aprotech Kaspersky IoT company

KasperskyOS Операционная система

Кибериммунитет промышленных систем

Дмитрий Соколов

Архитектор по информационной безопасности «Лаборатории Касперского»

Сегодня промышленные системы все чаще становятся целями атак злоумышленников, которые стараются вмешаться в работу систем АСУ ТП и полевых устройств, чтобы вывести из строя промышленное оборудование или проникнуть внутрь закрытых контуров предприятия. Для компаний, которые эксплуатируют объекты критической информационной инфраструктуры (КИИ), эти риски являются неприемлемыми не только с точки зрения законодательства, но и с точки зрения сохранения бизнеса. Для решения этих проблем была придумана концепция кибериммунных систем, которые имеют устойчивость к атакам извне.

Принципы кибериммунности

Кибериммунитет — это подход к построению исходно безопасных (secure-by-design) ИТ-систем, которые обладают «встроенной» защитой от кибератак. Кибериммунная система способна противостоять кибератакам без использования дополнительных (наложенных) средств безопасности. Подавляющее большинство типов атак на кибериммунную систему неэффективно и не может повлиять на выполнение ею критических функций.

«Лаборатория Касперского» разработала кибериммунный подход к созданию IT-решений, а также собственную операционную систему KasperskyOS — платформу для разработки кибериммунных продуктов. Такие специализированные операционные системы не чувствительны к внешним воздействиям, поскольку содержат встроенные механизмы контроля и защиты внутренних процессов, а также всех коммуникаций. Функционал системы, построенной на базе кибериммунной ОС, ограничен набором только тех функций, которые были определены при их разработке. Для информационной системы предприятия можно выделить три области, где кибериммунные системы наиболее эффективны:

- **Сегментирование.** При применении кибериммунных решений наиболее важной задачей является выделение промышленных информационных систем в корпоративную сеть. Сегментирование позволяет локализовать вредоносные воздействия в отдельных сегментах и не допустить распространения вредоносного ПО по всей корпоративной сети предприятия. При этом защищенные сегменты промышленной сети могут работать по своим протоколам, отличным от IP.

- **Само устройство.** Наиболее эффективной защитой является использование кибериммунной операционной системы со встроенными механизмами защиты на борту самого интеллектуального устройства: станка, автомобиля, инфомата или удаленного АРМ. Сейчас российскими производителями ведется работа по созданию и внедрению подобных решений, поэтому в процессе импортозамещения оборудования и при строительстве нового производства рекомендуется отдавать предпочтение именно таким системам со встроенной защитой.

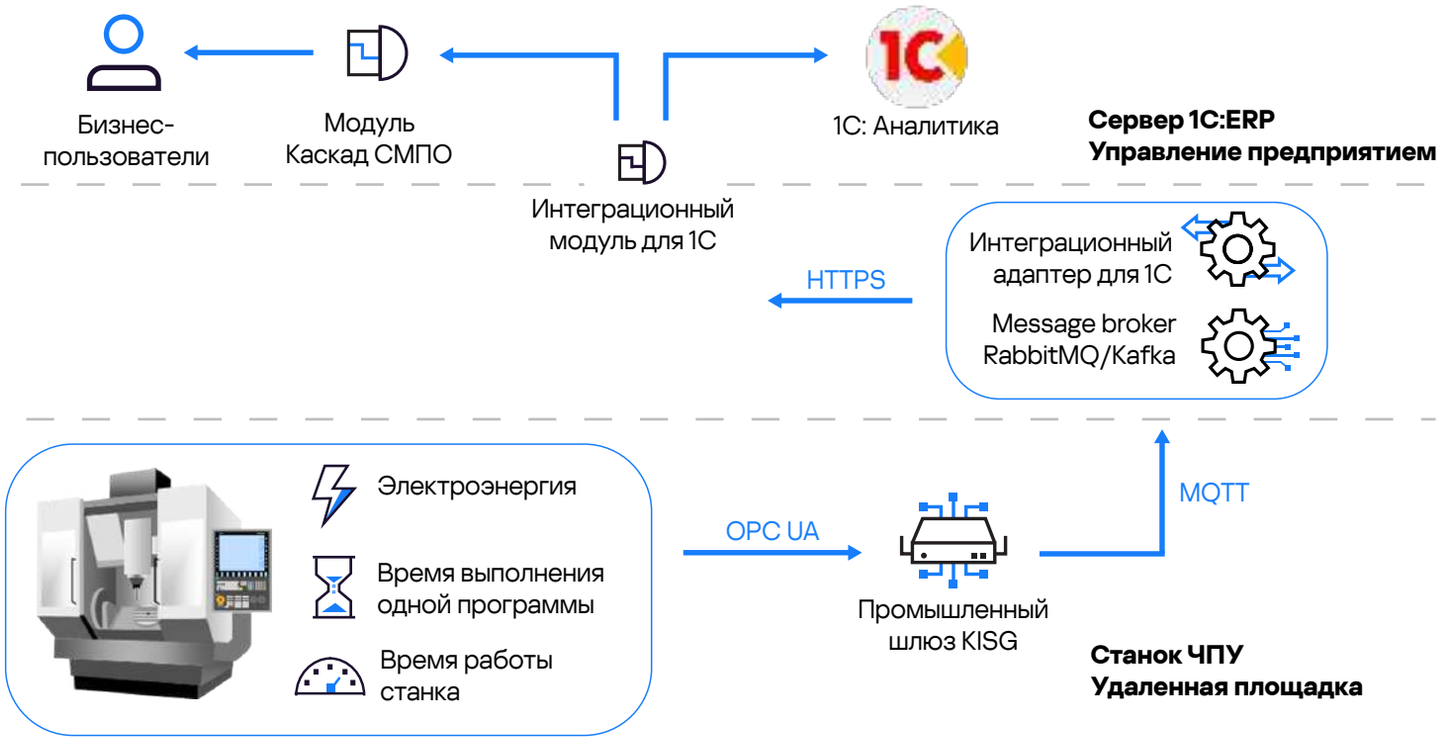
- **Защита сети.** Манипулирование стандартными сетевыми протоколами часто является основным способом несанкционированного проникновения в информационные системы предприятия, поэтому использование сетевых устройств со встроенными средствами защиты, иммунных к большинству известных атак, является важной задачей при построении защищенных промышленных информационных систем. Кибериммунные сетевые устройства позволяют блокировать распространение вредоносного воздействия на сетевые узлы информационной системы, даже если это неизвестные ранее типы атаки или вредоносный код. Поэтому использование в ядре корпоративной сети кибериммунных маршрутизаторов и коммутаторов может значительно усилить защищенность сети промышленного предприятия.

