ВЫВОД КОЛИЧЕСТВЕННЫХ ЗНАЧЕНИЙ ИЗ ДАННЫХ ОТ УСТРОЙСТВ IIoT

ЭРИК ДЖ. БАЙРЕС (ERIC J. BYRES)

Сам по себе сбор данных от устройств технологии промышленного «Интернета вещей» (англ. Industrial Internet of Things, IIoT) малопродуктивен и недостаточен. Проблема заключается в том, что компании, занятые обработкой полученных сведений, должны знать, что с ними делать, и иметь твердую гарантию того, что данные не были искажены.

Одна из самых больших проблем, связанных с распространением технологии промышленного «Интернета вещей», заключается в том, что нам необходимо знать, как извлечь выгоду из огромного потока данных, полученных в результате ее внедрения.

Хотя получение большого объема данных не является самоцелью внедрения технологии индустриального «Интернета вещей», он легко может стать побочным продуктом IIoT, и этот факт может быстро нивелировать выгоды от использования столь прогрессивной технологии. Иметь слишком много данных — малопродуктивно и даже способно стать отвлекающим и мешающим фактором. Успешная интерпретация данных и их перевод в полезную информацию — процесс, который основан на опыте, обучении и аналитике, но самое главное в нем — четко задать определенную стратегию применения полученной информации. Вот почему целью IIoT является не только сбор данных, но и точное понимание того, что с ними делать.

На крупнейшей конференции и выставке 2016 года в области «Интернета вещей» — IoT Tech Expo — Билл Браун (Bill Brown) из компании Stanley Black & Decker поделился своими мыслями о том, как целенаправленная работа в рамках IIoT улучшила одну из программ обслуживания продуктов его компании.

Компания Stanley Black & Decker производит автоматические раздвижные стеклянные двери, которые часто используются в большинстве супермаркетов и целом ряде других магазинов. До развертывания системы прогнозирования в рамках IIoT обслуживание таких дверей оказалось сложной задачей для торгующих организаций, сказал Браун. Поэтому компания Stanley Black & Decker запустила проект IIoT для сбора информации о функционировании своих дверей.

«Теперь нам не нужно ждать, пока двери перестанут работать и кто-то позвонит и скажет нам об этом, — подчеркнул Браун. — Мы можем просто посмотреть и увидеть, когда что-то пошло не так или один из моторов стал нагреваться больше других». В результате такого подхода Stanley Black & Decker удалось сократить текущие затраты и повысить удовлетворенность клиентов благодаря увеличению надежности продуктов, выпускаемых компанией.

РЕАЛЬНЫЕ ВЫГОДЫ И РЕАЛЬНЫЕ РИСКИ

Пример компании Stanley Black & Decker демонстрирует и то, что технология IIoT может служить не только целям сервисной поддержки, но и решать комплексные проблемы, связанные с безопасностью. Двери можно рассматривать как своеобразные межсетевые экраны мира физической безопасности, они могут контролировать, кто входит или выходит из здания. Подобно брандмауэрам, мониторинг их активности и сопоставление полученной

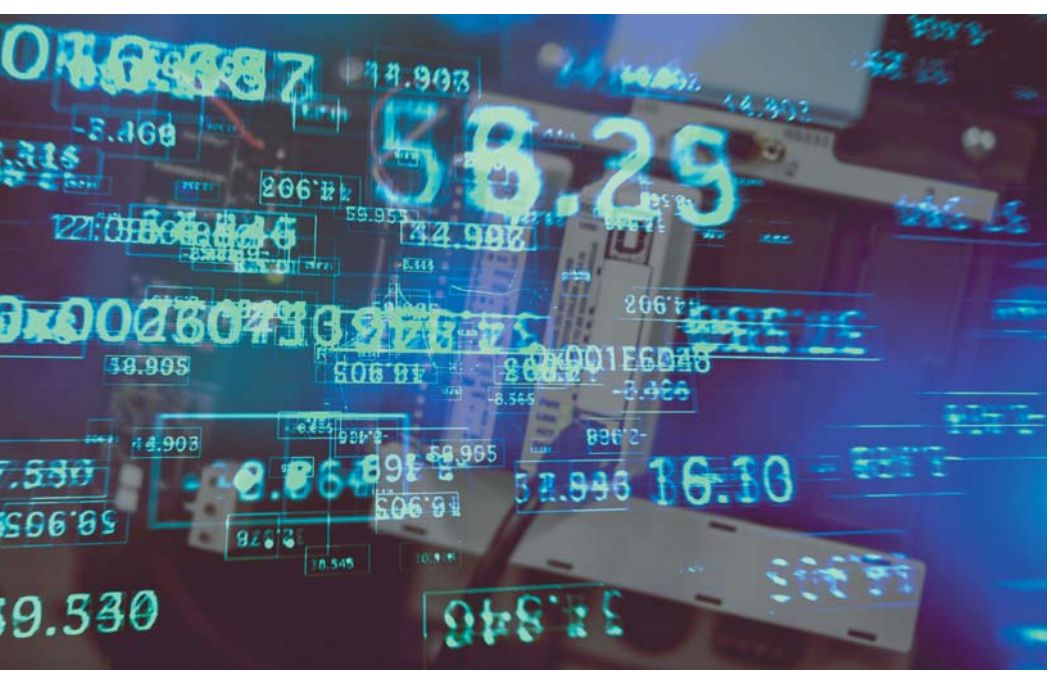
информации с данными от других систем (например, видеонаблюдение или отслеживание перемещения инвентаря и оборудования) может значительно повысить безопасность и сократить общие текущие потери.

