использовании и настройке, громоздкое по архитектуре и требующее перестройки всей инфраструктуры сети. На деле развертывание и запуск системы

SecureTower сродни установке любого коробочного продукта и занимает несколько часов, не требуя вызова многочисленных технических специалистов, покупки дополнительного дорогостоящего оборудования, оплаты услуг по внедрению и консалтингу, зачастую составляющих львиную долю бюджета, предназначенного на приобретение DLP-системы. По окончании установки система сразу же начнет полноценно функционировать, останется лишь привести SecureTower в соответствие с политиками безопасности, существующими в банке, создав правила безопасности в дополнение к уже имеющимся в комплекте поставки решения. Реальный эффект от внедрения несомненно будет получен еще на стадии тестирования полнофункциональной триал-версии.

Каковы современные тенденции в сфере информационной безопасности?

Тенденции на данный момент таковы, что DLP-решения становятся все более востребованными, причем банковский сектор находится здесь в авангарде и среди наших клиентов за последнее время значительно возросло количество банков, что во многом обусловлено ценностью имеющихся данных. Также, следует отметить, что на сегодняшний день борьба с внутренними угрозами уже не является прерогативой крупных банков, ведь даже небольшие частные банки владеют информацией, утечка которой может стать критичной для дальнейшего развития. Хотя это в полной мере касается и других областей ведения бизнеса.

Поэтому необходимо постоянное совершенствование методов перехвата и

анализа информации, расширение количества контролируемых путей утечки, богатый инструментарий для расследования любого инцидента в ретроспективе и, конечно, средства для контроля над деятельностью персонала. При этом внедрение системы в инфраструктуру банка и процесс настройки и эксплуатации должны быть максимально быстрыми, удобными и простыми, никак не влияющими на рабочий процесс. Именно в этом направлении и движется развитие DLP-системы SecureTower.

ООО "Фалконгейз"

Эксклюзивный представитель в

Беларуси — компания ДПА Бел

220116, г. Минск, пр-т Дзержинского,

104, офис 503

Тел./Факс: +375 (17) 277-26-37; 277-28-22

E-mail: info@dpa.by

УНП: 191125825

Проекты и решения

Системы видеоконференцсвязи на базе существующих систем коммуникаций. Объединение «Белорусская железная дорога».



Для повышения эффективности работы между отделениями, находящимися в других городах, и для проведения переговоров и обучающих мероприятий руководство «Белорусской железной дороги» приняло решение о создании **системы видеоконференцсвязи** на базе существующих систем коммуникаций. Также было принято решение о модернизации **центра диспетчерского контроля** состояния подвижного состава.

Задача

Оснащении студий «Белорусской железной дороги» аудио- и видеооборудованием для решения различного спектра задач — от проведения локальных мероприятий и семинаров до организации сеансов видеоконференцсвязи.

Выполненные работы

В зависимости от планируемых мероприятий каждая из студий может использоваться как в качестве презентационного зала, так и для проведения сеансов видеосвязи. В каждой студии имеется возможность вывода и передачи аудио- и видеоинформации с ноутбуков либо других источников. В главном управлении дороги оборудован конференц-зал с возможностью вывода и передачи аудио- и видеосигнала с 11-ти рабочих мест. Использование

современных технологий позволяет удаленно управлять оборудованием и устройствами в других студиях. Средствами ActiveX организована работа с файлами, находящимися на подключенном к сети Ethernet сервере, с выводом их на устройства отображения. Управление приложениями осуществляется посредством сенсорной панели.

Для обеспечения дежурных диспетчеров всей текущей информацией о состоянии и местонахождении подвижного состава и уменьшения времени на принятия решений в различных ситуациях в диспетчерском центре оборудована **информационная панель**, состоящая из 12 видеокубов.

Возможности (структура) системы

Главный диспетчер осуществляет управление раскладкой информационной панели и определяет важность вывода на основной экран той или иной информации, находясь при этом на своем рабочем месте. Проверка технического состояния и регулировка параметров любого из видеокубов осуществляется с помощью сенсорной панели.

Название предприятия, предоставившего описание

СП ООО «Информационные Производственные Архитектуры»