falcongaze®

Кейс клиента

Нелояльность сотрудников

Нарушение законодательства

Внутренняя угроза

Утечка информации о предстоящих акциях

В этом кейсе мы разберем, как с помощью DLP-системы Falcongaze SecureTower удалось установить факт передачи конкурентам коммерчески ценных данных о предстоящей промо-акции, а также выявить виновного и разорвать с ним трудовые отношения.

Проблема

В торговой сети произошла утечка данных о предстоящей промо-акции. Акция провалилась, торговая сеть не получила желаемую прибыль. В утечке подозревали кого-то из персонала, но доказать факт передачи коммерчески ценной информации не удалось. Поэтому решили сосредоточиться на том, чтобы ситуация больше не повторилась.

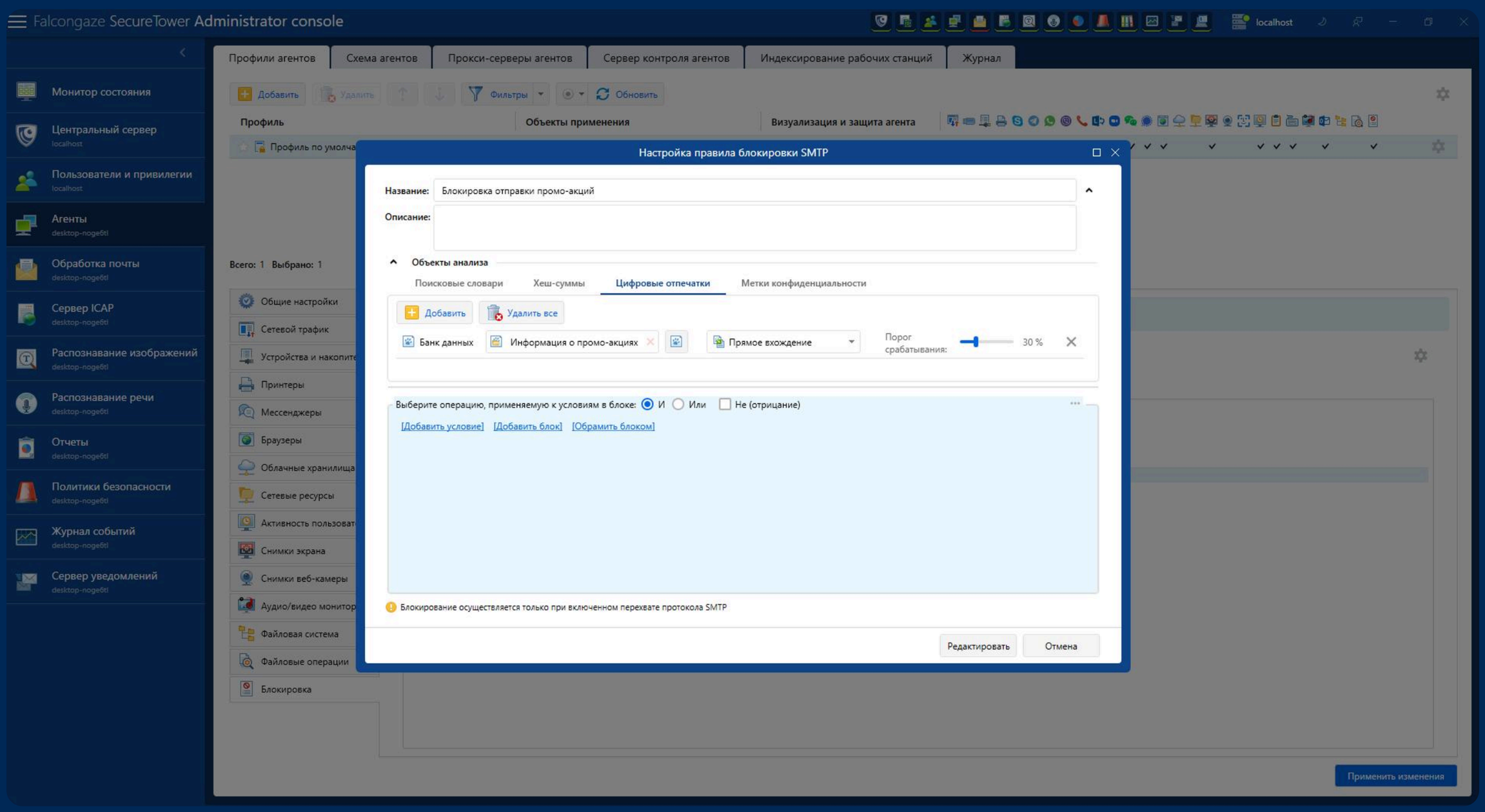
Решение

Для защиты коммерчески ценных данных компания приобрела SecureTower.

Система перехватывала данные во всех каналах коммуникации:

- электронная почта по протоколам SMTP, IMAP, MAPI и их шифрованным аналогам;
- мессенджеры (Telegram, Viber, Skype и еще 15 менее популярных аналогов);
- интернет (посещенные сайты, социальные сети, web-версии электронной почты, облачные хранилища и проч.);
- локальные и сетевые принтеры;
- буфер обмена;
- подключаемые устройства с внешней памятью и проч.

Помимо этого, были проанализированы все информационные ресурсы организации. С коммерчески ценных документов были сняты цифровые отпечатки (далее — ЦО). На основе собранных отпечатков был сформирован банк и настроена блокировка отправки документов, которые на 30% и более соответствовали снятым ЦО. Система автоматически блокировала отправку конфиденциальных данных по электронной почте, через мессенджеры, социальные сети, на внешние устройства с внутренней памятью, локальные и сетевые принтеры и проч.



Консоль Администратора (Настройка правила блокировки по протоколу SMTP)

На заметку! Создавая правила поиска по цифровым отпечаткам, вы можете выставлять порог срабатывания в соответствии с задачами безопасности вашей организаци

Кроме того, в модуле «Политики безопасности» были созданы правила, чтобы в случае обнаружения блокировки операций с такими документами SecureTower автоматически оповещала офицера безопасности.

Нарушительницу обнаружили следующим образом.

Сотрудница коммерческого отдела скопировала текст документа с данными о предстоящей акции и вставила его в середину другого многостраничного документа с названием «Стандартный договор». Затем она попыталась отправить готовый документ с подписью «Прошу ознакомиться со стандартным договором» не зарегистрированному в системе контакту, якобы новому поставщику.

Новое правило по цифровому отпечатку обнаружило соответствие текста и заблокировало попытку передачи конфиденциальных данных третьему лицу. SecureTower мгновенно оповестила уполномоченных.

Результат

- **Предотвращена утечка коммерчески ценных данных**

  Система заблокировала попытку отправки документа, содержащего данные о предстоящей промо-акции.

- **Выявлена недобросовестная сотрудница**

  С сотрудницей, совершившей нарушение, разорваны трудовые отношения.

Модули, которые были использованы:

🚨 Политики безопасности

Агенты (консоль Администратора)

falcongaze®