Безопасность сети АСУ ТП

Контрольный список мер по обеспечению защиты сетей АСУ ТП

ARMA arma.infowatch.ru

1 Провести инвентаризацию устройств

Анализ и подробное описание состава и конфигурации устройств.

2 Провести инвентаризацию сервисов и служб

Неиспользуемые сервисы и службы необходимо отключить.

3 Проверить доступность конечных устройств в интернете

Использовать поисковую сеть Shodan.

4 Актуализировать сетевую схему

Схема должна быть прозрачной для сотрудников, занимающихся поддержкой технических средств и администрированием. Детализация должна быть такой, чтобы сотрудники могли понимать, какие конечные устройства куда подключаются и с какой целью.

5 Сегментировать сеть

Корпоративные сети, сети АСУ ТП, сети, используемые для видеокамер, сети для принтеров, сети для СКУД и т. п. должны быть разделены на разные подсети.

6 Разработать проект по внедрению средств защиты информации

События безопасности должны централизованно обрабатываться (например, SIEM). Если ваше предприятие подпадает под требования №187-ФЗ или других, в проекте должны быть учтены соответствующие требования и меры.

7 Обеспечить внедрение СЗИ, может быть поэтапным

Установить и настроить СЗИ на границе промышленной сети. Настроить безопасное удалённое подключение для администрирования, внедрения СЗИ внутри АСУ ТП и т. п. для контроля промышленных протоколов и программируемых логических контроллеров.

Какие важные моменты необходимо учесть при настройке сетевого оборудования?

- [ ] Отключите неиспользуемые порты на сетевом оборудовании и разместите их на отдельный VLAN
- [ ] Ограничьте доступ к сетевым портам, разрешив только конкретным устройствам работать через них (самый простой способ — по MAC-адресу)
- [ ] Установите таймаут сессии
- [ ] Отключите Telnet для администрирования, ограничьте адрес для администрирования, сконфигурируйте SSH
- [ ] Убедитесь, что удалённый доступ извне компании (при крайней необходимости) доступен только с использованием VPN и авторизации
- [ ] Используйте SNMPv3
- [ ] Включите журналирование событий
- [ ] Отключите неиспользуемые сервисы (dhcpd, http-server и т. д.)

Какие важные моменты необходимо учесть при настройке межсетевых экранов?

- [ ] Создайте главную настройку: «белый список» — запрещено всё, что явно не разрешено
- [ ] Заблокируйте транзитную передачу данных из сети системы управления в корпоративную сеть. Все пересылки должны заканчиваться в DMZ. Лучше всего, если любой протокол, разрешённый между АСУ ТП и DMZ, не будет разрешён между DMZ и корпоративной сетью
- [ ] Убедитесь, что сети систем управления не подключены напрямую к интернету — даже через канал связи, защищённый с помощью МЭ
- [ ] С помощью DPI отключите неиспользуемые протоколы
- [ ] Убедитесь, что все разрешающие правила имеют конкретные IP-адреса и номера портов TCP / UDP и ограничивают трафик на определённый IP-адрес или диапазон адресов. Трафик должен быть описан по источникам передачи и иметь конкретного получателя с указанием используемого сервиса и сетевого порта