КИБЕРБЕЗОПАСНОСТЬ АКТИВОВ НЕФТЕГАЗОВОЙ ОТРАСЛИ

РУСЛАН СТЕФАНОВ
Ruslan.Stefanov@Honeywell.com

Предприятия нефтегазовой отрасли все шире внедряют цифровые технологии. Неотъемлемой составляющей этого процесса должно стать применение лучших практик кибербезопасности.

ЭФФЕКТИВНАЯ КИБЕРЗАЩИТА — УСЛОВИЕ УСПЕШНОЙ ЦИФРОВИЗАЦИИ

В нефтегазовой отрасли сложилось четкое понимание того, что технологии промышленного «Интернета вещей» (англ. Industrial Internet of Things, IIoT) — это неотъемлемое условие конкурентоспособности, а реализация таких концепций, как «подключенное предприятие» (Connected Plant) и «умное месторождение» (Smart Field), напрямую влияет на прибыльность. Новые инструменты существенно увеличивают производительность и усиливают безопасность производств, повышают качество и снижают себестоимость продукции. Даже скептики согласны с тем, что отказаться от внедрения инновационных технологий уже невозможно и в будущем уровень цифровизации будет только расти.

В то же время в контексте цифровой трансформации нельзя забывать о сопровождающих этот процесс киберугрозах. Чем более «подключенным» становится предприятие, тем острее стоит вопрос обеспечения его безопасности. Количество киберпреступлений во всем мире ежегодно увеличивается. Действия злоумышленников могут вызвать остановку производства, утечку конфиденциальных данных и, как следствие, финансовые и репутационные потери. В худших случаях хакерские атаки могут привести к экологическим катастрофам и человеческим жертвам.

Руководство предприятий зачастую не осознает масштабы проблемы из-за недостатка знаний и опыта в новой для него области и продолжает пользоваться устаревшими подходами к обеспечению кибербезопасности. Об этом свидетельствуют результаты исследования [1], проведенного компанией LNS Research по заказу Honeywell в 2017 г. В опросе приняли участие 130 руководителей малых и крупных предприятий нефтегазовой, машиностроительной и других отраслей промышленности из Северной и Южной Америки, Азиатско-Тихоокеанского региона, Европы, Ближнего Востока и Африки. Более половины из них отметили, что на предприятии, где они работают, уже были попытки взлома системы безопасности. При этом 45% респондентов сообщили, что в их компаниях еще не назначен руководящий сотрудник, ответственный за киберзащиту. Также выяснилось, что только 37% компаний отслеживает подозрительную активность в сети, а 20% предприятий даже не проводит регулярную оценку рисков. Подчеркнем, что речь не идет о технологически отстающих

компаниях: примерно 64% респондентов сообщили, что уже начали или в ближайшем году начнут внедрение технологий IIoT.

Атаки вирусов-шифровальщиков (например, WannaCry и Petya.C) уже затронули и крупнейшие российские нефтегазовые компании, однако эксперты полагают, что сегодня мы наблюдаем только самое начало эпохи киберпреступлений, а ее расцвет еще впереди. Согласно прогнозам исследовательской компании Cybersecurity Ventures, к 2021 г. глобальный ущерб от киберпреступлений вырастет до $6 трлн в год. При этом расходы компаний на кибербезопасность увеличатся до $1 трлн. Параллельно возникнет нехватка специалистов в сфере информационной безопасности: работодатели не смогут закрыть до полутора миллионов вакансий. По всей вероятности, в сфере кибербезопасности промышленных объектов дефицит квалифицированных кадров будет ощущаться еще острее, а ущерб от успешных атак составит большую долю общих потерь. Попробуем понять, почему ситуация развивается в этом направлении и что необходимо предпринять, чтобы ее изменить.

УЯЗВИМОСТЬ ПРОМЫШЛЕННЫХ СЕТЕЙ

До возникновения IIoT и тренда на подключение элементов производства к сети специалисты по АСУ ТП не сталкивались с киберугрозами. Неудивительно, что при обучении и инструктаже операторов, управляющих техпроцессами, максимум внимания традиционно уделяется правилам промышленной безопасности и охраны труда, но почти никто не говорит об информационной безопасности. В результате производственный персонал нередко относится к мерам по повышению кибербезопасности без должного внимания и не использует их. Например, сотрудники, не обученные основам промышленной кибербезопасности, могут подключить к связанному с АСУ ТП компьютеру принесенный с выставки рекламный USB-носитель или персональное мобильное устройство, тем самым создав риск заражения всей сети. В то же время сложно винить в этом рядовых сотрудников, если в организации отсутствует политика киберзащиты, поддерживаемая и контролируемая руководством.

