



ЛУЧШИЕ ПРАКТИКИ КИБЕРБЕЗОПАСНОСТИ ДЛЯ ПРОМЫШЛЕННЫХ КОНТРОЛЛЕРОВ

БЕНСОН ХУГЛАНД (BENSON HOUGLAND)
ПЕРЕВОД: ВЛАДИМИР РЕНТЮК

Защита систем промышленной автоматизации становится проще и эффективнее, если контроллеры содержат встроенные функции кибербезопасности.

Проблемы обеспечения безопасности оказывают влияние на работу всех типов цифровых систем. Несанкционированные вторжения в системы управления или нарушения их функционирования как минимум создают те или иные неудобства, но также могут поставить под угрозу целостность и достоверность данных или вызвать недозволённые действия. Последствия для конечных пользователей и связанные с ними проблемы различаются в зависимости от организации систем. Для пользователей промышленной автоматизации кибератаки могут привести к выпуску бракованного продукта, повреждению оборудования и прямым угрозам безопасности функционирования, включая последствия экологического характера. Потенциальная стоимость принятия должных мер и отсутствия систем-

ного подхода в области кибербезопасности высока и очевидна.

По мере развития систем операционных технологий (ОТ) их адаптация к кибератакам и требования безопасности меняются. В этом смысле более серьёзную потенциальную угрозу нарушения безопасности из-за кибератак технологических и производственных процессов предприятия создаёт тесная интеграция систем ОТ с системами информационных технологий (ИТ) и возможностью подключения к Интернету. Ключом к защите от этих типов угроз являются интеграция мер безопасности непосредственно в базовые функциональные узлы систем автоматизации и, естественно, постоянная бдительность. Здесь уместно вспомнить слова, сказанные ещё в 2000 г. известным криптографом и специалистом по компьютерной безопасности Брюсом Шнайне-

ром: «Безопасность — это процесс, а не продукт».

Для решения сложной, меняющейся природы безопасности пользователи в первую очередь должны понимать связанные с этим риски, цифровую среду, в которой они работают, и доступные для них инструменты безопасности. В данном направлении эксперты выделяют несколько элементов безопасности системы, включая физическую и сетевую безопасность, а также политики и процедуры.

Несомненно, что максимальная защищённость системы промышленной автоматизации в первую очередь зависит непосредственно от самого пользователя, но рассмотрим функции сетевой безопасности, встроенные в определённые продукты автоматизации, а также лучшие практики по организации защищённой сети конечной системы.

ОСНОВЫ БЕЗОПАСНОСТИ

Устройства и методы промышленной автоматизации развивались на протяжении многих десятилетий, что привело к предложению весьма широкого спектра коммерчески доступных продуктов. В данном случае интерес представляют приложения, в которых разработчики обычно развертывают отдельные контроллеры, даже если большинство из них используется параллельно в качестве одноранговых узлов.

Продукты, применяемые в этой среде, представляют собой цифровые или компьютеризированные контроллеры, подключенные к сети, в частности через Ethernet. Они содержат:

- «умные» или интеллектуальные реле;
- программируемые логические контроллеры (ПЛК);
- программируемые контроллеры автоматизации (ПКА);
- промышленные персональные компьютеры (ПК);
- пограничные программируемые промышленные контроллеры EPIC (Edge Programmable Industrial Controller).

Первые три продукта уходят корнями в истоки промышленной автоматизации и были задуманы до распространения ПК и еще до того, как появилось само понятие «кибербезопасность», причем многие ранние поколения этих продуктов остаются в эксплуатации и сегодня. Хотя справедливости ради надо сказать, что их последние модели уже обновляются с помощью современных вычислительных и сетевых технологий, но в целом они, как правило, ограничены предложением специализированной вычислительной среды, предназначенной для уровня управления, принятого в той или иной сфере индустрии.

