Комплексный анализ защищенности АСУ ТП и IIoT-систем

Выявление недостатков в защите АСУ ТП и IIoT-систем, оценка возможных последствий их эксплуатации и рекомендации для повышения уровня защищенности

rt-solar.ru

rt.ru

Ростелеком
Солар

Проблематика

Для эффективного выявления и предотвращения угроз необходима полная и актуальная информация о реальной защищенности инфраструктуры. Слабая осведомленность о недостатках системы безопасности повышает вероятность успешных кибератак, что в свою очередь грозит серьезными последствиями — такими как финансовые потери от остановки производства, репутационный ущерб, претензии регуляторов и т.д.

Ситуацию усугубляет ряд других факторов:

- Развитие инструментария и методик проникновения
- Появление зловредного ПО, специально разработанного для взлома промышленных систем
- Рост зависимости от уязвимых ИТ-технологий, хорошо изученных злоумышленниками
- Увеличение связанности технологических сетей с корпоративными и сетями общего пользования
- Рост использования удаленного управления
- Использование необновляемых операционных систем

72%

обнаруженных уязвимостей АСУ ТП — высокого и критического уровней

7 дней

уходит в среднем на успешный взлом большинства промышленных систем

90%+

промышленных систем взламываются с получением критического доступа к АСУ ТП

Данные: «Лаборатория кибербезопасности АСУ ТП» («Ростелеком-Солар», 2019) и Fortinet, 2018

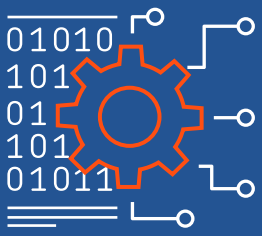
Государственное регулирование

Защита АСУ ТП и IIoT — вопрос, вызывающий обеспокоенность на самом высоком государственном уровне. Структура нормативно-правового регулирования включает следующие документы:

- **Доктрина информационной безопасности Российской Федерации:** указ Президента РФ № 646
- **ФЗ № 187-ФЗ** «О безопасности критической информационной инфраструктуры Российской Федерации»
- **ФЗ № 194-ФЗ** «О внесении изменений в Уголовный кодекс Российской Федерации...»
- **ФЗ № 193-ФЗ** «О внесении изменений в отдельные законодательные акты...»
- **Приказ ФСТЭК России № 239 от 25.12.2017** «Об утверждении Требований по обеспечению безопасности значимых объектов критической инфраструктуры Российской Федерации (в редакции Приказа ФСТЭК России от 26 марта 2019 г. **№ 60**)»
- **Приказ ФСТЭК России № 31 от 14.03.2014** «Об утверждении Требований к обеспечению защиты информации в АСУ ТП»
- **Методический документ** «Методика выявления уязвимостей и недекларированных возможностей в программном обеспечении», **ФСТЭК России, 2019 г.**

За несоблюдение требований законодательства Российской Федерации грозит административная и даже уголовная ответственность.

Уникальность



«Лаборатория кибербезопасности АСУ ТП» — это корпоративный центр компетенций для сбора, систематизации, распространения, приумножения знаний и лучших практик по обеспечению кибербезопасности систем промышленной автоматизации. Эксперты компании обладают реальным опытом разработки и внедрения проектов по защите АСУ ТП и являются одними из лидеров в рейтинге исследователей БДУ ФСТЭК России.

Решение

«Лаборатория кибербезопасности АСУ ТП» компании «Ростелеком-Солар» проводит комплексный анализ защищенности, позволяющий выявить максимальное число уязвимостей и недостатков, ставящих под угрозу деятельность компании.

Комплексная оценка реальной защищенности

Оценка возможных последствий эксплуатации уязвимостей

Рекомендации по совершенствованию защиты

По желанию заказчика может проводиться обследование и актуализация состава исследуемых АСУ ТП и IIoT-систем, сетей связи, вспомогательных систем и др. Глубина и детализация анализа защищенности отдельных компонентов исследуемых систем обговаривается отдельно и обычно зависит от возможности инструментального воздействия на исследуемый компонент.

Для того, чтобы выявить наиболее критические слабости инфраструктуры, позволяющие реализовать конкретные сценарии проникновения, рекомендуется проводить тестирование на проникновение. Комплексный анализ дает наиболее полную картину защищенности, в том числе неизвестных или плохо изученных систем.

Ключевые особенности

Выявление недостатков конфигурации оборудования и программного обеспечения

Определение возможных сценариев атак

Выявление недостатков в применяемых мерах информационной безопасности

- Комплексная и индивидуальная оценка защищенности по каждому компоненту АСУ ТП и IIoT-системы и вспомогательным системам
- Рекомендации по устранению недостатков, ошибок конфигурации или выявленных уязвимостей
- Команда с опытом проведения комплексного анализа защищенности с 2012 года в крупных промышленных холдингах и отдельных предприятиях различных отраслей

«Ростелеком-Солар» оказывает методическую помощь в организации процессов работы с уязвимостями и гармоничного встраивания услуги в процессы разработки безопасного ПО.

Что получает заказчик

Инвентаризация и актуализация системы и сетей

Выявление воздействий на системы

Выявление ошибок конфигураций и уязвимостей

Выявление недостатков мер ИБ и их оценка

Формирование сценариев возможных атак

Инструментальный анализ выбранных компонентов

Структура отчета

- Общее описание исследуемой системы, компонентного состава и хода работ
- Описание сетевого взаимодействия компонентов исследуемой системы друг с другом и внешними системами
- Описание локального взаимодействия программных компонентов, уязвимостей и ошибок конфигурирования компонентов
- Описание сценариев возможных атак
- Рекомендации по повышению уровня защищенности
- Общий вывод о защищенности на текущий момент и после исправления недостатков

Узнать подробнее или заказать услугу presale@rt-solar.ru

Услуги «Ростелеком-Солар»

− Кибербезопасность АСУ ТП

Приведение организации в соответствие с требованиями 187-ФЗ «О безопасности КИИ РФ»	Подключение к сервисам Solar JSOC для АСУ ТП
Выявление уязвимостей и НДВ в компонентах АСУ ТП и IIoT	Построение киберзащищенных АСУ ТП
Проведение киберучений	
Тестирование на проникновение АСУ ТП	Комплексный анализ защищенности АСУ ТП

+ Интеграционные услуги

+ Соответствие требованиям

О компании

«Ростелеком-Солар», компания группы ПАО «Ростелеком», — национальный провайдер сервисов и технологий для защиты информационных активов, целевого мониторинга и управления информационной безопасностью.

В основе наших технологий лежит понимание, что настоящая информационная безопасность возможна только через непрерывный мониторинг и удобное управление системами ИБ. Этот принцип реализован в продуктах и сервисах «Ростелеком-Солар».

Ростелеком Солар

info@rt-solar.ru rt.ru rt-solar.ru

+7 (499) 755-07-70

S.9.10.BR.ICS.SA.01