Роль SOC при реализации концепции Zero Trust Architecture в АСУ ТП

Владимир Карантаев

Руководитель направления
«Кибербезопасность АСУ ТП»
Руководитель WG D2.51 CIGRE

Ростелеком
Солар

Предпосылки. Варианты решения

Увеличение поверхности атаки

- Изменение архитектурных принципов построения ИС, АСУ ТП. «От пирамиды к mesh-сети»
- Появление новых активных взаимодействующих субъектов, например, просьюмеры в электроэнергетике
- Возрастающее количество угроз, вызванных ростом количества уязвимостей в прикладном и общесистемном ПО
- Развитие методов атак: преодоление периметра/компрометация периметровой защиты
- Применение технологий, уязвимых перед компьютерными атаками. Унификация и COST
  - ИКТ
  - Виртуализация/использование гипервизоров на ПЛК несколько операционных систем
  - Мультиагентные системы

Реализация политики ZeroTrust

- **Сегодня.** Уменьшение поверхности атаки до максимально достижимого
- **Завтра.** В пределе переход к архитектуре с нулевым доверием

Реальность vs теория

Вам приходилось слышать?

- У нас есть периметр безопасности в АСУ ТП
- Проблемы внутреннего нарушителя - нет. У нас контролируемая зона
- **Одиозное:** наша (наши) АСУ ТП - это закрытая система. Это в век IIoT и SmartGrid!

А мы помним о?

- О подрядчиках, осуществляющих наладку и эксплуатацию
- О том, что самая большая проблема – эксплуатация (т. е. люди)
- О системах удаленного мониторинга чего-либо кем-либо (турбины, процессы)

«Отцы-основатели» ZTA

- От сети всегда исходит угроза. Весь сетевой трафик не доверенный, его происхождение и источник не важны
- Внутренние и внешние угрозы всегда присутствуют
- Внутренняя сеть не равно доверенная сеть
- Каждое устройство, пользователь, информационный поток должны быть идентифицированы и аутентифицированы

ZTA в АСУ ТП. Проще сказать, чем сделать

- Идентификация и аутентификация всех типов объектов и субъектов доступа: физические и логические сущности
  - Идентификация и аутентификация M2M-взаимодействий. PLC, IED, PACS и т.д.
  - Идентификация и аутентификация H2M-взаимодействий
  - Идентификация и аутентификация приложений
- Точечное назначение привилегий; должен быть внедрен принцип наименьших привилегий
- IdM и мониторинг того, что делается с этими привилегиями
- Применение криптографических методов защиты всех видов сетевого трафика (не обязательно шифрование)
- Удаленная «аттестация» платформ в процессе взаимодействия: ПЛК, ПАЗ, РЗА и т.д.
- Харденинг устройств верхнего уровня АСУ ТП
- Реализация и использование комплекса встроенных механизмов защиты в устройства среднего и нижнего уровней

ZTA в АСУ ТП. Проще сказать, чем сделать.

- Все данные должны быть защищены вне зависимости от местоположения
  - При передаче
  - При хранении
  - Ну вы поняли … :)
- Осуществлена классификация обрабатываемой информации
  - Выявлены все информационные потоки
  - Предъявлены требования по обеспечению свойств информации
  - Целевые уровни безопасности
- Собираем и анализируем логи
  - Доверяем, но проверяем. Точно?
  - Проверяем и никогда не доверяем! Может, так?
- Реализуем политику Default Deny.
  - Разрешаем проходить трафику только известных и идентифицированных сервисов.
- Реализация доверенной вычислительной среды на основе стойких отечественных криптографических методов.

Роль SOC при реализации концепции Zero Trust Architecture в АСУ ТП

На всех этапах стремимся к реализации политики нулевого доверия!

Роль SOC при реализации концепции Zero Trust Architecture в АСУ ТП

Владимир Карантаев

Руководитель направления
«Кибербезопасность АСУ ТП»
Руководитель WG D2.51 CIGRE

Ростелеком
Солар