Что касается промышленных персональных компьютеров — это не что из ряда вон выходящее. Это просто надежная версия ПК, который конечные пользователи могут оснастить различными управляющими программами и элементами связи, необходимыми для решения тех или иных задач контроля и управления в рамках своего промышленного предприятия.

Последний продукт, EPIC, представляет собой новое поколение

промышленных контроллеров, упакованных в виде ПЛК и предлагающих аналогичные функции управления в режиме реального времени, но с добавлением многих функций, подобных ПК, и преимуществами связи, удобными для ИТ.

Если говорить об элементах цифровой коммуникации, то их включение для подобных продуктов имеет весьма большое значение. Причем это касается не только удобства конфигурирования и обслуживания, они не менее важны и для подключения дополнительных продуктов, таких как человеко-машинные интерфейсы (HMI) и другие современные интеллектуальные устройства — например, средства визуализации и в перспективе искусственного интеллекта (ИИ), элементы которого уже прокладывают себе дорогу на промышленных предприятиях.

Лучшие практики для правильного проектирования сетевой безопасности промышленных контроллеров требуют тщательного рассмотрения следующих моментов:

- операционные системы;
- сетевые интерфейсы;
- доступ пользователя;
- передача данных.

ОПЕРАЦИОННЫЕ СИСТЕМЫ

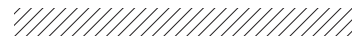
Операционная система (ОС) любого промышленного контроллера определяет степень его вычислительных возможностей и возможностей ввода/вывода (I/O). Обычно ПЛК и ПКА используют выделенные или встроенные ОС с закрытым исходным кодом, адаптированные к требуемому быстродействию логического решения. Индустриальные ПК также оснащены ОС с закрытым исходным кодом, чаще всего Microsoft Windows. Другой вариант ОС — применение Linux с открытым исходным кодом. Поэтому некоторые индустриальные ПК как раз и используют эту ОС, чтобы реализовать возможности, подобные ПК, многие EPIC обращаются и к ОС Линуса Торвальдса.

В отличие от ОС с закрытым исходным кодом ОС с открытым часто более безопасны. Однако негативные тенденции здесь связаны с их мировым признанием на рынке, что делает такие операционные системы, в частности Windows, лакомой целью

для кибератак и опять-таки для того, чтобы уже хакер мог получить признание в качестве их взломщика. И хотя перспективы для встраивания ОС с закрытым исходным кодом для использования в ПЛК пока еще относительно неясны, появление Stuxnet почти десять лет назад уже продемонстрировало, что коммерчески доступные платформы промышленного управления на основе закрытых систем не являются 100% жизнеспособными объектами, эффективно противостоящими кибератакам.

Win32/Stuxnet — сетевой червь, поражающий компьютеры под управлением операционной системы Windows. Впервые он был обнаружен в 2010 г., причем не только на ПК пользователей, но и в промышленных системах, управляющих автоматизированными производственными процессами. Это был первый известный компьютерный червь, перехватывающий и модифицирующий информационный поток между программируемыми логическими контроллерами марки и рабочими станциями SCADA (Supervisory Control And Data Acquisition). Это программный пакет, предназначенный для создания или обеспечения работы в реальном времени систем сбора, обработки, отображения и архивирования информации об объекте мониторинга или управления. Stuxnet мог быть использован в качестве средства несанкционированного сбора данных (шпионажа) и диверсий в АСУ ТП промышленных предприятий, электростанций, аэропортов и т. п. Уникальность программы заключалась в том, что впервые в истории кибератак вирус физически разрушал инфраструктуру. По одной из версий, Stuxnet был разработан спецслужбами США и Израиля для ядерной программы Ирана.

Преимущество открытого исходного кода заключается в его краудсорсинговой природе. То есть в возможности привлечения к решению тех или иных проблем инновационной производственной деятельности широкого круга лиц для использования их творческих способностей, знаний и опыта по типу субподрядной работы на добровольных началах с применением информационных технологий. Благодаря этому количество вовлеченных специалистов оказывается гораздо большим,



чем при традиционном производстве промышленных контроллеров с закрытым исходным кодом, что, в свою очередь, позволяет быстро реагировать на выявленные проблемы уязвимости.

