White Paper

Кибербезопасность в нефтегазовой отрасли

Содержание

Введение

Нефтяные и газовые компании владеют и управляют основными объектами критически важной инфраструктуры, которые имеют жизненно важное значение не только для деятельности компаний, но и для экономического и военного благосостояния страны. Операции по добыче, переработке и транспортировке сырья являются важнейшими объектами кибератак со стороны злоумышленников с различными мотивами - от личной выгоды до промышленного шпионажа и экономической дезорганизации. Из-за критически важного значения этих объектов нефтегазовые компании также сталкиваются с жесткими требованиями кибербезопасности.

Нефтегазовый сектор всегда был мишенью для злоумышленников. Изначально, вероятность серьезного инцидента из-за кибератака была крайне незначительной, поскольку предприятия обычно придерживались подхода, в соответствии с которым ОТ были изолированы и никогда не интегрировались в системы предприятия.

Однако в нынешнем сценарии появление Интернета вещей (Internet of Things (IoT)) и повсеместное проникновение новых технологий свело на нет базовые допущения о технологии эксплуатации. Уже долгое время промышленные объекты, такие как нефтяные и газовые месторождения, трубопроводы, НПЗ и ГПС уязвимы для кибератак.

В данном документе подробно обсуждаются ограничения и проблемы безопасности, с которыми сталкивается нефтегазовая промышленность, а также подходы, определяющие пути решения этих проблем.

Основные проблемы кибербезопасности

В нефтегазовой промышленности задействованы сложные и трудоемкие процессы. На высоком уровне все процессы в этой отрасли можно разделить на три типа, а именно, Up-stream, Mid-stream, Down-stream. Процессы в нефтегазовом секторе включают в себя разведку, сбор, добычу, переработку, хранение и транспортировку нефти и природного газа. ICS (Промышленные системы управления) и OT (Технологии эксплуатации). используются для управления промышленными операциями и позволяют осуществлять мониторинг и контроль этих операций по всей цепочке создания стоимости.

Автоматизация и диджитализация процесса жизненного цикла производства и дистрибьюции продукции привели к увеличению производительности и снижению затрат. Однако эти процессы также создают следующие препятствия:

- Небезопасное соединение между технологиями эксплуатации и корпоративной сетью, может быть использовано злоумышленником для получения доступа;
- Небезопасный удаленный доступ может позволить злоумышленнику взять под контроль технологические системы и повлиять на производство;
- Отсутствие тестирования эксплуатационных активов на предмет угроз безопасности создает лазейки в системе безопасности;
- Отстутсвие видимости и контроля за ИТ и ОТ активами могут подвергнуть эксплуатируемую сеть рискам киберинцидентов;
- Наличие неинтегрируемых решений, негативно влияющих на отслеживание, обнаружение и предотвращения кибератак.
-

Трансформация многих нефтегазовых компаний из состояния изолированных операционных систем и сред в полностью интегрированный бизнес привела к возникновению множества проблем. Киберинциденты в нефтегазовой промышленности:

- Остановка завода и производственного цикла;
- Утечка конфиденциальной информации;
- Модификация производственных процессов;
- Перебои в работе службы и перебои с поставками.

Комплексный подход, который может объединить безопасность ИТ и ОТ (технологии эксплуатации), является обязательным условием для решения проблем безопасности. Выявление потенциальных угроз и их последствий должны учитываться при создании комплексной системы управления безопасностью, должна оценивать и снижать вероятность воздействия, тем самым существенно минимизируя риски киберицнидентов. Чтобы избежать серьезных киберугроз крайне важно создать устойчивую, надежную и интегрированную систему информационной безопасности.

UP-STREAM

Геологоразведка и добыча

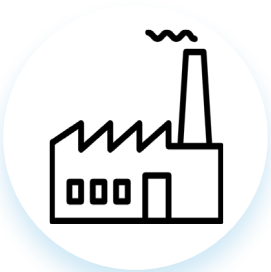
- Буровые работы
- Сепарация
- Оценка и проектирование

MID-STREAM

Транспортировка

- Хранение и распределение
- Обработка и сбор
- Транспортировка

DOWN-STREAM



Переработка и сбыт

- Переработка сырой нефти
- Доставка до потребителя
- Смешивание продуктов

ПРИМЕРЫ

Риск: Несанкционированный доступ к конфиденциальной информации о месторождении

Последствия: Финансовые потери. Утрата конкурентного преимущества

Риск: Несанкционированная модификация трубопроводных систем.

