ЭКСПЕРТНЫЕ СЕРВИСЫ KASPERSKY INDUSTRIAL CYBERSECURITY: АНАЛИЗ ЗАЩИЩЕННОСТИ ПРОМЫШЛЕННЫХ СИСТЕМ

Kaspersky Industrial CyberSecurity — это решение, состоящее из специализированных технологий и услуг, призванное защитить промышленные системы на каждом уровне, не создавая перебоев в работе и не нарушая технологический процесс.

Чтобы помочь организациям в оценке уровня защищенности промышленных систем от атак на информационные системы и объекты производственной инфраструктуры, «Лаборатория Касперского» предлагает сервис анализа защищенности в рамках решения Kaspersky Industrial CyberSecurity. С его помощью предприятия могут узнать об наиболее уязвимых объектах в инфраструктуре и повысить уровень защиты промышленных систем в соответствии с полученными рекомендациями.

Уязвимости в промышленных средах

Уязвимость современных АСУ ТП перед кибератаками вызвана несколькими причинами. Во-первых, исторически разрастающаяся сетевая архитектура систем, состоящая, как правило, из гетерогенных устройств, усложняет техническую поддержку и процедуру установки актуальных обновлений. Политики и правила использования далеко не всегда обеспечивают необходимый уровень безопасности, поскольку требуется обеспечить высокий уровень непрерывности функционирования системы и управления технологическими процессами. Слабый контроль доступа к интерфейсу критически важных систем может иметь катастрофические последствия.

Вторая причина заключается в коренном отличии между типовыми сценариями использования похожих решений в традиционной IT-среде и промышленной инфраструктуре. Прежде всего, для промышленных предприятий важна непрерывность работы, поэтому иногда системы функционируют без установки обновлений для критически важных уязвимостей, поскольку остановить работу АСУ ТП даже на короткое время невозможно. Вместе с этим АСУ ТП могут пострадать не только от уязвимостей в обычном ПО, но и в специализированном ПО для АСУ ТП. Злоумышленники могут использовать такие, часто встречающиеся для специализированных программ уязвимости, как переполнение буфера, использование небезопасных протоколов, содержащиеся в коде пароли и ключи, упрощенная процедура авторизации и т. п.

Кроме того, традиционные IT-системы чаще тестируются с большей внимательностью (так как они чаще подвержены атакам извне, в том числе из интернета), нежели АСУ ТП, где нет необходимости постоянного соединения с интернетом.

Комбинация этих и многих других факторов делает каждую АСУ ТП по-своему уникальной. Чтобы обеспечить безопасность АСУ ТП, необходим современный и методологически точный подход к выявлению потенциальных уязвимостей и угроз.

KASPERSKY lab

Цели сервиса:

- Независимая оценка текущего уровня защищенности информации, обрабатываемой в АСУ ТП.
- Независимая оценка устойчивости систем и приложений к наиболее распространенным видам внешних атак.
- Независимая оценка соответствия АСУ ТП требованиям нормативных документов (в частности, приказу ФСТЭК № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах...»).
- Развитие системы управления информационной безопасностью и подготовка рекомендаций по реализации комплекса мер, направленных на повышение уровня защищенности АСУ ТП.

Для достижения поставленных целей в ходе проведения работ решаются следующие задачи:

- Идентификация объектов защиты и оценка критичности АСУ ТП объектов защиты.
- Обследование выбранных объектов защиты.
- Построение частной модели угроз, включающую модель злоумышленника для АСУ ТП.
- Аудит безопасности АСУ ТП на основании анализа организационно-технической документации, документации, относящейся к ИБ, интервьюирования ответственного персонала, анализа конфигурации АСУ ТП, анализа используемого системного и прикладного ПО на компонентах объекта защиты и т. д.
- Аудит безопасности подключений сети АСУ ТП к другим информационным системам.
- Проведение инструментального тестирования на проникновение в АСУ ТП.
- Разработка организационно-технических рекомендаций по повышению уровня ИБ и развитию системы управления информационной безопасностью на основании проведенного тестирования на проникновение.