Когда ОС с открытым исходным кодом используются для промышленных приложений, они должны быть изготовлены на заказ для конкретного устройства и содержать только пакеты, необходимые устройству. Такое упорядочение сокращает возможные варианты для атаки, также известные в специализированной технической литературе как уменьшение векторов атаки или поверхности атаки.

Кроме того, ОС, специально созданная для промышленного контроллера, должна быть криптографически подписана ее производителем. Контроллер должен принимать только сборки ОС, утвержденные изготовителем, что гарантирует происхождение сборки и исключает несанкционированное изменение кода ОС.

СЕТЕВЫЕ ИНТЕРФЕЙСЫ

Современные промышленные контроллеры, хотя многие специализированные индустриальные полевые шины все еще используются, в значительной степени уже зависят от коммерческого Ethernet. В общем случае для промышленных

контроллеров Ethernet обеспечивается физически проводными сетевыми интерфейсами. Однако подключение устройств может быть реализовано и через беспроводные технологии, например через Wi-Fi.

Однако для любой сети важно понимать концепцию доверенной сети по отношению к недоверенной. Доверенная сеть обычно находится в частном учреждении и может быть сетью, управляемой ИТ, где известны все пользователи, имеющие доступ. Недоверенная сеть — это любая сеть, в которой неизвестны те, кто имеет к ней доступ, скажем, тот же Интернет.

Одним из важнейших элементов сетевой инфраструктуры является маршрутизатор — сетевое устройство, которое настраивается для маршрутизации трафика между любыми двумя сетями. Многие люди знакомы с маршрутизаторами для домашнего использования, поскольку эти устройства обрабатывают трафик между Интернетом и устройствами в домашней сети. Эти маршрутизаторы перемещают данные между обеими сетями — доверенной и недоверенной.

Что касается промышленных приложений, они имеют отличия. Это связано с тем, что им требуются контроллеры с несколькими независимыми сетевыми интерфейсами, а потому доверенные и недоверенные сети

могут быть разделены. Один сетевой интерфейс назначается как локальная доверенная сеть, а другой — как внешняя недоверенная сеть. И здесь есть нюанс: чтобы никакой внешний злоумышленник не мог подключиться к доверенной сети из недоверенной, эти интерфейсы не должны быть маршрутизируемыми (рис. 1).

Еще одна важная концепция сети — это шлюз безопасности (межсетевой защитный экран, брандмауэр), который предотвращает нежелательный трафик от доступа к сети, устройству или хосту. Как правило, локальные исходящие соединения, определяемые устройством, считаются заслуживающими доверия и, следовательно, разрешенными, как и соответствующие входящие ответы. Однако какие-либо попытки входящего соединения извне отклоняются, хотя брандмауэр может быть настроен и для открытия определенных назначенных портов и разрешения входящего трафика.

Промышленный контроллер должен иметь собственный брандмауэр и предоставлять средства для его настройки. При этом для промышленных приложений доверенному сетевому интерфейсу потребуются порты, связанные с логикой управления, соединениями с портами ввода/вывода (I/O) или другими промышленными протоколами.

