КИБЕРУЯЗВИМОСТЬ «УМНЫХ» ПРОИЗВОДСТВ

ЕКАТЕРИНА ТРОФИМОВА
ekaterina.trofimova@fsmedia.ru

Чтобы создать суперсовременный завод, необходимо прежде всего развернуть прогрессивную ИТ-инфраструктуру. Однако «прямолинейное» внедрение новых технологий, без учета требований информационной безопасности, может привести к серьезным проблемам на производстве, вплоть до техногенных катастроф. Предлагаемый материал основан на статье известной американской журналистки Энн Филд (Anne Field).

По данным исследования, проведенного Глобальным центром цифровых преобразований бизнеса (Global Center for Digital Business Transformation), цифровая революция в ближайшие пять лет вытеснит с рынка 40% компаний, занимающих лидирующее положение ныне. Тем не менее 75% из них еще только предстоит минимизировать эти риски, уделив первостепенное внимание своей цифровой стратегии.
Для сохранения конкурентоспособности предприятия таких отраслей, как обрабатывающая промышленность, транспорт, энергетика и нефтегазодобыча, должны наращивать производительность, повышать качество обслуживания заказчиков и потребителей. Этому мешает, прежде всего, операционная обособленность, т. е. факторы, разделяющие людей, машины, системы, информацию и целые сферы бизнеса, которые рассматривают информационные технологии вне технологий операционных.

В начале прошлого года в Чикаго (США) приступил к работе Институт по инновациям в сфере цифрового производства и промышленного дизайна (Digital Manufacturing and Design Innovation Institute, DMDII). Его общая площадь составляет почти 9 тыс. кв. м, при этом примерно треть пространства отведена под лабораторию, изучающую проблемы «интеллектуальной» промышленности. Задача лаборатории — ускорить развитие информационных технологий для так называемых «умных» производств.

Институт ориентирован на серьезные научные исследования по нескольким направлениям, причем одно из них никак не связано с разработкой и производством товаров. Речь идет об информационной безопасности (ИБ). В рамках данного направления изучаются проблемы определения и предотвращения специфических киберугроз, нацеленных на «умные» производства. Само собой, такие проблемы необходимо решить до того, как производители начнут активно применять «умные» технологии.

DMDII — едва ли не единственная организация, всерьез озабоченная решением таких проблем. Производственная деятельность стремительно развивается: увеличивается степень цифровизации, растет роль информационных систем и обработки данных в сфере разработки, происходит цифровое объединение производства и его поддержки, — и это является поводом говорить не только о преимуществах, но и о рисках.

Неосторожное (неквалифицированное) внедрение новых технологий может повлечь за собой катастрофические последствия — от хищения конфиденциальных данных до полного паралича производства. «Ситуация, когда цифровая деятельность напрямую влияет на физические производственные процессы, потенциально опасна: не имея надежных средств обеспечения ИБ, нельзя гарантировать полную защищенность бизнес-процессов», — говорит Ларри Джон (Larry John), старший аналитик из Analytic Services, некоммерческого исследовательского института. Именно этим объясняется то, что все больше исследователей, а также правительственные структуры и государственно-частные консорциумы усиливают деятельность по изучению уязвимости и поиску надежных методов противодействия кибератакам.

Очевидно, что новые средства киберзащиты невозможно тестировать в условиях реального производства, поскольку это может повлечь за собой замедление и даже остановку производственных процессов, что совершенно неприемлемо для бизнеса. По этой причине такого рода работа включает в себя этап прикладных исследований, на котором инженеры-разработчики используют специальное оборудование, по мере возможности имитирующее реальные производственные процессы.

К примеру, Национальный институт стандартов и технологий США (National Institute of Standards and Technology, NIST) занимается созданием лаборатории, способной измерять влияние систем ИБ на производительность промышленных предприятий. Как утверждает руководитель проекта по ИБ автоматизированных систем управления (АСУ) Кит Стуффер

АСУ ТП критически важных объектов особенно сейчас, в эпоху «цифровизации», находятся под угрозой со стороны киберзлоумышленников. В связи с этим защита их ИТ-инфраструктуры приобретает особую важность. Андрей Духвалов, руководитель управления перспективных технологий ЗАО «Лаборатории Касперского», считает, что основным критерием защищенности интеллектуального производства является способность всей структуры АСУ ТП к поддержанию стабильного, непрерывного и корректно работающего технологического процесса в рамках предопределенных ограничений и независимо от внешних воздействий. «Именно технологический процесс (выработка и передача электричества, транспортировка газа, переработка руды, очистка воды, управление городскими коммунальными службами и т. д.) является основной функциональностью таких объектов, а поддержание его корректного функционирования и есть ключевая задача всех ИТ-систем».

