Тестирование на проникновение для АСУ ТП и IIoT-систем

Исследование АСУ ТП и IIoT-систем для обнаружения возможных путей получения несанкционированного доступа и оказания нежелательных воздействий

rt-solar.ru

rt.ru

Ростелеком
Солар

Проблематика

АСУ ТП и системы промышленного интернета уязвимы перед атаками. Внешние и внутренние нарушители не только успешно внедряют зловредное ПО, но и монетизируют атаки на промышленный сектор — например, захватывают инфраструктуру и выдвигают требования по ее выкупу или выводят предприятия из строя по заказу конкурентов или геополитическим мотивам.

Анализ компонентов АСУ ТП показывает, что наиболее часто встречаются следующие типы уязвимостей:

Управление доступом (28%): проблемы с аутентификацией и авторизацией

Инъекции (17%): от XSS-инъекций в веб-интерфейсах до внедрения исполняемого кода с повышенными привилегиями

Разглашение информации (22%): например, хранение учетных данных в открытом виде

Криптография (15%): некорректная реализация применения методов криптографической защиты

90%+

промышленных систем взламываются с получением критического доступа к АСУ ТП

7 дней

уходит в среднем на успешный взлом большинства промышленных систем

700+

уязвимостей выявлено в компонентах АСУ ТП и IIoT-систем за 2017–2018 гг.

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

Проблемы защищенности АСУ ТП и IIoT-систем

Предприятия

- Недостаточная осведомленность о возможностях преступников по взлому АСУ ТП и IIoT-систем на всех уровнях организации
- Распространенность устаревших небезопасных технологий
- Слабый контроль доступа: во многих организациях зачастую используются ненадежные или установленные по умолчанию пароли
- Использование уже снятых с поддержки и необновляемых операционных систем

Технологии

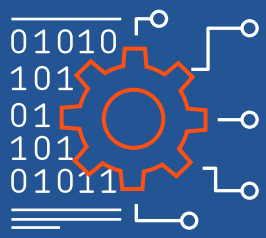
- Использование известных преступникам ИТ-технологий (стек протоколов TCP/IP)
- Постоянный рост сложности и связанности технологических и корпоративных сетей
- Массовое использование удаленного доступа
- Более активное внедрение автоматизированных систем управления производством, систем аналитики, улучшения качества и т. д.

Злоумышленники

- Развитие методик проникновения и инструментария, в том числе специализированного
- Появление вредоносного ПО, направленного на эксплуатацию уязвимостей в программном обеспечении и оборудовании известных производителей промышленных систем
- Появление у киберпреступников успешных способов монетизации взломов индустриальных систем управления

В соответствии с приказом № 239 ФСТЭК тестирование на проникновение в условиях, соответствующих возможностям нарушителей и определенных в модели угроз безопасности информации, является одной из мер повышения защищенности значимых объектов КИИ.

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» предлагает услуги по оценке возможности и тестированию на проникновение для обнаружения, имитации и, при желании заказчика, демонстрации на практике сценариев, приводящих к несанкционированному доступу и другим нежелательным последствиям в исследуемых АСУ ТП и IIoT-системах.

Варианты проведения

Из вспомогательных и гостевых сетей

Внешний злоумышленник без специального доступа

Из корпоративных сетей, связанных с технологическими

Внутренний злоумышленник с легитимным доступом к **корпоративной** сети

Внешний злоумышленник: нелегитимный доступ к **корпоративной** сети

Из сегмента технологической сети

Внутренний злоумышленник с легитимным доступом к **технологической** сети

Внешний злоумышленник: нелегитимный доступ к **технологической** сети

Ключевые особенности

Возможность трезво оценить реальный риск взлома и нежелательные последствия атаки

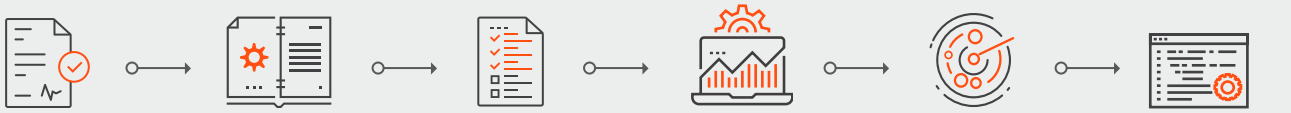
Результаты тестирования — аргумент в дискуссии о выделении бюджета на обеспечение информационной безопасности

Цель тестирования — выявить наиболее критические слабости инфраструктуры, позволяющие реализовать конкретные сценарии проникновения

- Команда экспертов, которую из года в год высоко оценивают крупные промышленные производители программных и аппаратных продуктов
- Команда экспертов с опытом проведения тестирований АСУ ТП с 2012 года в крупных холдингах и предприятиях нефтегазовой отрасли, электроэнергетики, тяжелой промышленности и др.
- Для более полной картины защищенности, в том числе неизвестных или плохо изученных систем, рекомендуется проводить комплексный анализ защищенности или лабораторные исследования компонентов рассматриваемых систем

Эксперты «Лаборатории» могут использовать как методы «серого», так и «белого ящика»: заранее обследуют инфраструктуру и собирают данные, оценивают защищенность, выстраивают векторы атак и согласуют варианты реальной демонстрации или имитации атак.

Этапы работы



Подписание договора о неразглашении → Подготовка ТЗ и подписание договора → Подготовка плана проведения работ → Сбор информации и конфигураций → Оценка или тестирование на проникновение → Подготовка отчета о найденных уязвимостях

Структура отчета

- Общие выводы о защищенности исследуемой системы
- Описание исследуемой системы, сетей и вероятных сценариев атаки
- Результаты проведения работ
- Список выявленных ошибок настроек сетевого оборудования и средств защиты
- Перечень уязвимостей компонентов АСУ ТП и IIoT-систем
- Список ошибок конфигураций ПО и оборудования АСУ ТП и IIoT-систем
- Рекомендации по повышению уровня защищенности

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.PEN.01