С другой стороны, одной из главных причин уязвимости промышленных сетей является устаревшее программное обеспечение и несвоевременное обновление антивирусных программ. Если в сфере ИТ программы и оборудование обновляются регулярно, то многие технологические установки до сих пор работают под управлением Windows XP, выпущенной в 2001 г. Конечно, такая операционная система не может учитывать современные угрозы и не позволяет установить ряд важных обновлений безопасности (для исправления ошибок в программе). Проектировщики большей части оборудования АСУ ТП не могли ориентироваться на сегодняшний уровень «подключенности» устройств и не предусмотрели легкое и быстрое обновление ПО.

Ситуация усугубляется тем, что в промышленных системах, управляющих сложными производственными установками, даже кратковременный сбой влечет за собой очень серьезные последствия. Конечно, внеплановая перезагрузка ИТ-серверов тоже сопряжена с проблемами для пользователей, но все же она менее опасна, чем аварийный останов оборудования, работающего при высоких температурах или с химически активным сырьем.

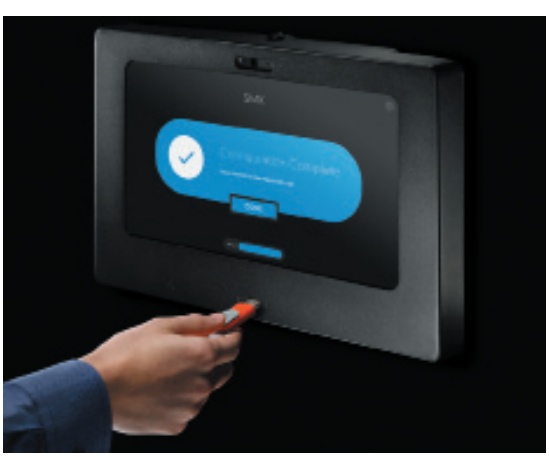
ТРЕБОВАНИЯ К СИСТЕМАМ ПРОМЫШЛЕННОЙ КИБЕРБЕЗОПАСНОСТИ

Чтобы изменить положение дел к лучшему, необходимо сделать вопросы обеспечения кибербезопасности на предприятиях нефтегазовой отрасли неотъемлемой частью цифровой трансформации. Они должны войти в ежедневную рабочую повестку генеральных директоров, учитываться при разработке инвестиционных планов и формировании бюджетов. Также важно обеспечить внедрение лучших практик кибербезопасности применительно к персоналу, процессам и технологиям. Необходимо устранить разобщенность между инженерами и ИТ-специалистами, создать на предприятии подразделение, отвечающее за киберзащиту, и привлечь внешнюю экспертизу для достижения наилучших результатов.

Предприятия нефтегазовой отрасли работают в высококонкурентной среде, поэтому для них важно, чтобы инвестиции в киберзащиту были экономически обоснованы. С учетом этого требования целесообразно перейти от традиционного метода защиты информации, основанного на анализе угроз, к более эффективному риск-ориентированному подходу, который предполагает оценку рисков в денежном выражении. Такая стратегия позволяет правильно расставить приоритеты и в первую очередь направить ресурсы на устранение проблем, наиболее критичных для стабильности производства.

Система промышленной кибербезопасности должна органично встраиваться в общую бизнес-стратегию предприятия и учитываться при модернизации производственных активов. Ее задача — не только минимизировать риски киберугроз, но и обеспечивать компаниям дополнительные преимущества: например, способствовать повышению производительности и безопасности техпроцессов. Также важно, чтобы специалисты, создающие систему кибербезопасности, были способны играть на опережение — предвидеть будущие угрозы и влиять на ход событий, — а не просто реагировали на действия киберпреступников. Это возможно в случае использования современных методов обнаружения (разведки) угроз и обмена информацией о них.

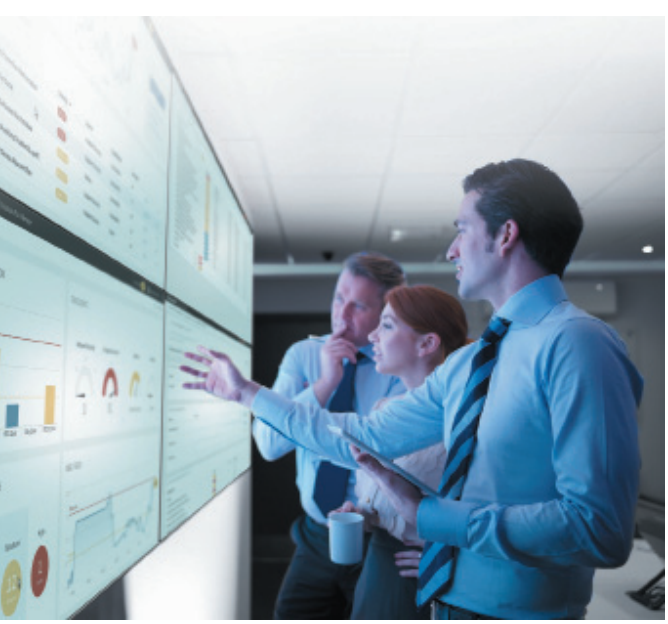
При этом решения, применяемые в системах промышленной кибербезопасности, не должны влиять на технологический процесс и оборудование. Поэтому многие стандартные продукты и подходы, зарекомендовавшие себя в сфере ИТ, непригодны для защиты АСУ ТП.