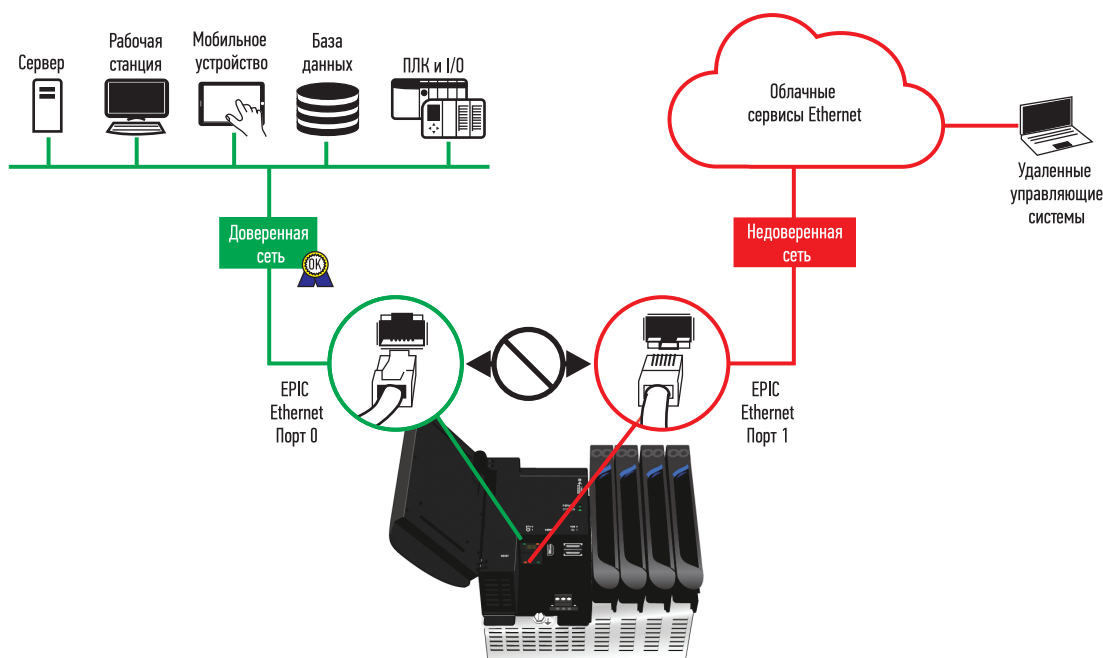


РИС. 1. ► Безопасность промышленного контроллера лучше всего реализовать с несколькими сетевыми интерфейсами, которые не маршрутизируют трафик между ними, защищая локальную доверенную сеть от внешнего недоверенного доступа. Все изображения предоставлены компанией Opto 22

Но у недоверенного сетевого интерфейса все порты, кроме безопасного порта, как правило, должны быть заблокированы. Это делается, чтобы разрешать получение доступа к контроллеру через зашифрованное соединение только аутентифицированным пользователям. Поэтому по умолчанию рекомендуется открывать только необходимые порты и блокировать все остальные порты, а недоверенному сетевому интерфейсу вообще блокировать все порты доступа (рис. 2).

Здесь крайне важна правильная конфигурация сети, и она должна быть в комплексе с тщательным назначением доступа пользователей и привилегий.

ДОСТУП ПОЛЬЗОВАТЕЛЯ

Ключевой особенностью современных компьютеризированных решений и подходов цифровой обработки, независимо от того, используются ли они на мобильных устройствах, ПК или промышленных контроллерах, является концепция учетных записей пользователей с назначенным доступом и привилегиями. Как правило, учетная запись администратора должна быть создана изначально, и только у него есть все необходимые глобальные привилегии. Однако этот аккаунт должен быть тщательно защищен владельцем.

Промышленный контроллер не должен предлагаться на имя пользователя или пароль по умолчанию для любой учетной записи. Вместо этого должен требовать, чтобы администратор выбирал уникальные учетные данные при создании каждой учетной записи. Учетные данные по умолчанию могут быть легко получены и использованы любым пользователем, в то время как уникальная учетная запись администратора лучше защищает контроллер от злоумышленников. Если учетные данные администратора потеряны, то учетная запись не подложит восстановлению и потребует сброс контроллера к заводским настройкам по умолчанию и создание новых записей.

Учетная запись администратора предусмотрена для создания учетных записей пользователей. Для промышленного контроллера авторизованными пользователями могут

быть не только люди, но и соответствующие программные сервисы с разрешенным доступом.