Проекты в области IIoT (как и приведенный в качестве наглядного примера опыт компании Stanley), первоначально предназначенные для повышения оперативности технического обслуживания, со временем могут быть интегрированы и в другие бизнес-системы. Причем сделать это можно совершенно разными способами, в том числе и не предусмотренными командой, первоначально работавшей над данным проектом. Именно возможность легко интегрировать информацию устройств технологии индустриального «Интернета вещей» в несколько систем имеет решающее значение для реализации и раскрытия всего потенциала IIoT.

Но общая забота о людях должна учитывать и тот факт, что взаимосвязанный характер использования технологии IIoT может подвергнуть активы компании новым и сложным внешним атакам. Это действительно важно, поскольку неконтролируемый обмен информацией в рамках IIoT несет риски. Что делать, если плохая организация в сфере кибербезопасности позволяет преступникам получить доступ к данным по операциям с дверьми? Могут ли злоумышленники использовать такой доступ для планирования (в частности, узнать, когда дверь снимается для технического обслуживания) или сокрытия преступлений, например путем подделки журналов активности (логов)?

Плохая организация системы безопасности может также препятствовать подтверждению достоверности полученных данных, приводя к сценарию «мусор на входе — мусор на выходе» (принцип, согласно которому программа выдает бессмысленные результаты при бессмысленных входных данных). Даже простая фальсификация незащищенных логов, полученных на начальном уровне, может дать неверное представление о том, что же происходит в реальности. В то же время плохое управление данными способно привести к еще более серьезным последствиям, включая утечку конфиденциальных сведений или секретных активов.

Устойчивая и надежная система безопасности освобождает сеть от ложной и преднамеренной перегрузки данными, обеспечивает стабильность и расширенные возможности функционирования. Сама по себе технология — это лишь инструменты, которые вы выбираете и используете. А безопасность — то, что позволяет вести процесс в защищенной среде, ставя на пути злоумышленника прочный барьер. Кстати, всегда следует помнить, что безопасность как таковая никогда не должна реализовываться задним числом. Привлекая к работе экспертов по безопасности, вы должны не только представить им свои планы по созданию архитектуры, но и обеспечить их проверку с соблюдением всех требований, с подписанными и юридически весомыми гарантиями полного соблюдения конфиденциальности. Таким образом вы получите уверенность в том, что сделали все необходимое еще до запуска соответствующих проектов.



КАК ДОЛЖНА БЫТЬ ПОСТРОЕНА НАДЕЖНАЯ ЗАЩИТА

Самые лучшие системы IIoT — те, что были разработаны с учетом требований по безопасности и надежности. Они содержат такие элементы, как автоматические функции обеспечения отказоустойчивости путем самовосстановления системы, повышенная устойчивость к кратковременным отказам и контроль безопасности в рамках функционирования предприятия.

