Тройной Контроль

Комплексная защита от внутренних угроз

По оценкам экспертов от 70% до 80% потерь от преступлений в сфере ИТ приходится на атаки изнутри. Компания ProLAN разработала комплексное решение, позволяющее эффективно защищать корпоративную сеть от внутренних угроз. Предлагаемое решение называется **Тройной Контроль**, и представляет собой аппаратно-программный комплекс, состоящий из следующих компонент:

- Видеокамер (IP-камер), имеющих интерфейс для подключения к сети Ethernet, используемых для видеонаблюдения.
- Одного (любого) из продуктов семейства ProLAN SLA-ON (ProLAN-Супервайзер, ProLAN-Администратор, ProLAN-Эксперт, ProLAN-Сервер), используемого для контроля действий пользователей, удаленного управления компьютерами пользователей, выявления аномалий в работе ИТ-Инфраструктуры и тестирования её «здоровья».
- Одного (любого) из продуктов семейства Observer компании Network Instruments (Observer, Expert Observer, Observer Suite), используемого для контроля сетевого трафика.

Рисунок 1. **Тройной Контроль** позволяет эффективно защищать корпоративную сеть при атаках изнутри.

Уникальность **Тройного Контроля** заключается в том, что все виды контроля - видеонаблюдение, контроль действий пользователей и контроль сетевого трафика интегрированы в единую систему управления «здоровьем» ИТ-Инфраструктуры. **Тройной Контроль** (далее **Т- Контроль**) возможен в двух вариантах: ручной **Т- Контроль** и автоматический **Т- Контроль**.

Ручной Т- Контроль

Идея ручного **Т- Контроля** заключается в следующем. Офицер службы безопасности на одном экране видит, во-первых, содержимое экранов пользователей сети, во-вторых, помещения, где они работают и их самих. Для этого используется приложение SLA-ON Operations, которое входит в состав всех продуктов семейства ProLAN SLA-ON.

