Выявление уязвимостей
и недостатков в системе
безопасности АСУ ТП

Kaspersky ICS Security Assessment

kaspersky АКТИВИРУЙ БУДУЩЕЕ

Сервис анализа защищенности АСУ ТП

Позволяет получить информацию об уязвимостях АСУ ТП, понять возможные последствия их эксплуатации, оценить эффективность используемых средств безопасности и запланировать дальнейшие действия для исправления обнаруженных недостатков и усиления защиты.

Анализ защищенности АСУ ТП

Долгое время стандартом защищенности АСУ ТП считалась их функциональная безопасность, то есть тот уровень надежности, который позволял избежать аварий на производстве, человеческих жертв и загрязнения окружающей среды. В рамках информационной безопасности основное внимание уделялось изоляции сетей и защите от физических воздействий. Однако в последние годы в промышленном оборудовании появляется все больше уязвимостей, а число вредоносных программ и целенаправленных атак на АСУ ТП растет, при этом все чаще возникает потребность в интеграции промышленных сетей передачи данных с корпоративными системами (например, с ERP). В этих условиях предприятиям следует пересмотреть свои подходы к защите производственных систем. Так или иначе, информационная безопасность АСУ ТП тесно связана с их функциональной безопасностью: успешная хакерская атака может привести к аварии на производстве.

Результаты анализа защищенности АСУ ТП

Сервис оценки защищенности АСУ ТП позволит обнаружить следующие уязвимости, используемые злоумышленником для получения несанкционированного доступа к критически важным компонентам промышленной сети:

- Уязвимости, вызванные использованием устаревших версий оборудования и ПО без установленных обновлений безопасности
- Уязвимости взаимодействия анализируемых компонентов АСУ ТП с другими системами (например, через систему управления производством – MES)
- Недостаточно строгая политика аутентификации и авторизации в различных службах (ненадежные пароли, предоставление пользователям слишком высоких полномочий и т.д.)
- Недостатки конфигурации промышленного и сетевого оборудования, в том числе несоответствие стандартам безопасности и невыполнение рекомендаций производителей
- Уязвимая архитектура сети, недостаточно защищенная сеть (в том числе ошибки при ограничении доступа к сети АСУ ТП)
- Уязвимости, вызванные ошибками в работе приложений (внедрение произвольного кода, обход каталога, внедрение операторов SQL и т. д.)
- Уязвимости в компонентах АСУ ТП (распределенной системе управления, системе противоаварийной защиты, программируемых контроллерах, интеллектуальных счетчиках и т. д.)
- Уязвимости, делающие возможным перехват и перенаправление сетевого трафика (в том числе в промышленных коммуникационных протоколах)
- Недостаточный уровень физической защиты оборудования АСУ ТП
- Раскрытие информации

Многоуровневая система защиты

Сервис анализа защищенности АСУ ТП призван выявить недостатки системы безопасности вашей АСУ ТП на всех уровнях: начиная с физической и сетевой безопасности и заканчивая уязвимостями в компонентах для АСУ ТП от различных производителей, например в системах диспетчерского контроля и сбора данных (SCADA) и программируемых логических контроллерах (ПЛК).

Зачем это нужно

Сервис анализа защищенности АСУ ТП помогает предприятиям:

Избежать человеческих жертв, неблагоприятного влияния на окружающую среду, финансовых, операционных и репутационных потерь в результате успешной атаки за счет своевременного обнаружения и устранения уязвимостей, которыми могут воспользоваться злоумышленники

Найти слабые звенья в функционировании АСУ ТП и повысить эффективность соответствующих процессов информационной безопасности

Проанализировать соответствие АСУ ТП отраслевым и региональным стандартам безопасности, например NERC CIP, NIST, IEC 62443 и т.д.

Выполнять требования государственных, отраслевых и внутрикорпоративных стандартов, требующих проведения анализа защищенности

Что мы проверяем

Эксперты «Лаборатории Касперского» могут протестировать АСУ ТП любого производителя, независимо от сектора промышленности. Производство и передача электроэнергии, транспортные системы, производство нефтепродуктов, добыча полезных ископаемых — вот лишь некоторые из поддерживаемых нами отраслей.

Методы анализа защищенности и их комбинации подбираются исходя из ваших потребностей и особенностей инфраструктуры.

Тестирование на проникновение

Метод анализа защищенности путем имитации действий злоумышленников, стремящихся расширить свои права и проникнуть в производственную среду. Вы сами выбираете векторы атаки для тестирования.

Анализ защищенности инфраструктуры АСУ ТП

Анализ защищенности методом «белого ящика», в ходе которого наши эксперты изучат имеющуюся техническую документацию для используемых промышленных систем, проведут интервьюирование специалистов, обслуживающих АСУ ТП, проанализируют текущие промышленные системы и протоколы и проведут комплексный технологический аудит компонентов АСУ ТП в производственной среде.

Анализ защищенности решений для АСУ ТП

Углубленный анализ безопасности и поиск уязвимостей нулевого дня в программных и аппаратных компонентах АСУ ТП на тестовом стенде с последующим выполнением заранее согласованных тестов на функционирующих системах.

Команда проекта

Это опытные специалисты, решающие практические проблемы безопасности, обладающие глубокими познаниями в этой области и постоянно совершенствующие свои навыки. На их счету уже множество успешно выполненных проектов по исследованию безопасности АСУ ТП.

Подробный отчет

По завершении анализа защищенности вы получите отчет с подробной технической информацией о ходе тестирования, его результатах и обнаруженных недостатках информационной безопасности. В отчете будут приведены рекомендации и четкий краткий итог, содержащий наши заключения по результатам тестирования и наглядное описание сценариев атак, типичных для вашей отрасли. При необходимости мы можем также подготовить видеоматериалы и презентации для технических подразделений и руководства.

Как мы это делаем

Работы проводят эксперты «Лаборатории Касперского» по информационной безопасности, которые соблюдают все требования к конфиденциальности, целостности и доступности ваших систем. Мы строго придерживаемся международных стандартов и следуем лучшим мировым методикам.

Методики и стандарты анализа

Выполняя анализ защищенности АСУ ТП, «Лаборатория Касперского» руководствуется следующими международными стандартами и принятыми в отрасли методиками:

- Стандарт проведения испытаний на проникновение (PTES)
- Методическое руководство по испытанию систем безопасности с открытым исходным кодом (OSSTMM)
- Техническое руководство по испытанию и оценке информационной безопасности (специальная публикация 800-115 института NIST)
- Классификация угроз, принятая консорциумом безопасности веб-приложений (WASC)
- Стандарты, разработанные Центром интернет-безопасности (CIS)
- Методика оценки безопасности информационных систем (ISSAF)
- Стандарт защиты критической инфраструктуры Североамериканской корпорации по обеспечению надежности электросистем (NERC CIP)
- Руководство по тестированию, разработанное в рамках открытого проекта по обеспечению безопасности веб-приложений (OWASP)
- Требования общей системы оценки уязвимостей (CVSS), а также другие стандарты в зависимости от рода деятельности вашей организации и ее расположения

Kaspersky ICS Security Assessment

Подробнее

www.kaspersky.ru

#kaspersky
#активируйбудущее