kaspersky

Оценка безопасности архитектуры продукта

Проблема

Многие киберфизические системы, такие как блок управления системой автомобиля или промышленный контроллер, крайне сложно или вообще невозможно эффективно защитить от кибератак наложенными мерами защиты, если встроенных механизмов безопасности оказывается недостаточно. Требования безопасности к таким системам должны быть заложены на стадии проектирования и учтены в их архитектуре и при выборе технологических компонентов и их поставщиков на самых ранних этапах разработки.

Решение

Комплексная оценка безопасности архитектуры киберфизического продукта и используемых им низкоуровневых технологических компонентов, включая чипы и протоколы связи, а также приоритизированные рекомендации по необходимым встроенным механизмам защиты для минимизации рисков успешных атак на всем жизненном цикле продукта.

Для кого

Производители продуктов для АСУ ТП, интернета вещей, автоматизации транспорта и транспортной инфраструктуры, производители OEM-продуктов и разработчики технологических решений для разных отраслей, таких как производство, транспорт (включая железнодорожный, речной, морской и воздушный), медицинских систем, систем связи и так далее.

Проблематика

Как и любые функции продукта, механизмы информационной безопасности могут быть реализованы с ошибками или не реализованы вовсе. В киберфизических системах это несет риски для реального физического мира: потери управления оборудованием, транспортом, физическим доступом к объектам и т. д.

Исследования проблем безопасности киберфизических систем, в том числе систем промышленной автоматизации, решений классов «интернет вещей» и «промышленный интернет вещей», автомобильной техники, авионики и т. д., проводимые экспертами Kaspersky ICS CERT, показывают, что наиболее существенные и трудноустранимые уязвимости чаще всего обусловлены неверными архитектурными решениями и неоптимальным выбором технологических компонентов.

Дефекты архитектуры и реализации часто сложно исправить без глубоких изменений в продукте.

Уязвимости в технологических компонентах массовых коммерческих продуктов нередко становятся точкой входа в систему. Компрометация таких компонентов киберфизической системы фактически означает компрометацию доверенной среды управления физическим объектом (производственным комплексом, транспортным средством).

Наиболее часто и сильно на безопасность итогового решения влияют проблемы безопасности технологических компонентов следующих типов:

- программные компоненты с открытым исходным кодом;
- различные программные и аппаратные модули сторонних производителей (например, LTE/5G модемы, SoC и прочие чипы, их прошивки и микрокод);
- стандартные стеки протоколов, используемые в новых контекстах (например, беспроводные протоколы);
- специфические низкоуровневые протоколы передачи данных (промышленные и транспортные шины);
- среды разработки и выполнения программ автоматизированного управления технологическим процессом (статьи 1, 2, 3);
- стеки протоколов и интерфейсы, связывающие контроллеры, криптомодули, датчики и исполнительные устройства;
- телеметрические модули, модемы и шлюзы, обеспечивающие удаленный доступ;
- сервисное и диагностическое ПО, механизмы обновления и удаленной конфигурации.

Даже при использовании только собственного кода без внешних библиотек экспертная оценка архитектуры, алгоритмов и протоколов остается критически важной. Наиболее частая ошибка — монолитная архитектура без четкой декомпозиции на компоненты и домены безопасности и без контроля коммуникаций между ними. В случае уязвимости в одном из функциональных компонентов системы, например, удаленного исполнения кода, это может привести к полной компрометации функций продукта. Встречаются и другие ошибки — например, «домашняя» реализация алгоритмов криптографической защиты трафика в промышленных контроллерах не способна защитить не только данные, но и ключ, которым они зашифрованы.

Кроме того, в мире киберфизических систем при разработке даже самых современных продуктов часто приходится учитывать необходимость интеграции с устаревшими технологиями — в целях совместимости, для реализации интерфейсов взаимодействия с уже имеющимися системами. Как минимум, частично нейтрализовать угрозы безопасности, связанные с уязвимостями наследуемых технологий, можно за счет правильного выбора безопасных архитектурных решений.

Цифры и факты

Эксперты Kaspersky ICS CERT выявили более 400 уязвимостей нулевого дня в промышленных системах, системах IIoT/IoT и других типах решений.

Что мы предлагаем

Оценка безопасности архитектуры продукта — это комплексный консалтинговый проект, в рамках которого мы помогаем спроектировать или доработать архитектуру киберфизического продукта так, чтобы она надежно противостояла актуальным и возможным будущим угрозам и соответствовала при этом бизнес-целям, требованиям регуляторов и эксплуатационным ограничениям.