Рекомендуется создавать учетные записи только для разрешенных пользователей, предоставлять им лишь необходимые привилегии, назначать надежные пароли и всегда требовать проверки подлинности. Именно это является наилучшей практикой в части кибербезопасности. Тщательное управление учетными записями пользователей дает администратору полный и детальный контроль над тем, кто и что может получить доступ к системе и, следовательно, кто и что не может от нее получать или изменять в ней (рис. 3).

Общим требованием для внешних пользователей является подключение к контроллеру через Интернет. Безопасный порт, который шифрует всю передачу данных и разрешает подключаться только аутентифицированным пользователям, может выполнить это требование, создав безопасное соединение.

Другой способ — использование отдельного устройства в сети, способного создать для внешних клиентов или серверов защищенный туннель виртуальной частной сети (Virtual Private Network — VPN). Однако настройка VPN может потребовать широкого участия и координации с ИТ-персоналом. Поэтому лучшим вариантом считается выбор контроллера с уже встроенными возможностями безопасного VPN-туннеля, что дает персоналу ОТ полный контроль над VPN-подключениями для безопасного соответствия их потребностям (рис. 4) без участия третьих лиц.

Независимо от того, используете вы контроллер с уже встроенными функциями безопасности или сетевые устройства узла, для удаленных подключений через любую форму ненадежной сети рекомендуется всегда применять правильно настроенный безопасный VPN-туннель и отключать его, когда в нем нет необходимости.

ПЕРЕДАЧА ДАННЫХ

Смысл оснащения контроллеров сетевыми интерфейсами заключается в обеспечении соединений для передачи данных. Однако основная цель этой статьи заключается в том, как предотвратить соединения, по край-

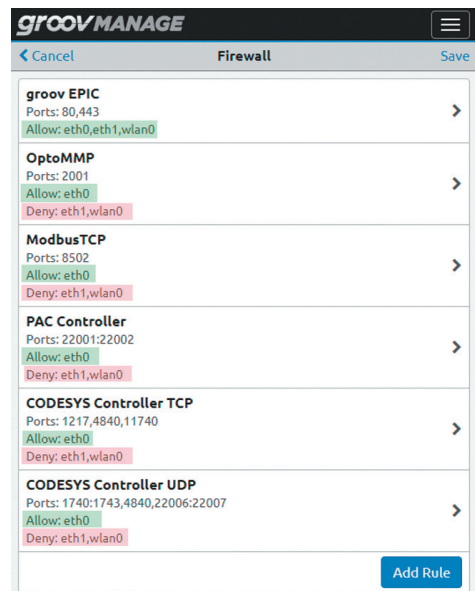
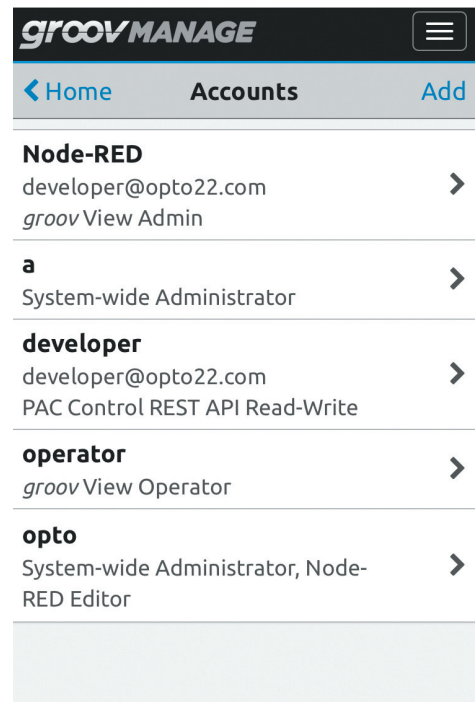