Здесь нужны специальные способы защиты, учитывающие потребности производства. Иными словами, успеха в защите от угроз можно добиться лишь за счет объединения информационных (ИТ) и операционных технологий (ОТ). А ответственный персонал должен не только обладать компетенциями в сфере кибербезопасности, но и хорошо знать особенности технологических процессов конкретного предприятия.

РЕШЕНИЕ КАДРОВОЙ ПРОБЛЕМЫ

Как отмечалось выше, дефицит квалифицированных специалистов — одна из главных проблем молодой и еще не до конца сложившейся отрасли промышленной кибербезопасности. Даже компетентному в сфере киберзащиты персоналу требуется достаточно много времени, чтобы разобраться со спецификой конкретного производства. Предприятиям приходится вкладывать значительные ресурсы в обучение, потому что найти готовых специалистов на эти позиции трудно. А с учетом того, что большая часть российских нефтегазовых активов находится вдали от столицы, в зонах с суровым климатом и неразвитой социальной инфраструктурой, привлечение квалифицированных сотрудников и создание полноценной службы, ответственной за киберзащиту, превращается в весьма дорогостоящую задачу.



Опыт компании Honeywell в области промышленной кибербезопасности показывает, что в такой ситуации клиенты могут выбрать один из двух сценариев решения проблемы: централизовать управление киберзащитой или отдать эту функцию на аутсорсинг, например стороннему центру управления информационной безопасностью (англ. Security Operations Center, SOC). Зачастую предприятию лучше всего подходит комбинация этих подходов.

Первый вариант предполагает, что все территориально разбросанные активы нефтегазовой компании подключаются с помощью защищенного канала связи к центральной операторной. В штабе создается единый центр компетенций по кибербезопасности, работающий в режиме 24/7. Все его сотрудники находятся в тесном взаимодействии, их не разделяют тысячи километров и несколько часовых поясов. Это позволяет команде моментально оповещать друг друга об аномалиях, сообща подбирать оптимальные решения и оперативно внедрять их на практике. В таких условиях новички быстрее входят в курс дела, а с региональных предприятий снимается сложная задача по поиску специалистов.

Но главное — инфраструктуру, разработанную для централизованной киберзащиты, можно использовать для решения широкого круга задач в рамках концепции «подключенного производства». Систему удаленного доступа можно применять для различных видов мониторинга и управления промышленными рисками.

Для компаний, которые стремятся к минимизации штата или имеют ограниченную централизацию, решением кадровой проблемы станет заключение договора с провайдерами услуг в области кибербезопасности. Один из таких провайдеров — подразделение управляемых услуг обеспечения безопасности Honeywell, обслуживающее несколько сотен предприятий нефтегазовой, нефтехимической и целлюлозно-бумажной отрасли. Профильные специалисты хорошо знают специфику этих производств и могут найти оптимальный баланс между производственными приоритетами и требованиями кибербезопасности. При этом внешние эксперты готовы поделиться своими знаниями и накопленной отраслевой статистикой для сравнительного анализа.

Поддержка внешней команды специалистов не только помогает в сложных ситуациях, но и гарантирует, что все базовые, однако отнюдь не менее важные операции (установка пакетов исправлений, управление межсетевыми экранами и системами обнаружения вторжений и т. д.) будут выполняться четко и своевременно. У внутренних команд, сосредоточенных на решении множества разных задач, такие операции порой уходят на второй план и реализуются, «когда появилось время».

Благодаря аутсорсингу даже компании, не обладающие собственными компетенциями, могут пользоваться опытной экспертизой в сфере промышленной киберзащиты. Те же, кто имеет небольшой профильный отдел, могут выбрать модель с частичной поддержкой. Нередко бывает так, что на первых стадиях запуска нового бизнес-направления кибербезопасность полностью отдают на аутсорсинг, а по мере укрепления позиций на рынке начинают наращивать собственные компетенции.

ИНСТРУМЕНТЫ КИБЕРЗАЩИТЫ

Стоит подчеркнуть, что решения для защиты систем автоматизации технологических процессов (или ОТ) имеют свою специфику по сравнению с защитой систем автоматизации бизнес-процессов (или ИТ) и сегодня активно разрабатываются и совершенствуются. Тем не менее уже есть реальные примеры готовых эффективных решений, созданных специально для защиты систем автоматизации технологических процессов.