Услуги «Лаборатории Касперского» по анализу защищенности

Этап 1. Сбор информации и анализ документации

На первоначальном этапе осуществляется анализ необходимой документации по объектам защиты. В рамках данного этапа создается частная модель угроз, включающая модель злоумышленника, на основании внутренней методики построения модели угроз и с учетом требования используемых отраслевых стандартов.

В случае если в производственную инфраструктуру входят несколько объектов защиты, то определяются необходимые критерии и методика отбора объектов защиты для проведения анализа защищенности. При выборе критериев учитываются такие факторы, как:

- масштаб возможного ущерба от нарушения штатного режима функционирования АСУ ТП или несанкционированного вмешательства в процессы функционирования АСУ ТП;
- возможный ущерб от кибератаки на объект производственной инфраструктуры, учитывающий прямой финансовый ущерб, а также прямые и косвенные потери от простоя объекта, включая репутационные потери.

Полученные критерии позволяют выявить наиболее критичные объекты защиты среди всех объектов производственной инфраструктуры.

По итогам этапа вы получаете:

- план проведения обследования АСУ ТП;
- частную модель угроз АСУ ТП.

Этап 2. Очное обследование объекта защиты

В рамках данного этапа производится очное обследование объектов защиты с целью выявления потенциальных изъянов в ИБ АСУ ТП.

По итогам этапа вы получаете:

- уточнения и дополнения в частной модели угроз АСУ ТП;
- описание объектов АСУ ТП;
- описание взаимодействия объектов АСУ ТП с другими информационными системами или сетями;
- принятые организационно-технические меры по обеспечению ИБ АСУ ТП;
- состав используемых средств защиты информации.

Этап 3. Аудит безопасности подключений сети АСУ ТП к другим информационным системам

На этом этапе производится получение и анализ конфигураций активного сетевого оборудования и сетевых экранов, получение и анализ конфигураций АРМ операторов и инженеров АСУ ТП, инструментальная проверка ошибок конфигурации активного сетевого оборудования и сетевых экранов. Для подтверждения уязвимостей эксперты KICS проводят инструментальную проверку ошибок конфигурации.

По итогам этапа вы получаете:

- актуальный перечень сетевых маршрутов между сетями АСУ ТП и внешними сетями;
- актуальный перечень используемых сетевых протоколов в сети АСУ ТП и при взаимодействии с внешними сетями;
- информацию по актуальным уязвимостям в конфигурации сетевого оборудования и маршрутов сети АСУ ТП.

Эксперты KICS могут дополнительно провести поиск следов вредоносной активности в инфраструктуре (в том числе целенаправленных атак) и следов атак за пределами инфраструктуры.

Этап 4. Инструментальный аудит безопасности отдельных компонентов АСУ ТП

В рамках проведения инструментального аудита безопасности отдельных компонентов АСУ ТП эксперты «Лаборатории Касперского» осуществляют поиск слабых мест в системе безопасности, в том числе уязвимостей «нулевого дня» в компонентах АСУ ТП. На основании данного этапа работ разрабатываются рекомендации по минимизации потенциального ущерба от найденных уязвимостей до момента выпуска производителями официальных обновлений.

По итогам этапа вы получаете:

- перечень найденных слабых мест в системе безопасности и уязвимостей в исследуемых компонентах АСУ ТП с описанием эксплуатации;
- описание негативного воздействия на технологические процессы и потенциального ущерба в случае эксплуатации слабых мест в безопасности и найденных уязвимостей в исследуемых компонентах АСУ ТП;
- перечень рекомендаций по минимизации потенциального ущерба от найденных уязвимостей.