РИС. 2. ▲

В этом примере конфигурация брандмауэра открывает только определенные порты для протоколов ОТ и лишь в локальной доверенной сети (в данном случае — eth0), запрещая все подключения из недоверенной сети (eth1). Доступ к контроллеру groov EPIC возможен только через порты 80 и 443 (когда порт 80 открыт, любой входящий трафик автоматически перенаправляется на порт 443, который является безопасным)

РИС. 3. ▼

Для эффективной безопасности решающее значение имеют детальный контроль учетных записей пользователей и применение сложных паролей для аутентификации, поскольку они помогают отражать атаки злоумышленников



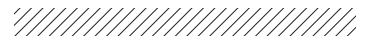
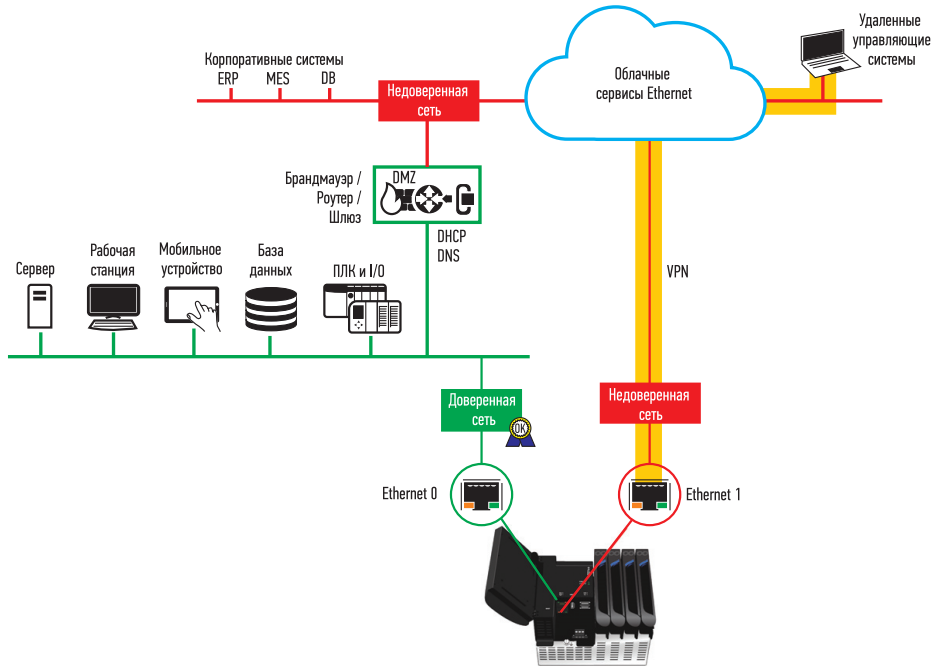


РИС. 4. ►

Некоторые контроллеры для удаленного подключения могут быть настроены персоналом ОТ для установки безопасного VPN-туннеля, показанного здесь оранжевой подсветкой. Это может быть полезно как на временной основе для устранения неполадок, так и на постоянной для нормальной работы