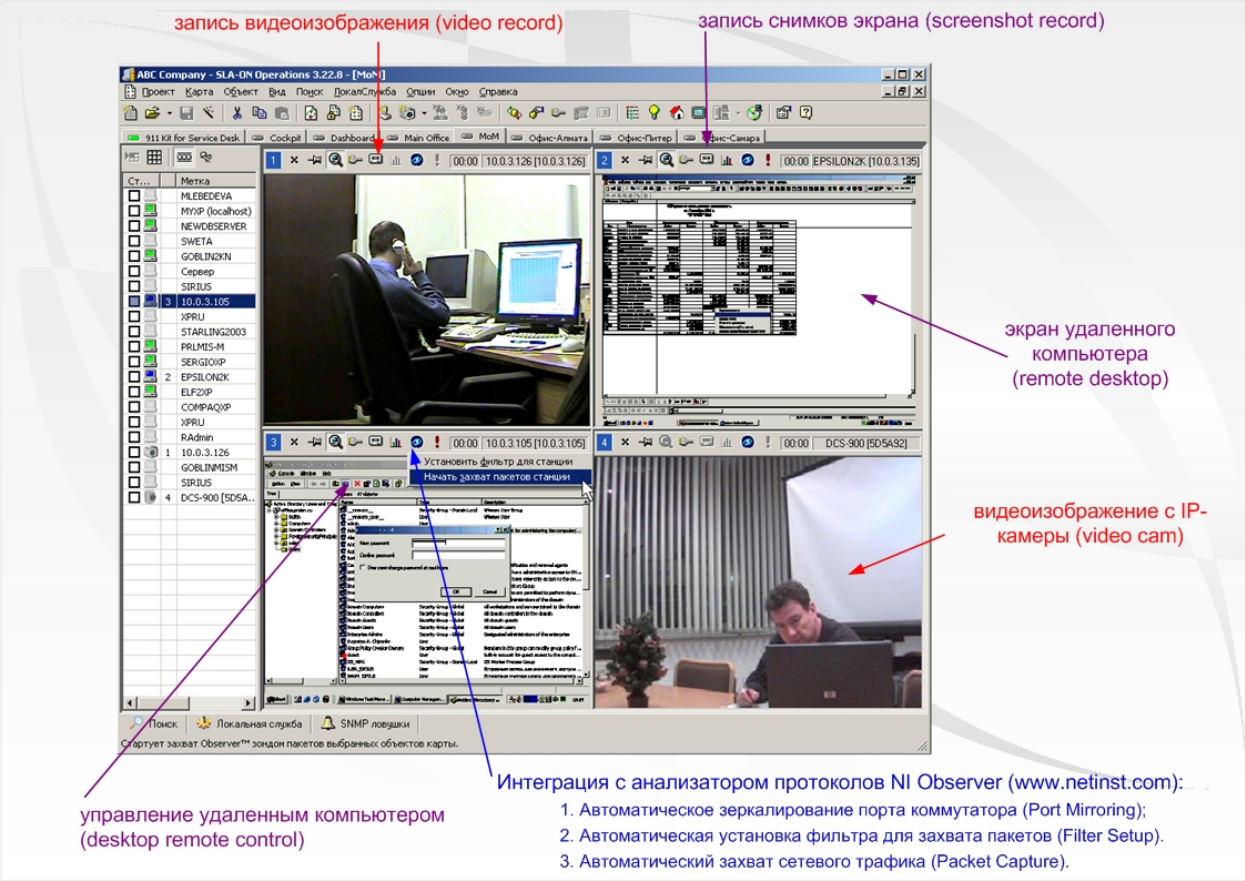

Рисунок 2. Окно MOM (Monitor of Monitors) приложения SLA-ON Operations, входящего в состав всех продуктов семейства ProLAN SLA-ON.

Приложение SLA-ON Operations позволяет устанавливать соответствие между компьютерами пользователей и установленными в сети видеокамерами, поэтому, обнаружив подозрительное содержимое какого-либо экрана, офицер может быстро определить – кто именно работает с представляющим угрозу приложением. Обнаружив подозрительное поведение какого-либо пользователя, офицер может быстро определить, – с каким приложением он сейчас работает, и что именно сейчас делает.

Обнаружив что-либо подозрительное в действиях пользователя, офицер может, во-первых, начать запись на диск снимков экрана его компьютера, во-вторых, начать запись видеоизображений с соответствующих видеокамер, в-третьих, начать контролировать и/или записывать весь сетевой трафик, создаваемый этим пользователем. Снимки экрана и видеоизображения сохраняются с помощью приложения SLA-ON Operations. Для сохранения и анализа сетевого трафика используется анализатор сетевых протоколов Observer компании Network Instruments, консоль которого должна быть установлена на компьютере офицера службы безопасности (зонды могут быть установлены на других компьютерах сети).

Для захвата и/или анализа сетевого трафика любого пользователя, экран которого отображается приложением SLA-ON Operations, офицеру достаточно кликнуть на пиктограмму с изображение глаза, расположенную над маленьким окошком, в котором отображается экран этого пользователя (смотри рисунок 2). Приложение SLA-ON Operations интегрировано с анализатором протоколов Observer, поэтому все операции (установка фильтра, захват трафика и т.д.) выполняются автоматически.

Ручной **Т- Контроль** поддерживается любым продуктом семейства ProLAN SLA-ON, в частности, младшей моделью – программным пакетом ProLAN-Супервайзер. Основное достоинство ручного **Т- Контроля** – простота внедрения и экономичность. Основное ограничение – выявление подозрительной активности пользователей должно производиться вручную.

Автоматический Т- Контроль

Автоматический Т- Контроль отличается тем, что выявление подозрительной активности пользователей делается автоматически, а не вручную (офицером службы безопасности). Для этого используется специальная технология компании ProLAN, которая называется 911 Help. Эта технология заключается в следующем.

На зонде SLA-ON Probe, установленном в любом месте сети, непрерывно выполняется оценочный тест (специальная программа на языке VBScript), который автоматически выявляет аномальную (не типичную) работу сети. Это может быть, например, аномальный сетевой трафик, попытка сканирования портов сетевого устройства, запуск пользователем запрещенного приложения, несанкционированное подключение к компьютеру пользователя записывающего устройства и т.п.

Обнаружив какую-либо аномалию в работе сети, тест автоматически выполняет следующие действия. Во-первых, автоматически определяет IP-адрес компьютера, который является причиной аномалии. Во-вторых, автоматически выводит на консоль офицера службы безопасности содержимое экрана этого компьютера (являющегося причиной аномалии). В-третьих, если это задано, выполняет различные управляющие воздействия, например, отключает компьютер подозрительного пользователя от сети или даже выключает его компьютер.

Для организации автоматического **Т- Контроля,** в большинстве случаев, необходима предварительная настройка оценочного теста под конкретную топологию и/или архитектуру сети. О технологии автоматического определения сетевых аномалий можно прочесть в описании решения ProDefense.

Автоматический **Т- Контроль** поддерживается только старшими моделями продуктов семейства ProLAN SLA-ON. Основное достоинство автоматического **Т- Контроля** – быстрота выявления злонамеренных действий внутренних пользователей и возможность быстро предпринимать адекватные защитные действия. Зонд SLA-ON Probe, поддерживающий технологию 911 Help, входит в состав старших моделей продуктов семейства ProLAN SLA-ON, в частности в состав программного продукта ProLAN-Эксперт и аппаратно-программного комплекса ProLAN-Сервер.

- Демонстрационную версию анализатора сетевых протоколов Observer компании Network Instruments можно загрузить здесь.
- Демонстрационную версию программных пакетов ProLAN-Супервайзер и ProLAN-Администратор можно загрузить здесь.