В своем выступлении Браун пояснил, что развертывание IIoT в Stanley Black & Decker не могло быть основано на облачных технологиях — компании было необходимо обеспечить возможность работать в служебных помещениях. Он объясняет это требование следующим образом: «Если интернет-соединение будет прервано, ваша система должна продолжать функционировать». Такие эксперты, как Стивен К. Венема (Steven C. Venema), главный архитектор систем безопасности в компании Polyverse Corp., рекомендуют пересмотреть стандарты ISA/IEC 62443 (ранее известные под названием ISA99). Это нужно, чтобы сформировать предварительную «дорожную карту» для перехода к многораздельным архитектурам для домена ICS/SCADA (ICS — industrial control systems, системы управления производственными процессами; SCADA — Supervisory Control And Data Acquisition, комплексная автоматизированная система диспетчерского управления). «Разделите оборудование и систему, — сказал Венема. — Это даст гарантию того, что компоненты безопасности будут обновляться

быстрее, чем другие операционные элементы системы».

Стандарт ISA/IEC 62443 — комплексный документ, который иногда также называют полной программой жизненного цикла безопасности для промышленной автоматизации и систем управления. Он состоит из одиннадцати стандартов и технических отчетов, вводит понятие зон, представляющих собой группировки логических или физических активов, которые используются совместно, и содержит общие требования безопасности, основанные на критичности, последствиях и других подобных факторах. Оборудование в зоне должно совместно использовать мощные возможности уровня безопасности и каналы, которые являются путями для информационного потока между зонами. Стандарты ISA/IEC 62443 также обеспечивают требования, основанные на оценке компанией рисков кибератак и уязвимостей.

В контрольном списке требований по выполнению условий безопасности в рамках IIoT необходимо разработать стратегию для обеспечения и реализации следующих упреждающих и защитных мер:

- Внедрению мер обеспечения безопасности необходимо уделить особое внимание с самого начала проекта. Никогда не оставлять эту работу на потом, чтобы не пришлось заниматься ею впопыхах.
- Заручиться поддержкой экспертов. Организовать сотрудничество представителей высшего руководства и специалистов по безопасности, которые могут общаться и работать вместе, это позволит сформировать стратегию по созданию защитных мер, которые будут предназначены как для предприятия в целом, так и для любых продуктов и услуг (сервисов).
- Разделить на категории IIoT в зонах безопасности. Это поможет предотвратить распространение вредоносных программ по всему предприятию. Кроме того, следует интегрировать лучшие практики безопасности на каждом этапе процесса разработки системы предприятия.

Вести постоянный контроль и мониторинг системы IIoT, что позволит понять уязвимости и управлять возникающими угрозами. Необходимо выявлять проблемы как можно раньше.

Система на базе технологии IIoT не должна быть сырой или экспериментальной. Она должна быть спроектирована максимально надежной, с постоянно обновляющимися функциями безопасности. Все, что касается безопасности, должно своевременно отслеживаться и обновляться. В противном случае данная система не будет ничем отличаться от установки обычной системы охранной сигнализации в доме и ничто не помешает ее деактивировать.

Как сказал Вимал Капур (Vimal Kapur), президент компании Honeywell Process Solutions, «IIoT — это эволюция... она переносит унаследованные системы в эпоху новых технологий, чтобы использовать в своих интересах все, что должны принести нам новые технологии и возможности подключения».

ПОЛУЧЕНИЕ ДОСТУПА К ИНФОРМАЦИИ

В своей основе технология IIoT представляет собой стратегию, которая базируется на более быстром принятии решений, основанных на видении перспективы. Это новый способ изучения любой имеющейся проблемы. У нас и раньше всегда были результаты тестирования данных, аналитика, информация об управлении активами и техническом обслуживании. Однако сведения поступали постфактум, в текущих операционных процедурах информация часто была недоступна, упускалась из виду или была скрыта.

Если мы сможем правильно реализовать стратегию безопасности, то у нас появится возможность переосмыслить, как индустрия интегрирует данные, которые буквально находятся в недрах производственного процесса.

Ведущие компании цифрового будущего станут решать свои проблемы и реализовывать возможности через технологию IIoT, используя данное конкурентное преимущество для того, чтобы обеспечить быстрый рост компании и ее устойчивый успех на рынке. Внедрение технологии IIoT обеспечивает немедленную экономическую выгоду, а также повышение надежности и сокращение простоев оборудования. Одновременно, благодаря переходу количества в качество в области информации, она предоставляет и долгосрочные преимущества, создавая платформу для постоянного развития, предполагая большую отдачу от вложенных инвестиций.

Создавая прогрессивную культуру компании, поддерживая корпоративную направленность и разрабатывая системы IIoT с соответствующими мерами безопасности, бизнес может преодолеть препятствия и стратегически реализовать лучшие практики IIoT, что позволит получить огромное конкурентное преимущество в цифровом будущем. ⬢