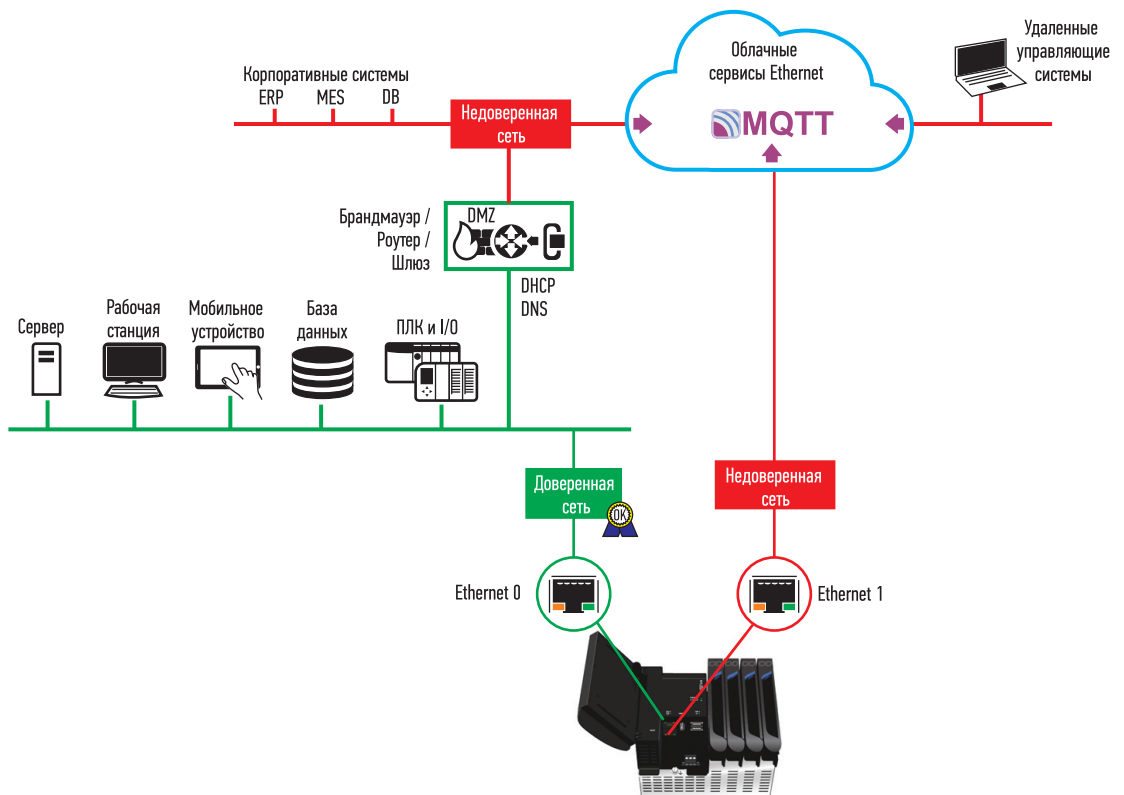
ней мере от неавторизованных лиц. Связь на доверенной стороне для контроллера относительно проста, и, как уже говорилось, входящие соединения по ненадежной сети

должны проходить через VPN или быть заблокированы. Но давайте рассмотрим вопрос, как вы будете передавать данные, если VPN сложно настроить? Например, как OEM-

производитель будет получать необходимые для него данные от машин на объектах клиентов для выставления счетов или технического обслуживания?

РИС. 5. ►

Исходящие протоколы, такие как MQTT, позволяют контроллерам безопасно инициировать соединения для передачи данных через брандмауэр и, не требуя открытия входящих портов, обеспечивают лучшую безопасность



Ответ заключается в использовании исходящих протоколов обмена данными от устройств. Одним из таких протоколов является MQTT (message queuing telemetry transport) — упрощенный сетевой протокол, работающий поверх TCP/IP и ориентированный для обмена сообщениями между устройствами по принципу «издатель-подписчик» (рис. 5). Обмен сообщениями в протоколе MQTT осуществляется между клиентом (client), который может быть издателем или подписчиком (publisher/subscriber) сообщений, и брокером (broker) сообщений.

Как сказано выше, исходящие соединения обычно разрешаются через брандмауэр, потому что они являются доверенными. Контроллер с использованием исходящего соединения настроен на выдачу (здесь он выступает как издатель) данных, представляющих интерес, для внешнего центрального брокера. Удаленные пользователи подключаются и подписываются на центрального брокера аналогичным образом. Потому что только так соединение разрешает двусторонний поток данных, при этом все соединения будут аутентифицированы и зашифрованы.