  Следует отметить, что на данный момент стандартов, которые определяют принципы построения кибериммунных систем, нет, но работа в этом направлении ведется. Существует предварительный стандарт построения систем сбора данных, которые отвечают основным принципам конструктивной безопасности. Стандарт ПНСТ 819-2023 «Информационные технологии. Интернет вещей. Системы с разделением доменов. Термины и определения» содержит основные определения для построения защищенных систем Интернета вещей, а ПНСТ 818-2023 «Базовые компоненты» описывает набор основных компонентов для кибериммунных систем.

start@aprotech.ru
+7 495 970 71 17

Пример конструктивно безопасной системы

Для иллюстрации принципов построения кибериммунных систем можно рассмотреть следующий пример информационной системы. В этой конфигурации кибериммунный шлюз взаимодействует с промышленным оборудованием по протоколу OPC-UA. Далее шлюз преобразовывает сообщения от оборудования в стандартный формат MQTT и передает их во внешний мир с использованием алгоритмов шифрования TLS, которые вместе гарантируют доставку промышленных данных в корпоративные системы, их конфиденциальность и достоверность. Для работы устройства необходимо развернуть в целевой ИТ-среде брокер сообщений MQTT (MQTT Broker), который будет обеспечивать администрирование и доставку сообщений подписчикам (различным ИТ-приложениям). Переданные промышленные данные после сохранения и анализа в дальнейшем используются в работе систем управления производством.



Таким образом, за счет преобразования протоколов кибериммунное устройство обеспечивает разделение сегментов промышленной и ИТ-сетей, безопасную и надежную доставку промышленных данных в системы MES/ERP/PLM и др. Например, для подключения промышленного оборудования к системам на базе «1С: ERP» через кибериммунный шлюз на базе KasperskyOS может быть использован специальный продукт «Легковесный ETL-движок».

Особенности кибериммунных решений

При проектировании своих решений мы руководствуемся принципами и методологиями, наработанными за многие годы внутри компании. Чтобы решение на базе KasperskyOS было кибериммунным, необходимо следовать специальной методологии:

- четко определить цели безопасности (например, конфиденциальность данных), а также условия, в которых будет эксплуатироваться система;
- разделить решения на изолированные домены безопасности, учитывая функциональность и степень доверия к каждому из них;
- обеспечить контроль информационных потоков между этими доменами, разрешая только заданные виды взаимодействий.

Для интегратора, который занимается построением промышленных систем, использование кибериммунного устройства в общей схеме подключения снимает значительную часть вопросов обеспечения ИБ – они решаются на уровне программно-аппаратного комплекса, не замедляя работу основных систем.

Если говорить про конкретное устройство, которое мы использовали в своих проектах, то существенным преимуществом оказались встроенные возможности ПАК транслировать поток данных из протокола OPC UA в события MQTT. Это позволило на аппаратном уровне сразу «из коробки» упростить реализацию целевой интеграционной схемы для определенного класса задач: автоматизировать передачу большого потока информации от промышленного устройства в систему мониторинга, гарантировать ее целостность, конфиденциальность и доставку, а также обеспечить минимальную задержку. Устройство выступает в роли диода данных, однако его функционал может быть несколько шире.

В рамках внедрения кибериммунных систем мы можем выполнять комплекс работ, связанных как с безопасностью, так и с анализом и хранением данных производственного процесса, получаемых с промышленного оборудования. Например, проект может включать в себя бесшовную интеграцию оборудования с их цифровыми двойниками и системами класса ERP, а также визуализацию и анализ данных производства на Dashboard.

start@aprotech.ru
+7 495 970 71 17