ТЕХНИЧЕСКИЙ ОБЗОР

Защита сетевых устройств в соответствии со стандартом МЭК 62443-4-2

Что необходимо об этом знать

MOXA®

Предпосылки необходимости обеспечения кибербезопасности в промышленности

По мере того как промышленный интернет вещей (IIoT) продолжает набирать обороты, все большее количество устройств подключается к инфраструктуре сети. Данную тенденцию можно наблюдать по процессу перехода закрытых сетевых структур в частные IT-сети, которые доступны из открытой сети Интернет. Вместе с повышением эксплуатационной эффективности данная тенденция также вызывает повышенную обеспокоенность владельцев систем угрозами кибербезопасности. Данные опасения оправданы. В недавнем отчете, опубликованном группой ICS-CERT (Industrial Control Systems Cybersecurity Emergency Response Team), подсчитано, что исследователи зафиксировали 392 случая кибератак на промышленную инфраструктуру в США в 2016 году, что больше по сравнению с 295 случаями в предыдущем году. Темпы роста количества уязвимостей составили 32,88% в период с 2015 по 2016 год. Поэтому неудивительно, что владельцы промышленных систем все чаще нуждаются в решениях кибербезопасности, позволяющих им создавать защищенные системы для промышленных задач.

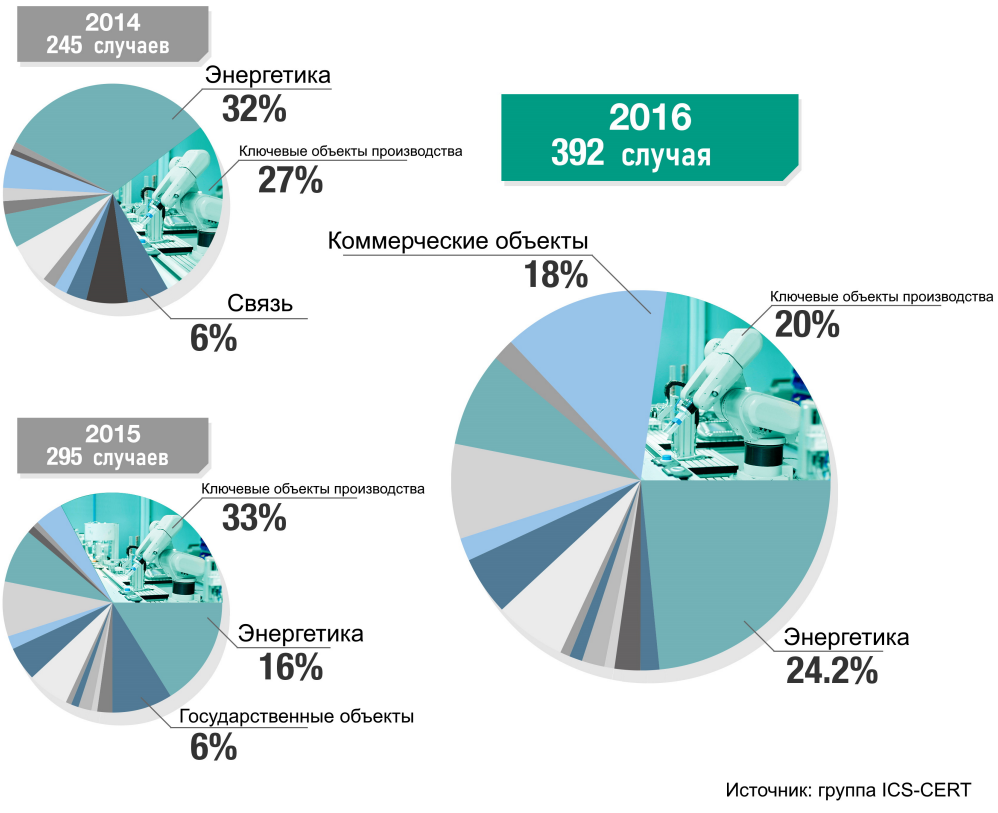

Рисунок 1 – Количество кибератак на ключевые производственные секторы США за 2014-2016 годы

Эволюция стандартов кибербезопасности

В 2002 году международное общество по автоматизации (ISA) выпустило документ под названием ISA-99, в котором были приведены советы для предприятий сферы автоматизации по методам защиты от киберугроз. Пятнадцать лет назад тема кибербезопасности не была столь обсуждаема, как сейчас. Документы ISA были приведены в соответствие с документами, которые чаще всего используются международной электротехнической комиссией (МЭК), поскольку количество проблем, связанных с кибербезопасностью, увеличилось с момента появления стандартов ISA. В настоящее время стандарт МЭК 62443 представляет собой серию стандартов, отчетов и другой соответствующей документации, в которой определяются процедуры внедрения систем промышленной автоматизации и управления (IACS) с электронной защитой. Следование рекомендациям стандарта МЭК 62443 значительно снизит вероятность кибератак, влияющих на работу сети.

