DOI: 10.22184/1992-4178.2019.182.1.18.20

Кибербезопасность с момента «рождения» цифровой информации

Рассказывает менеджер по системам безопасности подразделения доверенных решений безопасности компании Analog Devices Э. Халтен

В 2016 году компания Analog Devices, Inc. – один из мировых лидеров в области интегральных схем для различных отраслей, таких как автоматизация, телекоммуникации, автомобильная, медицинская, промышленная электроника и др. – расширила свои возможности, приобретя подразделение решений в области кибербезопасности компании Sypris Electronics.

В современном мире, который становится все более цифровым и в котором обмен данными затрагивает все больше аспектов человеческой деятельности, кибербезопасность играет роль, важную как никогда. О том, какие изменения происходят в этой области, как меняются подходы к обеспечению кибербезопасности в промышленности и какое место в этом занимают решения Analog Devices, на выставке electronica 2018, прошедшей в Мюнхене в ноябре прошлого года, нам рассказал менеджер по системам безопасности подразделения доверенных решений безопасности компании Analog Devices Эрик Халтен (Erik Halthen).

В настоящее время подходы к обеспечению кибербезопасности претерпевают существенные изменения. Это связано с цифровизацией, с такими трендами, как Интернет вещей (IoT) и «Индустрия 4.0». В сеть объединяется огромное количество устройств, взаимодействующих с реальным миром посредством датчиков и исполнительных механизмов.

Традиционно для защиты промышленных систем управления от кибератак информационная инфраструктура предприятий разделялась на отдельные сетевые сегменты и контуры, данные сегрегировались, управление в каждом контуре выполнялось независимо. При этом целостность данных внутри сегмента сети обеспечивалась путем мониторинга и управления этими данными на основе четкого представления, какие именно устройства подключены к этому сегменту. Таким образом, внутри сегмента существовала доверенная среда, а вопрос безопасности возникал на периферии сегмента, то есть в точке подключения этого сегмента к внешней среде, например на уровне шлюза или даже сервера. В качестве средств обеспечения безопасности в этих точках применялись такие средства, как, например, межсетевой экран (firewall).

Однако для задач построения цифровых производств, «Индустрии 4.0» этот подход имеет множество ограничений. В новых условиях к сети подключается очень большое количество устройств, сильно возрастает объем передаваемой информации, которая обрабатывается на различных уровнях с применением в том числе граничных и облачных вычислений, систем искусственного интеллекта. Мониторинг и управление этим трафиком оказываются затруднены, что дополнительно осложняется ростом необходимости в обмене данными в реальном времени. Кроме того, информационные системы цифрового предприятия могут обмениваться данными не только с облаком, но и с другими предприятиями, а также взаимодействовать с различными пользователями и с самими изделиями в течение всего их жизненного цикла.

Таким образом, в условиях цифровых производств обеспечение уверенности в том, что в любой момент данным информационной системы можно доверять, и в том, что не произошло никаких сбоев или утечки информации, становится непростой задачей, требующей принципиально новых подходов. Для обеспечения кибербезопасности необходим системный подход; достичь желаемого результата невозможно, полагаясь только на одно решение. Для этого необходима кооперация, внедрение решений на различных уровнях и по всей цепочке передачи информации, в каждой точке от периферийного устройства (узла) до облака. Этот подход нашел отражение в так называемой модели нулевого доверия (Zero Trust).

Применительно к цифровым производствам идентификация и целостность данных должна обеспечиваться, фактически начиная с той точки, в которой цифровая система взаимодействует с реальным миром, то есть с датчиков.

Аналогичные проблемы обеспечения кибербезопасности проявляют себя и в других областях, поскольку гиперсвязность приводит к существенным изменениям по всему рынку. Так например, автомобильная промышленность движется в направлении подключенных автомобилей и автономного транспорта, где транспортные средства должны очень быстро и надежно обмениваться информацией не только между собой, но и с инфраструктурой. Еще одним направлением, ставящим новые задачи в области кибербезопасности, является обеспечение надежной инфраструктуры виртуальных рабочих столов (VDI).