Этап 5. Проведение инструментального теста на проникновение и анализ защищенности АСУ ТП

Работы по проведению инструментального теста на проникновения в АСУ ТП осуществляются из смежных сетей или информационных систем. Работы проводятся в режиме «черного ящика».

Работы по анализу защищенности АСУ ТП позволят оценить возможности:

- несанкционированного воздействия на объекты автоматизации технологических процессов производства с целью вмешательства в алгоритмы их работы или вывода из строя;
- получения доступа к ПЛК, программному коду (проекту).

Целью данной стадии является выявление потенциально уязвимых компонентов инфраструктуры для различных типов злоумышленника. Эксперты «Лаборатории Касперского» осуществляют тестирование на проникновение, имитируя действия потенциальных нарушителей, с целью проверки возможности получения несанкционированного доступа к компонентам объектов защиты.

По итогам этапа вы получаете:

- описание и анализ уязвимостей, которые были выявлены в процессе анализа защищенности объектов защиты для различных типов злоумышленников;
- актуальные векторы атак на АСУ ТП;
- потенциальные сценарии несанкционированного воздействия на АСУ ТП со стороны различных типов злоумышленников;
- потенциальное влияние выявленных уязвимостей на АСУ ТП:

Этап 6. Оценка соответствия АСУ ТП требованиям приказа ФСТЭК России от 14 марта 2014 г. № 31

Целью данной стадии является получение независимой оценки соответствия АСУ ТП требованиям приказа ФСТЭК России от 14 марта 2014 г. № 31.

По итогам этапа вы получаете:

- анализ соответствия АСУ ТП требованиям Приказа ФСТЭК России от 14 марта 2014 г. № 31;
- рекомендации по развитию СУИБ и приведению в соответствие ИБ АСУ ТП с требованиями приказа ФСТЭК России от 14 марта 2014 г. № 31.

Этап 7. Разработка рекомендаций по составу и содержанию необходимых мер, направленных на повышение уровня защищенности объектов АСУ ТП

На заключительном этапе проводится экспертная оценка уровня обеспечения ИБ АСУ ТП и систематизация рекомендаций по повышению уровня ИБ АСУ ТП. Работы включают в себя:

- выработку первоочередных рекомендаций по составу мероприятий организационного уровня, внесению изменений и дополнений в существующие конфигурации и настройки программного и аппаратного обеспечения объектов защиты;
- определение перечня рекомендуемых средств зашиты информации, входящих в состав модернизированной (перспективной) СУИБ АСУ ТП;
- проведение презентации по результатам проведенных работ.

По итогам этапа вы получаете:

- результаты оценки соответствия ИБ АСУ ТП требованиям Приказа ФСТЭК России от 14 марта 2014 г. № 31;
- рекомендации по устранению выявленных несоответствий и недостатков обеспечения ИБ АСУ ТП, повышения уровня ИБ АСУ ТП и развития СУИБ.

Преимущества «Лаборатории Касперского»

«Лаборатория Касперского» — одна из немногих компаний, обладающих реальным опытом и знаниями в области защиты промышленных систем.

- Команда экспертов по кибербезопасности промышленных предприятий, которая специализируется на безопасности систем автоматизации.
- Более чем десятилетний опыт обнаружения и анализа комплексных сложных угроз и целевых атак, включая атаки на критичные объекты промышленной инфраструктуры.
- Уникальная методика поиска векторов атак, способных нарушить производственные процессы.
- Обширный практический опыт в расследовании компьютерных инцидентов и поиске уязвимостей нулевого дня.
- Практические и теоретические исследования в области защиты промышленных систем.

О решении

Kaspersky Industrial CyberSecurity — это всеобъемлющее решение, состоящее из сервисов и технологий, предназначенных для защиты от вредоносных программ и кибератак, обучения и повышения осведомленности, мониторинга промышленных сетей, реагирования на инциденты безопасности и многого другого. Таким образом, вы можете приобрести абсолютно все необходимые компоненты для защиты промышленных систем у одного поставщика.