КОРПОРАТИВНАЯ БЕЗОПАСНОСТЬ: ЧТО ТАКОЕ DLP-СИСТЕМА И ЗАЧЕМ ОНА НУЖНА БИЗНЕСУ

РОМАН БОЖКОВ
R.Bazhkou@falcongaze.ru

Говоря о киберугрозах, мы обычно представляем себе беспрерывно стучащих по клавиатуре хакеров в черных толстовках, однако на деле большинство корпоративных утечек данных происходит не вследствие хитроумных технологичных взломов, а гораздо более тривиальными путями. В частности, через инсайдеров — сотрудников организации, намеренно или случайно предоставляющих конфиденциальную информацию злоумышленникам. Именно на предотвращение такой ситуации ориентированы DLP-решения (Data Leak Prevention), такие как разработка компании Falcongaze — система SecureTower.

ПРИНЦИП РАБОТЫ DLP

Для предотвращения утечек SecureTower интегрируется в корпоративную сеть организации и контролирует весь внутренний и внешний трафик, такой как электронная почта, веб-активность, мессенджеры, USB-подключения и т. д. Для мониторинга применяются две схемы перехвата (рис. 1) — серверный и агентский. В первом случае решение анализирует трафик на сервере, во втором перехват происходит непосредственно на рабочих станциях. Второй способ перехвата позволяет значительно расширить перехватываемые каналы, охватив в том числе большинство мессенджеров и веб-трафик по протоколу HTTPS. В зависимости от нужд заказчика способы перехвата могут комбинироваться или использовать только определенные модули системы. Также существуют методы перехвата без установки агентов, такие как совместная работа SecureTower с proxy-устройствами при помощи ICAP-интеграции (контроль веб-трафика) и интеграция с почтовым сервером (контроль корпоративной почты).

Все перехваченные данные анализируются системой для выявления инцидентов, представляющих интерес для соответствующей службы. Их анализ происходит на основе заранее заданных правил безопасности, которые могут быть самыми разными

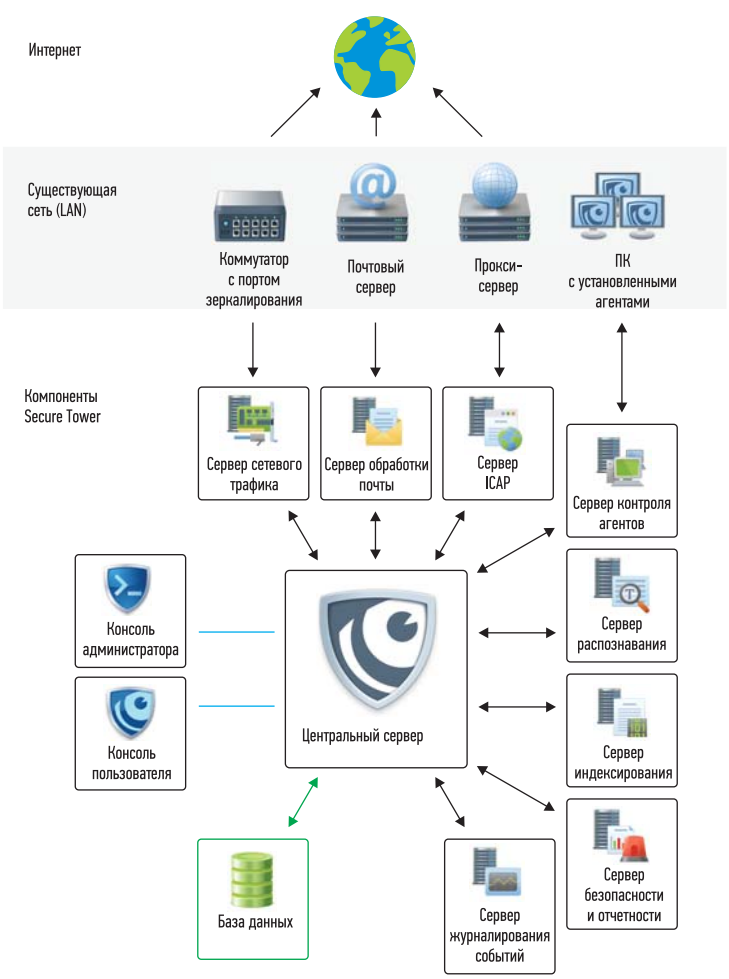


РИС. 1. ◀
Схема внедрения SecureTower

и сколь угодно сложными: система способна, например, уведомлять о передаче большого числа файлов на печать сотрудниками определенного отдела или блокировать передачу по электронной почте документа, содержащего данные из базы конфиденциальных документов. Все уведомления о событиях отправляются ответственному лицу, которое уже принимает решение, был ли инцидент правомерным или необходимо начать расследование.