(Keith Stouffer), эта лаборатория будет, помимо прочего, ориентирована на проблемы роботизированного производства и промышленных систем автоматизации на предприятиях химической отрасли. Основная задача лаборатории — убедиться, что системы ИБ не только надежно функционируют, но и не снижают производительность предприятия. На специальной лабораторной площадке собраны полностью функциональные линии роботизированного производства и АСУ, соединенные с рабочей моделью химического завода.

ИТ-БЕЗОПАСНОСТЬ VS БЕЗОПАСНОСТЬ АСУ ТП

Независимо от того, каким путем злоумышленник проникает в систему, существует ряд причин, способствующих тому, чтобы этот инцидент вообще мог произойти. Зачастую во многих компаниях полагаются на ИТ-департамент в отношении обеспечения безопасности систем, находящихся в сфере деятельности отделов АСУ ТП. Но здесь имеет место расхождение в видении целей: «айтишник» считает, к примеру, конфиденциальность данных первостепенной задачей, а «производственник» фокусирует свое внимание прежде всего на безопасности людей и завода. Это различие на практике влечет за собой огромную разницу в методах защиты. Например, применение стандартной процедуры блокирования при помощи пароля неприемлемо для большинства операторских станций — здесь гарантированный доступ для диспетчеров по умолчанию требуется в большей степени, нежели блокировка, что противоречит традиционным представлениям специалистов по ИБ.

Эти работы ведутся на базе системы киберзащиты, разработанной около года назад NIST в сотрудничестве с государственными организациями и представителями разных индустрий. Система рассчитана на 16 областей, включая химические компании, энергетический сектор и электротехническое производство, и состоит из следующих компонентов:

- определение процессов и активов, нуждающихся в защите;
- защита процессов и активов посредством механизмов обеспечения безопасности и контроля;
- обнаружение нарушений систем защиты;
- противодействие нарушениям ИБ с использованием методов, способных обеспечить контроль над любыми возможными инцидентами;
- возобновление нормальной работоспособности с помощью технологий восстановления системы.

В Национальной лаборатории Айдахо (Idaho National Laboratory, INL), действующей под эгидой Министерства энергетики США (DOE), исследователи занимаются изучением различных аспектов того, что Крейг Ригер (Craig Rieger), старший исследователь лаборатории, называет «отказоустойчивыми системами контроля». В числе прочего эти исследования включают вопросы информационной безопасности.

В частности, лаборатория работает над проблемами улучшения сенсорных систем обнаружения и предотвращения вторжений. Одно из направлений этой работы состоит в создании специальных меток разнообразных атак, что облегчит обнаружение в случае, если атака повторится. Другой подход — отслеживание любых отклонений от заранее заданного, нормального хода работы систем. Исследователи INL пытаются создать взаимодополняющие системы обнаружения, которые будут использовать специальную физическую модель для определения базового уровня функционирования.

К примеру, инженеры могут заблаговременно определить температурный режим работы промышленной печи. Если они разработают, скажем, схему теплопередачи для определенных температур и определенных процессов, то получат возможность использовать эту схему для выявления изменений в уровнях нагрева, что позволит своевременно распознать возможную компрометацию системы. Таким образом, можно будет диагностировать как неполадки с самой печью, так и проблемы в соответствующих компьютерных системах.

Создается специальная физическая модель для определения базового уровня функционирования, внедряют сенсоры, позволяющие вести наблюдение за определенной частью устройства. Система сможет опрашивать эти сенсоры и получать информацию о состоянии рабочих процессов. В случае если по каким-то причинам будет невозможно считать показатели какого-то сенсора (например, термодатчика), система воспользуется другим датчиком и преодолеет возникшую проблему. Или же система сможет сопоставить схему теплопередачи и данные другого, исправного сенсора, расположенного достаточно близко, чтобы определить температуру в точке возникновения проблемы. Печь продолжит функционировать, рабочий процесс останется в пределах нормы. При этом соответствующие специалисты будут знать, что один из сенсоров неисправен.

Ведутся и долгосрочные исследования в интересах дальнейшего развития этого направления. Помимо разнообразных средств обнаружения инцидентов ИБ, системы будут оснащаться дополнительными сенсорами, предназначенными для контроля промышленных операций. Это позволит продолжать работу производственной линии и в то же время информировать операторов о том, что специалистам ИБ необходимо провести работы по выявлению возможной компрометации системы.

* * *

Проблема ИБ на промышленных предприятиях стоит очень остро. Ее значимость повышается с внедрением инновационных цифровых решений. Но риски возможно максимально снизить, если уделять этому аспекту пристальное внимание и использовать решения по защите, которые уже существуют на рынке.

ЛИТЕРАТУРА

1. http://newsroom.cisco.com/cybersecurity2016
2. http://thenetwork.cisco.com/
3. http://cyberleninka.ru/article/n/kiberataki-na-kriticheski-vazhnye-obekty-veroyatnaya-prichina-katastrof#ixzz3yYPB9ZQc
4. www.modcon.ru/wp-content/uploads/2014/08/Ind-Security.pdf