> Мы придерживаемся принципа, что усилия в сфере безопасности следует направлять в первую очередь на предупреждение угроз, а не на борьбу с уже реализованными угрозами. Такой подход позволяет оптимизировать затраты ресурсов на безопасность и снизить стоимость исправления ошибок в будущем.

Например, иногда достаточно изменить схему аутентификации пользователя или разделение ролей между компонентами, чтобы избежать необходимости сложной кастомной криптографии, где высок риск ошибок.

Как мы работаем

Формулируем цели и контекст безопасности

Совместно с клиентом определяем критичные функции и активы продукта, сценарии его применения, типовые и экстремальные режимы работы, внешние системы и пользователей (включая обслуживающий персонал, интеграторов, партнеров и регуляторов).

Строим и актуализируем модель угроз

На основании контекста и целей безопасности формируем модель угроз и нарушителей для продукта, учитывая:

- внешние и внутренние источники атак;
- сценарии компрометации через каналы связи, телеметрические модули, беспроводные подключения, диагностические интерфейсы, цепочку поставок;
- угрозы, связанные с компонентами сторонних производителей и открытым исходным кодом;

- особенности отрасли (производство, транспорт, энергетика, критическая инфраструктура и др.).

Анализируем архитектуру и поверхность атаки

Анализируем на нескольких уровнях:

- функциональная архитектура (основные подсистемы и их задачи);
- компонентная архитектура (ПО и аппаратные компоненты, модули, интерфейсы);
- диаграммы потоков данных для ключевых сценариев работы;
- внешние интерфейсы и протоколы взаимодействия (полевые шины, IP-сети, беспроводные каналы, облачные сервисы, мобильные приложения);
- внутренние протоколы взаимодействия компонентов (процессоры, криптомодули, контроллеры, датчики, исполнительные устройства).

На этом шаге мы описываем поверхность атаки, определяем потенциальные векторы атак и точки, через которые злоумышленник может повлиять на безопасность продукта — как напрямую, так и через смежные системы.

Выполняем композиционный анализ и анализ уязвимостей

На основе описанной архитектуры и выявленных векторов атак:

- анализируем используемые компоненты (библиотеки, прошивки, ОС, протоколы) по открытым источникам и базам уязвимостей;
- учитываем факторы цепочки поставок (версии, происхождение, доступность обновлений и исправлений);
- оцениваем устойчивость к модификации предустановленного ПО и вмешательству в аппаратные соединения (например, между процессором и модемом, между процессором и криптомодулем);
- рассматриваем уязвимости сервисного и диагностического ПО, процедур обновления и удаленного доступа.

Оцениваем риски и разрабатываем рекомендации

Для ключевых сценариев атак:

- потенциальный ущерб (для бизнеса, клиентов, безопасности людей и окружающей среды);
- осуществимость сценариев (наличие инструментов, необходимая квалификация атакующего, сложность доступа);
- совокупный риск (по методикам, применимым в отрасли и/или требованиям регуляторов, например методикам ФСТЭК России и ГОСТ Р ИСО 27005).

По результатам этих работ формируем:

- набор архитектурных паттернов и контрмер, устраняющих или существенно снижающих ключевые риски;
- предложения по изменению архитектуры, протоколов и политик взаимодействия с внешними системами, включая регламенты обновлений и диагностики;
- при необходимости — альтернативные варианты решений обнаруженных проблем ИБ с описанием плюсов и минусов, влияния на стоимость, сроки разработки и эксплуатационные характеристики продукта.

***

Мы применяем системный подход к моделированию угроз, чтобы заранее выявить все потенциально опасные сценарии атак на продукт. Каждый тип нарушения безопасности мы детально прорабатываем в конкретные угрозы, проверяя их на основе реальных инцидентов и известных атак.

При анализе угроз и оценке безопасности архитектуры мы учитываем широкий спектр факторов, влияющих на итоговый уровень защищенности:

- организацию цикла разработки у производителя;
- использование в продуктах стороннего кода и его происхождение;
- использование устаревших технологий для обратной совместимости;
- сетевые протоколы управления и обмена данными;
- необходимость удаленного доступа к функциям продукта;
- интерфейсы и сценарии доступа к другим системам;
- необходимость определенных гарантий в отношении функциональной безопасности, надежности, устойчивости решения;
- нефункциональные требования к продукту, такие как ресурсные ограничения и требования к производительности, гарантии свойств реального времени;
- технические аспекты доступа, например, для установки обновлений безопасности, использование решения в зонах с затрудненным доступом;
- применение продукта на предприятиях, где высока цена простоя и т. п.