Обзор стандарта МЭК 62443

Стандарт МЭК 62443 включает рекомендации для различных частей сети и для тех, кто выполняет различные обязанности при работе с ней. В прошлом владельцы оборудования для организации безопасности сети полагались на решения системных интеграторов (СИ), таких как Siemens, Honeywell и ABB. Однако многие СИ в настоящее время требуют, чтобы поставщики компонентов соблюдали подраздел стандарта МЭК 62443, касающийся их устройств. На диаграмме ниже (рис. 2) представлен краткий обзор стандарта, включающий в себя объем и значение каждой части для тех, кто должен обеспечить безопасную работу сети.

Рисунок 2 – Структура стандарта МЭК 62443

Рекомендации МЭК 62443 определяют четыре уровня угроз безопасности. Уровень 2 является базовым требованием в отрасли автоматизации. Это относится к киберугрозам, создаваемым хакерами и представляющим собой наиболее распространенные атаки, которым подвергаются системные интеграторы, защищающие промышленные сети. Уровень 1 предназначен для защиты от случайного неавторизованного доступа, а уровни 3 и 4 – от преднамеренного доступа хакеров, которые используют специализированные навыки и инструменты.

МЭК 62443-4-2 Уровень 2: Базовые требования в отрасли автоматизации

В стандарте МЭК 62443 есть несколько подразделов, которые относятся к разным частям системы. Поскольку СИ требуют соблюдения требований подраздела МЭК 62443-4-2, в котором указаны руководства для поставщиков компонентов, то данный подраздел становится все более важным. Требования к компонентам основаны на ключевых аспектах, включающих в себя контроль идентификации и аутентификации, контроль пользователей, целостность и конфиденциальность данных, а также обеспечение резервного копирования данных для непрерывной доступности ресурсов. Ввиду того, что поставщики компонентов играют все более важную роль в сетях IIoT, оставшаяся часть этого документа будет посвящена детализации требований безопасности, которым должны соответствовать производители при разработке устройств для развертывания в сетях IIoT.

Инфраструктура

Если компонент сети позволяет пользователям получать доступ к устройствам или приложениям, то этот сетевой компонент должен иметь возможность однозначной идентификации и аутентификации всех пользователей, включая людей, процессы и устройства. Это позволяет разделить обязанности и обеспечивает принцип привилегий, который гарантирует, что каждый пользователь будет иметь доступ только к той информации и тем устройствам, которые ему необходимы, чтобы выполнять назначенную ему роль в сети. Важно избежать ненужного риска, связанного с предоставлением пользователям большего доступа к сети, чем им необходимо для выполнения своих обязанностей. Предотвращение этого ненужного риска безопасности ограничит возможности злоумышленников причинить большой ущерб сети. Следование этим принципам поможет защитить инфраструктуру сети и обеспечит надежную основу для ее развития, что позволит решать текущие и будущие задачи безопасности.

Управление учетными записями

Возможность управления учетными записями, включая операции по их созданию, активации, изменению, отключению и удалению, должна поддерживаться по всей сети. Это гарантирует, что никакие учетные записи не создаются, изменяются или удаляются, если не было предоставлено разрешение, а также запрещает устройствам устанавливать любые неавторизованные соединения. Функция управления учетными записями имеет несколько возможных сценариев, которые, если данную функцию не реализовать, могут вызвать проблемы у владельцев систем. Например, человек, работающий в сети, получает повышение по службе, поэтому теперь требуется расширение прав доступа к устройствам и приложениям, и его уровень доступа должен быть соответствующим образом скорректирован. Другой часто встречающийся пример – когда сотрудник покидает организацию. Как только он перестает быть сотрудником, он больше не может иметь доступа к сети и должен лишиться своих сетевых привилегий. Несложно представить, что может встретиться недовольный бывший сотрудник, у которого будет злой умысел при доступе в сеть.

Управление идентификацией

Любой компонент сети, имеющий пользовательский интерфейс, должен напрямую интегрироваться в систему, которая идентифицирует людей по пользовательскому, групповому, ролевому и/или системному интерфейсу. Это лишает пользователей возможности подключения к сетевым устройствам, доступ к которым им не предоставлен. Пользователи с разными ролями в сети имеют разные привилегии. Например, учетная запись сетевого администратора может управлять настройками устройств в сети,

а учетные записи, которые имеют доступ на уровне гостя, могут только просматривать устройства, но не изменять их настройки. Также должны существовать механизмы безопасности, позволяющие деактивировать учетную запись, если через нее не было обращений в течение определенного периода времени. Функция управления идентификацией позволяет контролировать учетные записи каждого пользователя в сети и гарантирует, что они ограничены ролями, назначенными им сетевыми администраторами. Это обеспечит защиту от случайного или преднамеренного доступа пользователей к тем частям сети, доступ к которым им не нужен.

