Internet вещей в промышленности: как получить преимущества и избежать рисков

А.В. Никишин (Компания "Лаборатория Касперского")

Показано, что при использовании преимуществ промышленного Internet и облачных технологий необходимо помнить не только о функциональности новых устройств, но в первую очередь об их кибербезопасности.

Ключевые слова: Internet вещей, облачные технологии, кибербезопасность, угрозы, АСУТП.

В последнее время разговоры об использовании Internet в промышленности плавно перетекли в разговоры об использовании промышленного Internet. То есть вопрос подключаться или не подключаться к Всемирной сети сегодня уже нет смысла обсуждать, — так или иначе практически любое предприятие имеет выход в Internet и использует различные сервисы, повышающие производительность, например, облачные технологии или так называемые «большие данные». И вот теперь настало время сделать следующий шаг — навстречу промышленному Internet вещей. А это значит принять те плюсы, которые несет с собой всеобщая информатизация, и перейти на использование соответствующего оборудования.

Вместе с тем, сделав шаг в этом направлении, предприятия не только получат массу преимуществ, но также столкнутся с новыми рисками. Раньше угрозу непрерывности производственного процесса создавал выход из строя оборудования, саботаж, реализованный путем физического доступа к оборудованию, и пр. В эпоху промышленного Internet угроза саботажа никуда не исчезает, однако теперь для этого злоумышленникам не нужен физический контакт с оборудованием — они могут добиться своего путем кибератаки. Например, если у устройства есть USB, то возможно внедрить вредоносный код через подключение зараженной флешки. Исходя из конкретной ситуации, этот риск может выливаться в различного рода сценарии: кибершпионаж, шантаж с целью получения выкупа, остановка производственного процесса и т.д.

К сожалению, безопасность сегодня не является одним из ключевых вопросов, на которые компании обращают внимание при принятии решения, использовать или нет промышленный Internet. Причина проста: обычно от внедрения «умных устройств» видят скорее преимущества, чем риски. Более того, многие производители оборудования до сих пор пренебрегают обеспечением его должной киберзащитой. Хотя все же стоит заметить, что крупные производители систем промышленной автоматизации за последние годы сделали огромный шаг навстречу кибербезопасности.

И все же в большинстве своем производители и некоторые интеграторы индустриального оборудования используют возможность подключения к Сети как некое преимущество, которое, с одной стороны, повышает их продажи, а с другой — повышает производительность их заказчиков. Казалось бы, всем хорошо. Однако при этом и заказчики, и поставщики забывают об одном важном моменте — подключенное к Сети устройство перестало быть изолированным или чисто физическим устройством. Оно стало киберфизическим устройством со всеми вытекающими отсюда последствиями.

В отличие от оборудования доцифровой эпохи устройства Internet нельзя настроить и отладить раз и навсегда, обеспечив тем самым их безопасное использование. Теперь у предприятий есть новое измерение безопасности — информационная безопасность [1–4]. Устройство из серии промышленного Internet будет кибербезопасным до тех пор, пока в нем не будет обнаружена уязвимость или пока злоумышленники не изобретут новый метод атаки. Для кибербезопасности устройства его ПО нужно все время обновлять. А инженеры, которые привыкли работать с функциональной безопасностью, зачастую не понимают и не учитывают этого. И последствия могут быть (и даже уже бывают) самыми плачевными.

При этом речь о подключении к Сети не просто компьютеров, набитых цифровыми данными, а устройств, управляющих реальными производственными процессами — перекачкой нефти, сборкой автомобиля, выплавкой стали, выработкой электроэнергии и т.д. Несложно представить себе последствия успешной кибератаки на такую систему. Для наглядности приведем пример атаки на сталелитейный завод в Германии в 2014 г., в результате которой была остановлена сталеплавильная печь. Восстановить ее не удалось, потребовалась замена. Другой пример: атака BlackEnergy на энергетическую компанию в украинском Ивано-Франковске в конце 2015 г. оставила без электричества примерно 220 тыс. потребителей.