На основе этого глубокого анализа мы разрабатываем рекомендации, основанные на лучших отраслевых практиках. Наша цель — предложить не просто точечные исправления, а архитектурные решения, которые комплексно повышают кибербезопасность, устойчивость, функциональную безопасность и общую надежность продукта.

Услуга может быть использована

- На начальном этапе разработки нового продукта.
- При планировании выпуска нового продукта или решения, призванного исправить недостатки предыдущих версий, в которых часто обнаруживались уязвимости — признак небезопасной архитектуры.
- На любой стадии, когда к продукту предъявляются новые требования по обеспечению кибербезопасности (со стороны регулятора, партнеров или рынка), либо после инцидентов в отрасли, которые повышают ожидания к уровню защищенности.

Результат

По итогам проекта клиент получает:

- Прикладную модель угроз, построенную с учетом целей безопасности для своего продукта и решения и описывающую векторы атак настолько подробно, насколько это имеет практический смысл и возможно с учетом имеющегося описания решения.
- Конкретные рекомендации по улучшению архитектуры безопасности, включая состав компонентов, способ и интерфейсы их взаимодействия, базовые технологии, фреймворки, протоколы взаимодействия.
- Четкие требования к ключевым компонентам безопасности, включая способы проверки и обеспечения их целостности и аутентичности.

Дополнительно мы обеспечиваем соответствие стандартам. Помогаем адаптировать модель угроз и рекомендации под требования конкретного регулятора или отраслевого стандарта.

- ФСТЭК, Роскомнадзор, ГОСТы
- IEC 62443: Security for operational technology in automation and control systems
- ISO/SAE 21434: Road vehicles — Cybersecurity Engineering
- UNECE WP.29: UN regulation for vehicle cybersecurity

Преимущества

1. Снижение финансовых и репутационных рисков за счет выявления и устранения критических уязвимостей до выхода продукта на рынок.
2. Соответствие отраслевым стандартам и требованиям регуляторов благодаря экспертной оценке, которая учитывает специфику индустрии клиента.

3. Оптимизация долгосрочных затрат на разработку и поддержку, так как инвестиции в безопасность на этапе проектирования многократно ниже затрат на последующие исправления и убытков от инцидентов.
4. Уверенность в устойчивости продукта к современным кибератакам, обеспеченная проработанной архитектурой, а не часто неполным набором сложно согласуемых разрозненных защитных функций.
5. Детализированная дорожная карта улучшений с практическими рекомендациями, которые легко интегрировать в процесс разработки.

Мы помогаем перестроить архитектуру продукта так, чтобы будущие угрозы были либо невозможны, либо необоснованно затратны для злоумышленников.

Запросить консультацию специалиста

Статьи по теме

- God Mode On: исследователи запустили Doom на головном устройстве автомобиля, удаленно атаковав его модем
- Исследование безопасности модема Cinterion EHS5 3G UMTS/HSPA
- Секреты протокола Schneider Electric UMAS
- Исследование безопасности OPC UA
- ISaPWN — исследование безопасности ISaGRAF Runtime
- Исследование безопасности: CODESYS Runtime — фреймворк для управления ПЛК. Часть 1
- Исследование безопасности: CODESYS Runtime — фреймворк для управления ПЛК. Часть 2
- Исследование безопасности: CODESYS Runtime — фреймворк для управления ПЛК. Часть 3
- Криптографические смертные грехи в защите ПЛК Modicon M100/M200/M221

Рекомендуем дополнительно

- Поток машиночитаемых данных об уязвимостях АСУ ТП
- Аналитика известных уязвимостей АСУ для принятия критически важных решений в части информационной безопасности
- Информация об уязвимостях и угрозах для АСУ ТП
- Расследование киберинцидентов на промышленных предприятиях

Запросить консультацию специалиста

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky ICS CERT) — глобальный проект «Лаборатории Касперского», направленный на координацию усилий производителей систем автоматизации, владельцев и операторов промышленных объектов, а также исследователей ИТ-безопасности для защиты промышленных предприятий от кибератак. Kaspersky ICS CERT направляет свои усилия в первую очередь на выявление потенциальных и существующих угроз, нацеленных на системы промышленной автоматизации и промышленный интернет вещей.

Kaspersky ICS CERT ics-cert@kaspersky.com