ДЛЯ ЧЕГО НУЖНА DLP

Первоочередная задача, решаемая с помощью внедрения DLP-системы, — защита корпоративных данных от утечки. Использование системы — один из ключевых элементов в процессе построения эффективной системы управления информационной безопасностью. Без нее говорить о какой-либо защищенности от инсайдеров в компании бессмысленно.

Эффективность DLP проявляется не только в упреждении угроз информационной безопасности, но и в работе с бизнес-процессами. Благодаря тому что весь информационный трафик становится доступен для просмотра и оценки, появляется возможность для существенной оптимизации процессов — в том числе с точки зрения бизнес-составляющей. Задачи, на которые без DLP уходили бы значительные временные и человеческие ресурсы (например, классификация информационных активов), решаются значительно быстрее и качественнее.

DLP-система является эффективным инструментом для руководителей и HR-менеджеров. С помощью нее можно получать полную картину рабочего дня сотрудников, корректировать сроки и распределение задач, выявлять слабые места во взаимодействии персонала. В системе также возможен учет рабочего времени и активности сотрудников в рабочих программах.

Для создания полной картины информационных потоков DLP сохраняет все переданные и полученные данные. Это позволяет использовать SecureTower как инструмент ведения архивов бизнес-коммуникации. Любой диалог, а также переданный или полученный документ, можно восстановить из архива.

КАК РАБОТАТЬ С DLP

Для работы с системой предусмотрены две консоли — для администратора и для клиента. Первая позволяет взаимодействовать с серверными компонентами, а вторая предназначена для непосредственной работы с продуктом.

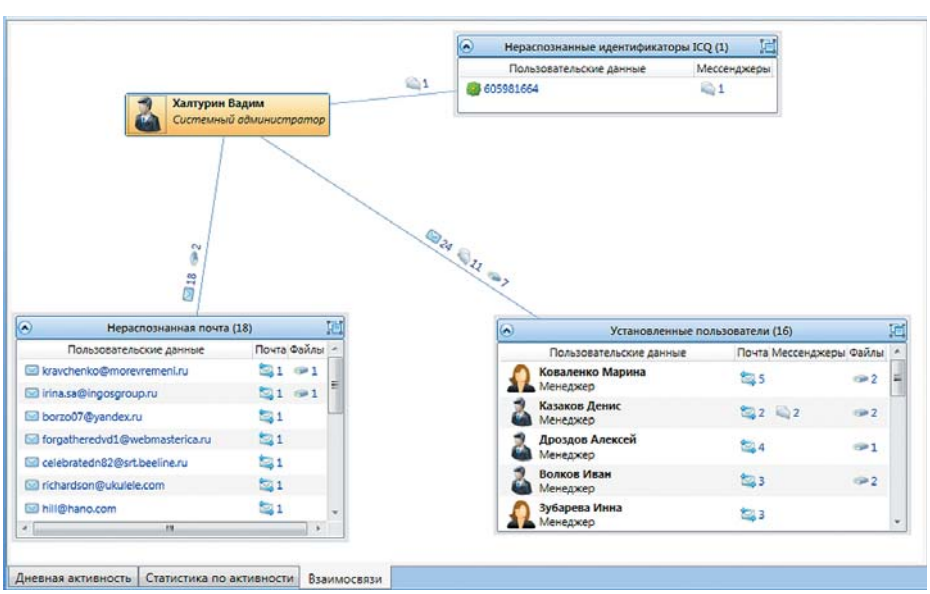
В клиентской консоли для работы с системой доступны семь модулей: модуль активности пользователей, модуль поиска информации, мониторинг файловых систем, модуль комбинированного поиска, центр обеспечения безопасности, центр отчетности и мониторинг в режиме реального времени.