Примером программного решения для защиты от киберугроз в разветвленных АСУ ТП может служить система Honeywell ICS Shield, которая управляет тысячами промышленных объектов по всему миру. Данная платформа подходит для систем автоматизации с оборудованием и ПО разных производителей. Решение обеспечивает централизованное управление защитой промышленных систем управления, охватывающих несколько территориально удаленных площадок, из единого операционного центра защиты.

Honeywell интегрировала и усовершенствовала технологию ICS Shield

после того, как год назад приобрела компанию Nextnine — одного из ведущих поставщиков решений для киберзащиты промышленных объектов. Эта покупка позволила Honeywell значительно увеличить клиентскую базу и расширить ассортимент решений в сфере защищенного удаленного доступа, мониторинга и киберзащиты АСУ ТП и критической информационной инфраструктуры. Такая интеграция опыта и компетенций двух компаний привела к более широкому внедрению концепции Honeywell Connected Plant.

Компании, продвинутые в сфере информационной безопасности, отличает четкое понимание уровня своей защищенности от киберугроз. Для оценки зрелости имеющейся системы промышленной киберзащиты и управления рисками подходит решение Honeywell Industrial Cyber Security Risk Manager. Оно обеспечивает непрерывную наблюдаемость, проактивную идентификацию уязвимостей и количественную оценку рисков. С помощью интуитивно понятного интерфейса даже несведущие пользователи могут правильно оценить текущую ситуацию, расставить приоритеты и управлять ситуацией в режиме онлайн.

Для защиты промышленных систем от угроз, связанных с применением съемных носителей информации, была разработана технология Honeywell Secure Media Exchange (SMX). Этот пакет позволяет подключать к АСУ ТП только USB-накопители, прошедшие предварительную проверку и регистрацию. Кроме того, данное решение является частью глобальной системы обнаружения (разведки) угроз Honeywell Advanced Threat Intelligence Exchange, что существенно повышает эффективность использования SMX для защиты от кибератак.

ПОВЫШЕНИЕ УРОВНЯ КИБЕРБЕЗОПАСНОСТИ НА НПЗ TOTAL

На примере нефтеперерабатывающего завода (НПЗ) компании Total в Порт-Артуре (США) можно проследить, как предприятие способно в короткие сроки повысить защищенность от киберугроз. Этот крупнейший НПЗ с производственной мощностью 169 тыс. баррелей в сутки, начиная с обнаружения Stuxnet в 2010 г., не раз подвергался хакерским атакам.

В рамках проекта Honeywell провел аудит для выявления основных уязвимостей и источников угроз распределенной системы управления (РСУ) НПЗ. На промышленных предприятиях к ним можно отнести:

- отсутствие политики кибербезопасности и соответствующих процедур;
- использование устаревших антивирусных программ, а также давно выпущенных операционных систем, которые невозможно поддерживать с помощью обновлений и исправлений безопасности;
- архитектура корпоративной сети, реализованная без сегментации;
- нерегулярное и неполноценное резервное копирование данных и др.

В случае с НПЗ Total в Порт-Артуре работу системы, состоящей из примерно 120 серверов и рабочих станций, контролировал небольшой коллектив инженеров. Заказчик принял решение передать управление информационной защитой в руки подразделения управляемых услуг обеспечения кибербезопасности Honeywell.

На первом этапе был создан защищенный канал передачи данных, позволяющий экспертам провайдера удаленно взаимодействовать с системой киберзащиты. Установка патчей и обновление антивирусных программ были автоматизированы. Также была создана система, которая обеспечивает непрерывный мониторинг состояния РСУ, включая контроллеры, серверы и рабочие станции. Помимо этого, была налажена интеллектуальная система оповещений, преобразующая статистику в тренды, которые требуют конкретных действий.

В результате заказчик не только защитил промышленное и сетевое оборудование от кибератак, но и получил дополнительные выгоды, связанные с большей стабильностью и надежностью РСУ, снижением времени простоев и повышением производительности предприятия. По мнению Total, партнерство с Honeywell было экономически целесообразно. Положительный опыт планируется распространить на другие активы компании.

ЗАКЛЮЧЕНИЕ

Примеры ведущих игроков нефтегазовой отрасли показывают, что цифровизация производства невозможна без совершенствования систем кибербезопасности. Для успешной защиты от постоянно развивающихся киберугроз нужен комплексный подход, объединяющий глубокие знания в области производственных процессов и лучшие практики в сфере защиты информации. Важно, чтобы в каждом проекте, реализующем цифровую программу предприятия, вопросы выбора сил и средств киберзащиты обсуждались с самого начала формирования требований проекта.

ЛИТЕРАТУРА

1. www.honeywellprocess.com/en-US/news-and-events/Pages/pr-12062017-honeywell-survey-shows-low-adoption-of-industrial-cyber-security-measures.aspx