Еще одна ключевая функция, которую нужно иметь в промышленном контроллере, — встроенное управление сертификатами безопасности. Сертификат безопасности в основном проверяет подлинность одного оборудования для другого, поэтому оборудование, генерирующее исходящий поток данных, может быть уверено в том, что оно подключается к соответствующему целевому назначению, а не к самозванцу.

Сертификаты могут быть реализованы различными способами, они могут быть созданы конечным пользователем или зарегистрированы через центр сертификации (рис. 6). Промышленные контроллеры, поскольку от их должного функционирования зависит не только качество продукции, но и безопасность персонала и среды, должны использовать отраслевые стандарты сертификации, аналогичные банковским и сайтам электронной коммерции.

Однако даже с учетом всех этих рекомендаций по безопасности существуют и другие передовые практики, которые также следует принять во внимание.

КАКИЕ ЕЩЕ СУЩЕСТВУЮТ ПРАКТИКИ И РЕКОМЕНДАЦИИ

До сих пор мы рассматривали конфигурацию и лучшие практики для проектирования системы. Тем не менее существуют еще и процедурные рекомендации по улучшению безопасности.

- Минимизация использования интерфейсов: самая кибербезопасная система — это физически разделенная система (отключенная от сети) и не имеющая внешних интерфейсов. Однако, как правило, это непрактично, но возможно, если контроллер предлагает уже встроенный интерфейс. В любом случае всегда удаляйте ненужные сетевые соединения и блокируйте неиспользуемые порты.
- Минимизация доступа: назначьте пользователям минимально возможные привилегии в соответствии с тем, что им конкретно нужно видеть и делать, и требуйте, чтобы они выходили из системы, когда они неактивны, особенно это касается пользователей с правами администратора. Данный совет распространяется на все элементы системы управления, включая HMI, которые должны по возможности выполняться в информационном режиме и только для чтения.
- Разработка и эксплуатация системы в условиях производства: помните, что это разные вещи. Ограничения иногда смягчаются для тестирования и создания прототипов. Убедитесь, что контроллер полностью защищен после тестирования и перед вводом в эксплуатацию. Некоторые контроллеры на основе Linux для разработки пользовательских приложений разрешают пользователям применять безопасный доступ к оболочке (Secure Shell, SSH). После завершения разработки убедитесь, что доступ к оболочке отключен.

ЗАЛОГ УСПЕХА

Лучшие практики, изложенные в этой статье, служат хорошей отправной точкой для начала любого нового проекта промышленной автоматизации или для повторного использования уже действующего

проекта. Важно не забывать о том, что надежная защита должна быть тщательно реализована на всех уровнях. Она будет наиболее эффективна, когда меры безопасности уже встроены в продукты автоматизации, а не представлены внешними устройствами. Встроенные функции безопасности помогут быстро внедрить систему безопасности с минимальными затратами.

Однако каждая конкретная ситуация имеет те или иные отличия и дать универсальный рецепт, пригодный на все случаи жизни, тем более в рамках статьи, сложно. Только вам известны все особенности ваших приложений и сетевых архитектур, а значит, именно вы ответственны за их должное и безопасное функционирование. Встроенные функции сетевой безопасности для промышленных контроллеров могут помочь спроектировать и поддерживать защищенную систему, но, повторюсь, в конечном итоге вы несете ответственность за их разумное использование в вашем приложении как часть вашей общей стратегии безопасности. ●

РИС. 6. ▼ Рекомендуется, чтобы контроллеры поддерживали стандартные сертификаты безопасности, как банковские сайты и сайты электронной коммерции

groovMANAGE ☰

[< Back](#) **View Certificate**

The Server SSL certificate is used to provide secure HTTPS communication with the internal web applications, including *groov Manage*, *groov View*, and Node-RED.

Certificate Details

Last Modified	2/11/2019 3:36:00 PM
----------------------	-------------------------

View Decoded Certificate [>](#)

View Encoded Certificate [>](#)

[Download Public Certificate](#)

[Download Private Key](#)

[Download CSR](#)