CommView® помогает компании Connetic обеспечить безопасность сети клиента

Пример использования

Незаконное использование сети своими сотрудниками

Как аутсорсинговая IT-фирма, специализирующаяся на безопасности, Connetic часто берется за выполнение сложных работ по обеспечению защиты сетей своих клиентов. Не так давно произошел случай, когда публичная компания, которая работает в сфере недвижимости,, была вынуждена уволить более 75% своих IT-сотрудников. Это случилось после того, как выяснилось, что IT-директор и другие работники занимались хищением трафика и серверных мощностей с целью создания нелегального Интернет-бизнеса (действительного нелегального, а не просто противоречащего внутренним правилам компании). Единственные, кто сохранил свои места после "кадровой чистки", были IT-сотрудники низшего звена, которые были не в курсе всех подробностей этой схемы.

В компанию Connetic обратились с предложением провести скрытое наблюдение сети и подготовиться взять ее под контроль. На подготовку было дано три дня. "Нам даже не было известно заранее, будет ли у нас возможность восстановить административные пароли для Windows-доменов и сетевых устройств", - говорит Метью Стребе, занимающий пост CIO в Connetic.

К тому моменту, когда персонал поставили в известность, сотрудники Connetic уже были готовы установить контроль над сетью, отключить любые сегменты сети, через которые был возможен удаленный доступ, наблюдать за ситуацией во всей сети, проводить сканирование на уязвимости и "потайные ходы", устранять уязвимости с высоким показателем риска или предотвращать возможные направления атак, а затем восстанавливать сервисы, которые ранее приходилось отключать от сети и давать рекомендации по повышению безопасности и контроля над сетью в будущем.

Установление контроля над ситуацией

Наиболее сложной задачей является организация защиты неизвестной сети от тех самых людей, которые занимались ее настройкой. Эти люди, как правило, очень заинтересованы в получении удаленного доступа к сети, поскольку сеть клиента являлась основным активом их нелегального бизнеса. Обязательным условием было то,, чтобы у злоумышленников не было возможности повторного доступа к сети с целью сокрытия улик. К счастью, сотрудникам Connetic удалось тайным образом получить доступ к паролям до того, как пришлось бы скрытным образом устанавливать аппаратный регистратор нажатий клавиш. Таким образом, удалось избежать перевода всех Интернет-сервисов в состояние "offline" с целью последующего взлома административных паролей или реинициализации сетевого оборудования, например, брандмауэра. Получив пароли, команда Connetic была готова восстановить контроль над сетью уже на месте.

Пока со служащими компании проводилась беседа, сотрудников Connetic сопроводили в серверную комнату, чтобы они начали процесс смены паролей на всех устройствах и тем самым закрыли доступ для всех служащих компании. Поскольку Connetic не располагала подробной документацией о структуре сети, в процессе

установления контроля над сеть крайне важной была возможность видеть все входящие в сеть и исходящие из нее потоки данных.

CommView обеспечивает прозрачность сети

Для достижения этой цели была создана точка мониторинга с использованием концентратора для маршрутизации соединения между главными коммутаторами и портом LAN главного брандмауэра. Теперь весь входящий и исходящий Интернет-трафик должен был проходить через этот концентратор, но поскольку концентратор находился за брандмауэром, трафик уже был отфильтрован от обычного "шума", который всегда присутствует от случайных попыток хакерских атак, сканирования портов и другой подобной сетевой активности.

После создания точки мониторинга к сети был подключен ноутбук с CommView для наблюдения за трафиком. По словам Метью Стребе, "пользуясь возможностью CommView отображать TCP-соединения в реальном времени, мы без труда могли отслеживать обычную сетевую активность и с помощью фильтров программы исключать трафик, который мы сочли допустимым. Способность CommView реконструировать потоки TCP с помощью одного клика мышью по соединению оказалась неоценима в данной ситуации – это позволило нам гораздо быстрее понять природу соединения и наблюдать за ситуацией действительно в реальном времени без необходимости увязания в деталях при формировании цепочки пакетов на сетевом уровне".

По окончании работы Connetic смогла обеспечить контроль за сетью и гарантировать клиенту, что случаев несанкционированного доступа к сети не было, и что все улики остались нетронутыми. Такая степень уверенности была бы невозможна без способности CommView рациональным и эффективным образом обеспечить прозрачность сетевого трафика в режиме реального времени.

О программе CommView

CommView – это мощный сетевой монитор и анализатор для сетей Ethernet. Имея множество удобных функций, CommView сочетает в себе производительность и гибкость с простотой использования.

О компании TamoSoft

Компания TamoSoft – один из мировых лидеров на рынке программных сетевых анализаторов и легального перехвата информации в компьютерных сетях. Самые современные стандарты и технологии, используемые в продуктах компании, помогут вам быстро и качественно решить стоящие перед вами задачи администрирования компьютерных сетей, поиска уязвимостей в них, отслеживания потоков данных, возможных вторжений в сеть извне или утечки информации изнутри сети.

TamoSoft
PO Box 1385
Christchurch 8140
New Zealand

Phone (USA): +1 866 582 6675
Phone (Russia): +7 495 6486296
Fax: +64 3 310 2413

sales@tamos.com
WWW.TAMOS.COM
WWW.TAMOS.RU