Управление аутентификацией

Все устройства в сети должны иметь возможность подтверждать достоверность любых запросов на обновление системы/встроенного программного обеспечения и проверять, что источник не пытается загрузить какие-либо вирусы или вредоносные программы. Это достигается за счет использования токенов, ключей, сертификатов или паролей. Если нет системы управления аутентификацией, то любой, кто захочет атаковать сеть, может легко загрузить вредоносное ПО, что позволит ему изменить настройки или взять на себя управление сетью.

Аутентификация на основе пароля

Для сетевых компонентов, которые используют аутентификацию на основе пароля, должна быть интегрирована политика паролей, которая обеспечивает следующее:

А) В структуре пароля должно быть указано, какой тип символов разрешен, а также количество символов, необходимое для того, чтобы пароль был принят в качестве действительного

Б) Частота смены пароля

Преимущество использования пароля в том, что для сетевых администраторов это простой способ защитить свою сеть, который не требует дополнительной работы от системного инженера. Использование эффективной политики паролей не позволит большинству хакеров получить доступ к сетям, используя грубую силу для взлома слабых паролей. В сети, которая не поддерживает политику паролей, или в сети, которая позволяет использовать слабые пароли, риск получения хакерами доступа к сети гораздо выше.

Аутентификация на основе открытого ключа

Аутентификация на основе открытого ключа должна использоваться для создания безопасного соединения между серверами и устройствами или между устройствами. Чтобы включить эту функцию, каждый компонент сети должен иметь возможность проверять сертификаты через аутентификацию подписи, а также через проверку актуальности сертификата. Кроме того, должен быть организован доступ к авторизованному центру сертификации или, в случае самоподписанных сертификатов, должны быть загружены сертификаты на всех хостах, взаимодействующих с субъектом, которому выдан данный сертификат. Аутентификация с открытым ключом важна, потому что она предотвращает отправку информации в неправильное место, а также предотвращает передачу конфиденциальной информации, которая должна оставаться в сети, в неподтвержденные источники извне.

Контроль пользователей

Все устройства, которые появляются в сети, должны поддерживать аутентификацию при входе в систему. Чтобы запретить нежелательным пользователям доступ к устройству или сети, приложение или устройство должны ограничивать количество попыток ввода

пользователем неправильного пароля перед своей блокировкой. Поскольку большинство атак на промышленные сети осуществляются хакерами, использующими атаки методом "грубой силы" (brute force – перебор паролей), аутентификация при входе в систему является чрезвычайно эффективным способом предотвращения доступа хакеров в сеть. Кроме того, система или устройство также должны иметь возможность информировать пользователей, была их попытка входа в систему успешной или нет. Информирование пользователей о том, что они успешно вошли в сеть, позволяет им подтвердить свой статус и продолжить работу с сетевыми настройками или устройствами, зная, что все их действия аутентифицированы.

Целостность данных

Во всех сетях IIoT целостность данных играет жизненно важную роль. Это гарантирует, что данные точны и что они могут быть обработаны и получены. Существует несколько мер безопасности, которые можно использовать для защиты данных, включая протокол SSL, который обеспечивает шифрование между web-браузером и сервером. Поскольку информация постоянно перемещается по сети, то сетевые операторы должны быть уверены, что данные передаются безопасным, надежным и эффективным способом. Если данные отправятся случайным получателям, то операторы сети не только потеряют контроль над своими данными, но и сделают свои сети уязвимыми для хакеров.

Резервное копирование данных для непрерывной доступности ресурсов

Все приложения или устройства, находящиеся в сети, должны иметь возможность выполнять резервное копирование данных, не мешая работе сети. Основное преимущество выполнения регулярных резервных копий заключается в том, что обеспечивается сохранность данных. А в случае, если сеть испытывает некоторые проблемы в работе, есть возможность использовать данные из резервной копии, чтобы вернуть ее в нормальное состояние. Кроме того, процесс резервного копирования должен гарантировать, что любая частная информация, которая находится в сети, хранится в соответствии с политиками защиты данных и недоступна для тех, кто не должен иметь доступ к этой информации. В некоторых случаях это означает, что данные нельзя хранить вне сети. Любое нарушение условий хранения данных, содержащих личную информацию пользователей, наносит огромный ущерб операторам сети, а также тем, чьи данные были доступны в результате утечки к случайным лицам.

Вывод

Поскольку к сети постоянно подключается все больше устройств обеспечение их безопасности имеет первостепенное значение для владельцев систем. Применение передовых подходов к обеспечению безопасности дает владельцам систем наилучшие шансы защитить свою сеть от доступа злоумышленников. Полная безопасность на уровне системы должна строиться на основе, которая состоит из функций безопасности каждого отдельного компонента.

Подробнее о кибербезопасности: https://moxa.ru/landing/Cybersecurity-Microsite/index.htm