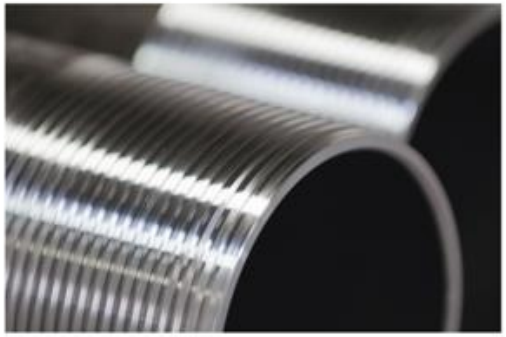
ТРУБНАЯ МЕТАЛЛУРГИЧЕСКАЯ КОМПАНИЯ



2020

ОСОБЕННОСТИ АУДИТА АСУТП

Подготовил: Севостьянов А.В.
Должность: Начальник Отдела защиты информации СЭБ

Город: Москва

Дата:15.07.20

Немного о проблемах и сложностях

При обследовании промышленных сетей необходимо учитывать следующее:

- они обеспечивают режим 24/7
- они могут быть сильно устаревшими в части железа и ПО
- они значительно распределены по локациям
- за их администрирование и сопровождение могут отвечать как работники ИТ, так и АСУ
- оборудование может находится на гарантийном обслуживании у поставщика
- ПО АСУ критично к малейшим сбоям по временным показателям передачи данных

Немного о нюансах

В процессе аудита следует учитывать следующее:

- не следует осуществлять сбор информации с работающего оборудования
- не следует проводить обследование в режиме удаленного доступа из-за ИТ-периметра Предприятия
- не следует запускать на ПК АСУ скрипты и ПО активного поиска «вредоносов» (типа Dr.web cureit)
- наиболее правильная тактика: выгрузка Log-файлов прикладного ПО и операционной системы на съемный носитель, с последующим их изучением вне среды АСУ
- не следует проводить классические пентесты («kali») на проникновение напрямую в ИТ-инфраструктуру сегмента АСУ (если только в период ППР)

Аудит чего?

Проверяем на соответствие:

I. корпоративным стандартам информационной и кибер-безопасности (правила и политики к моменту аудита должны быть утверждены и официально введены в действие; доведены до ответственных работников)
II. требованиям законодательства, т.е. 187-ФЗ (изначально, до проведения проверки, необходимо провести и завершить предусмотренное законом категорирование)

А также:

I. обязательно проверяем наличие влияния оборудования ИТ-сегментов Холдинговых подрядных Организаций на промышленные сети Предприятия, в случае аренды вычислительных мощностей!

Что проверяем? - 1

Организационный уровень:

- наличие ЛНА по безопасности промышленных сетей (есть или нет, а может пора обновлять)
- ознакомлен ли персонала АСУ с требованиями по информационной безопасности
- есть ли ответственные за безопасность АСУ
- ведется ли учет сбоев и простоев оборудования по причинам ИТ **(!)** – *возможно сокрытие фактов*
- имеется и используется инструмент расследования Инцидентов ИБ в сегменте АСУ (работает ли инцидент менеджмент) и скорость оповещения ИБ о событиях

Что проверяем? - 2

Прикладной уровень:

- физическая защищенность помещений АСУ: пультовые, серверные, шкафы и места хранения зап.частей ИТ-компонентов (охранная, пожарная сигнализации; СКУД и ВН; кондиционирование)
- визуальное состояние компьютерной техники (изолированное исполнение или нет)
- наличие актуальных версий ПО АСУ и ОС, а также прошивок PLC (патч-менеджмент), включая способ их установки (через съемные носители информации или через удаленный доступ к сайту производителя). Где и у кого диски с исходниками? ☺
- наличие постороннего (в т.ч. пиратского) ПО на ПК: игровой и развлекательный медиа- контент
- наличие и работоспособность антивирусных систем
- методы и способы разграничения сегментов сетей (АСУ от корпоративной) и соответствие сетевой безопасности
- наличие контроля съемных носителей информации
- наличие фактов подключений wifi и 3g модемов к ПК АСУ

Об ответственности

При наличии официально введённой нормативной документации по защите информации и доведенной до ответственных работников АСУ:

- **привлекаем к дисциплинарной ответственности за грубые нарушения политик информационной безопасности в ИТ-инфраструктуре промышленного сегмента!**

Спасибо за внимание!

WWW.TMK-GROUP.COM