Понимание необходимости изменения подхода к кибербезопасности существует у множества компаний, однако реализация этого перехода может оказаться слабым звеном, которое способно привести к задержке развития «Индустрии 4.0» и других концепций, связанных с новыми моделями обмена данными и их обработки.

Исторически основная деятельность компании Analog Devices связана именно с той частью электронных устройств и систем, где происходит преобразование аналогового сигнала в цифровые данные и наоборот, и в этой области у нас наиболее сильные позиции и богатый опыт. Поэтому нашей компанией созданы решения, помогающие заказчикам быстрее осуществить переход к новым моделям обеспечения кибербезопасности, по сути, сдвигая границу доверенности информации с периферии сегмента сети к точке взаимодействия информационных систем с реальным миром.

Таким решением, например, является платформа RapID на основе ИС многопротокольного коммутатора Ethernet реального времени fido5000. Эта платформа позволяет выполнять подключение с помощью двух портов и поддерживает практически все распространенные промышленные протоколы Ethernet, включая PROFINET класса C (IRT) и B (RT); Ethernet/IP, в том числе с кольцом уровня физических устройств (DLR); Modbus TCP; EtherCAT; Powerlink и др. Данное решение может использоваться в месте подключения устройства сбора данных к протоколу Ethernet, который продолжает играть важную роль в системах автоматизации предприятий. Платформа обеспечивает генерацию и управление ключами, безопасные загрузку, обновление ПО и доступ к памяти. Это очень важно, поскольку, несмотря на то, что в настоящее время многие решения для обеспечения безопасности данных реализуются на аппаратном уровне, за ее существенную часть продолжает отвечать ПО, и защита устройства от несанкционированной загрузки программы является критической задачей кибербезопасности.

Еще один аспект заключается в том, что сегодня безопасность не является чем-то, что вы должны обеспечить один раз и навсегда. Ситуация постоянно меняется, меняется набор подключенных устройств, обмен данными осуществляется с различными внешними сетями. Чтобы быть готовым к будущему, необходимо постоянно осуществлять мониторинг в течение жизненного цикла изделий, прогнозировать возможные проблемы, понимать, в каком направлении вы должны двигаться в области кибербезопасности. И этот вопрос очень индивидуален, он не имеет единого ответа для всех. Поэтому в компании Analog Devices мы выбрали подход, который нацелен на глубокое понимание проблем наших заказчиков, на системный взгляд и взвешенные решения.

Когда вы принимаете решение о том, как будет достигаться кибербезопасность в вашем случае, вы в конечном счете рассматриваете ресурсы, которые необходимо защитить. Однако получить абсолютно защищенную систему невозможно. А чем ближе вы подходите к идеалу, стараясь защитить как можно больше ресурсов, тем дороже будет стоить такое решение. Поэтому это всегда компромисс. Необходимо оценить возможные риски, понять, что и от чего вы защищаете, выделить те ресурсы, которые представляют наибольшую ценность. И, защитив эти ресурсы, вы должны обеспечить возможность быстрого и наиболее безболезненного восстановления после кибератаки, возврата к нормальной работе за возможно короткий период времени. Этот подход получил название «устойчивость к киберугрозам» (cyber resilience).

Те решения, которые мы предлагаем в области кибербезопасности, не основаны на каких-либо уникальных методах. Для заказчиков часто важно иметь возможность масштабирования внедренных решений, они предпочитают, чтобы эти решения базировались на типовых стандартах и требованиях. Однако наша особенность заключается в том, что мы работаем на стыке цифровой системы и реального мира. Обеспечивая идентификацию и целостность данных в тот момент, когда они преобразуются в цифровую форму, наши решения позволяют заказчикам доверять информации, полученной от датчиков, при принятии решений на ее основе. Наше преимущество в том, что мы можем добавить безопасность в самом начале цепочки передачи данных в полном соответствии с традиционными стандартами.

Материал подготовлен Ю. Ковалевским