Активность пользователей

Система в автоматическом режиме сохраняет всю перехваченную пользовательскую информацию. Данный модуль обеспечивает возможность ее просмотра и ретроспективного анализа. Здесь можно увидеть всю активность работника за любой период времени. Для каждого сотрудника в системе заводится профайл, в который можно экспортировать данные из Active Directory, а также дополнить его почтовыми адресами, аккаунтами в мессенджерах и т. д. В ходе работы системы профайлы могут заводиться и на всех внешних абонентов, с которыми сотрудник ведет общение, т. е. если сотрудник общается с каким-то внешним контактом, есть возможность посмотреть, с кем еще из работников организации ведет переписку этот контакт. Для удобства все эти данные визуализированы в граф-анализаторе (рис. 2).

Пользователей можно структурировать по группам, в зависимости, например, от отдела. Доступна статистика по активности каждого сотрудника в течение рабочего дня: количество полученных и отправленных писем, пересылаемых документов, использование принтера и т. д. Все документы можно просмотреть непосредственно в системе или сохранить их на локальный компьютер. В этом же модуле можно увидеть скриншоты рабочего стола пользователя, автоматически создаваемые через заданные промежутки времени.

РИС. 2. ▼
Граф-анализатор



Поиск информации/ комбинированный поиск/ мониторинг файловых систем

Данные модули позволяют осуществлять поиск нужных документов в перехваченной информации и на компьютерах пользователей. С помощью простого поиска можно находить нужные файлы среди перехваченных документов. Параметры запроса можно конфигурировать, а в результатах поиска просмотреть, когда и какими сотрудниками был передан искомый документ.

Мониторинг файловых систем позволяет выявлять конфиденциальные корпоративные документы, которые по какой-то причине оказались на компьютерах сотрудников. Для контроля передвижения критически важных данных в системе можно создать банк эталонных документов, оборот которых необходимо контролировать. Монито-

ринг рабочих станций сотрудников осуществляется автоматически: настроенные в системе правила безопасности срабатывают при появлении на компьютере того или иного работника документа, совпадающего с образцом, хранящимся в банке данных.

При комбинированном поиске можно использовать сложные правила и задавать несколько условий: например, вести поиск среди перехваченной информации определенного отдела документа определенного формата, более чем на 70% совпадающего с конфиденциальным.

Центр обеспечения безопасности

В этом разделе можно задать правила безопасности и просматривать архив уведомлений об их нарушениях. Правила устанавливаются как обычные, так и статистические. Также существует возможность задания правил безопасности с контролем по словарю (словари создаются предварительно в системе) или цифровым отпечаткам (базы данных цифровых отпечатков основаны на конфиденциальных документах). Для каждого установленного правила можно назначать подписчиков на уведомления — как сотрудников службы безопасности, так и, например, руководителей отделов.

Центр отчетности

В этом модуле можно просмотреть отчеты за произвольный промежуток времени по всем пользователям (или группам пользователей) и перехватываемым каналам. Отчеты полностью настраиваемые и дают возможность как оценить ежедневную работу сотрудников, так и получить актуальную информацию по инцидентам безопасности. Здесь же можно настроить автоматическое создание отчетов по расписанию и отправку их на электронную почту.

Мониторинг в режиме реального времени

В данном модуле можно в режиме реального времени подключиться к компьютеру работника. Доступен как аудиомониторинг (через подключенную к компьютеру гарнитуру), так и режим просмотра рабочего стола сотрудника.

ВНЕДРЕНИЕ DLP

На первом этапе компании, решившей внедрить у себя DLP-систему, следует провести пилотное тестирование выбранного продукта. Для его проведения предоставляется бесплатная триальная версия на ограниченное количество рабочих мест. Уже во время тестирования становятся видны первые результаты работы системы — выявляются остававшиеся до этого незаметными нарушители. Полученные результаты чаще всего обеспечивают окупаемость системы уже на стадии пилота.

Отличительной чертой внедрения SecureTower является простота этого процесса. Для установки этой системы не требуется привлечение консалтинга или наличие специального оборудования, настройка производится из одной консоли, а развертывание и запуск системы занимает считанные часы.

После внедрения работа с DLP становится частью ежедневных процессов службы безопасности. Постоянное улучшение правил безопасности и выявление критических мест позволяет обеспечить должный уровень защищенности организации. ⬣