Специалисты «Лаборатории Касперского» в конце 2015 г. проводили эксперимент, в ходе которого состоялся «показательный взлом» стенда электроподстанции, построенной по современным технологиям в соответствии со стандартом IEC61850. Попробовать себя в роли хакеров-злоумышленников согласились несколько специалистов по информационной безопасности. При этом они не были экспертами в промышленном оборудовании, которое им предстояло "взломать". Целью мероприятия было изучение критически значимых векторов атак против инфраструктуры предприятия и проверка эффективности новой технологии компании по детектированию подобных атак. В результате уже через 3 часа «кибертеррористы» устроили на подстанции короткое замыкание,

причем сразу двумя способами, а всего за 2 дня стенд взломали 26 раз, остановив технологический процесс и нарушив работу абсолютно всех устройств.

Подобных реальных инцидентов на производствах уже довольно много. Отчасти подобные происшествия скрываются от общественности операторами производственных и инфраструктурных предприятий, но еще больше инцидентов остаются незамеченными долгие годы. Например, тот же вирус Stuxnet успешно работал несколько лет, прежде чем остановил производство по обогащению урана в Иране и был обнаружен.

Корень проблем лежит в неверной оценке рисков от подключения оборудования и предприятий к Сети или полном отсутствии такой оценки. Люди привыкли, что важно соблюсти функциональную безопасность и безопасность труда, а о кибербезопасности забывают. В результате технологические сети уязвимы. В наличии устаревшие протоколы обмена данными без авторизации и идентификации пользователя (Modbus, Fieldbus, DPN3, Profibus), отсутствие шифрования данных, большое число найденных и возможных уязвимостей остаются незакрытыми. В какой-то мере это объясняется особенностями функционирования индустриальных объектов с их большим циклом замены оборудования, фокусом на непрерывность процессов. Однако в итоге вся эта ситуация приводит к тому, что взломать технологическую сеть объекта критически важной инфраструктуры становится проще, чем сеть среднего офиса.

Таким образом, предприятия, решающиеся на промышленный Internet, должны понять и признать, что киберугрозы реальны и исходящие от них риски необходимо учитывать при планировании новой системы. Кроме того, имеет смысл провести аудит кибербезопасности предприятия, чтобы узнать, как же на самом деле обстоят дела с подключенным оборудованием, и уже на основании этого аудита корректировать меры, направленные на снижение риска столкновения с киберугрозами. Также на промышленных предприятиях кроме инструктажа по технике безопасности необходимо проводить и инструктаж по кибербезопасности.

В свою очередь, производители промышленного оборудования должны признать, что новые устройства из мира Internet вещей надо проектировать по-новому, с оглядкой не только на функциональную, но и на информационную безопасность. Для устройств Internet вещей сделать «навесную» защиту дорого, сложно, а порой и вовсе невозможно. Единственный способ обезопасить такое устройство — это сделать его безопасным изначально, оно должно быть произведено с учетом требований безопасности. Но для каждого устройства эти требования разные, они зависят от свойств устройства, его характеристик, коммуникационных возможностей, предназначения. В связи с этим для каждого устройства на этапе разработки его концепта необходимо создавать модель угроз, на основании которой уже можно понять, какие требования безопасности нужно применить конкретно к этому устройству. И только после этого стоит разрабатывать конечный продукт.

Справедливости ради отметим, что сегодня производители оборудования все же начинают задумываться о безопасности. И с ростом использования описанной выше методологии безопасной разработки ПО мы будем получать все больше и больше безопасных устройств, что ускорит процесс их внедрения в промышленности.

Список литературы

1. *Арефьев А.С.* Таргетированные атаки на промышленный сектор: новое оружие в кибервойне // Автоматизация в промышленности. 2015. №2.
2. *Шипулин А.С., Соболев А.Ю.* Мониторинг активности в промышленных системах и сетях как безопасный подход к борьбе с киберугрозами // Автоматизация в промышленности. 2015. №2.
3. *Бадеха И.А.* Актуальные вызовы и адекватные подходы к обеспечению информационной безопасности АСУТП//Автоматизация в промышленности. 2015. № 2.
4. *Белов В.С., Брызгин А.А.* Безопасность (и/или) АСУТП//Автоматизация в промышленности. 2015. № 2.

Никишин Андрей Викторович *– руководитель отдела развития технологический проектов "Лаборатории Касперского".*
Контактный телефон +7 (495) 797-87-00.