Последствия: Взрыв, утечка, задержка поставок

Риск: Несанкционированная модификация процессов технологий эксплуатации.

Последствия: Нарушение поставок, потеря репутации

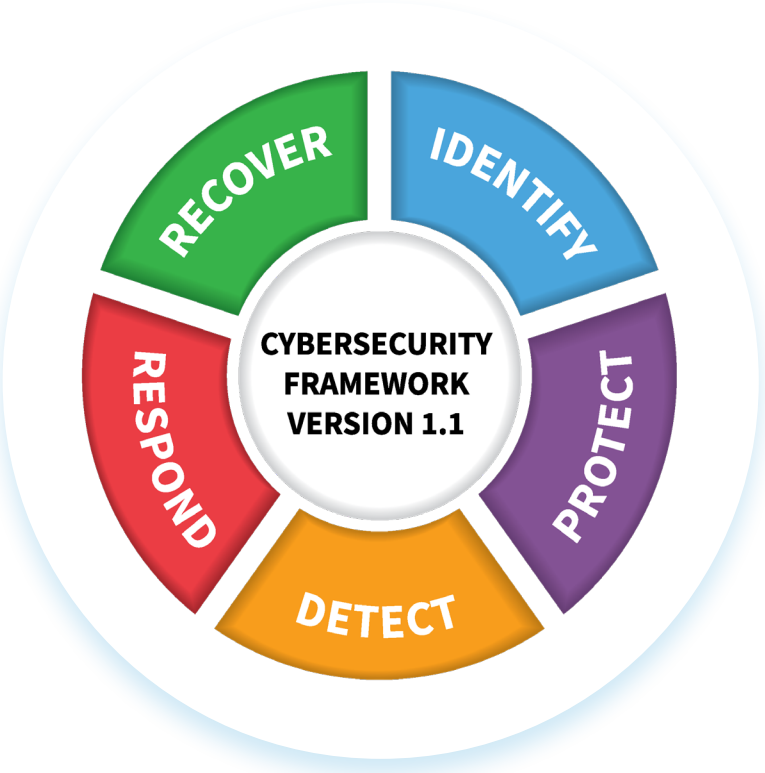
Традиционно, безопасность была главным приоритетом, когда дело доходило до проектирования и развертывания процессов и систем в операционной среде.

Поскольку отрасль сталкивается с новыми вызовами, она вынуждена модернизировать свой подход к кибербезопасности. Организациям необходимо внедрять новые и передовые технологии в сфере информационной безопасности.

Стратегия кибербезопасности для предприятий нефтегазовой отрасли должна представлять собой сочетание практики, процессов и технологий, предназначенных для защиты сетей управления технологическими процессами, систем, компьютеров, программ и данных от компроментации, несанкционированного доступ или неправильноого использования.

Основная цель стратегии - создать операционную среду, способую идентифицировать, обнаруживать, предотвращать и реагировать на киберугрозы, а также восстанавливать данные в случае киберинцидентов.

За основу стратегии информационной безопасности можно взять один из классических фреймворков ИБ (NIST, CIS, Cyber Essentials и др.)



Идентификация

Необходимо четко понимать требования бизнеса и регуляторов. Оценить системы, активы, данные и возможности для управления рисками кибербезопасности. Деятельность в рамках функции идентификации имеет жизненно важное значение для планирования безопасной среды.

Данный этап необходим для определения нынешнего положения организации в области безопасности, потенциальных угрозы и шагов, необходимых для улучшения ситуации и минимизации рисков.

Защита

Разработка и внедрение средств контроля безопасности для обеспечения непрерывности и доступности критически важной инфраструктуры. Мероприятия по защите помогают организации предотвращать вредоносные действия и вторжения в сеть. На основе первого шага определяются меры контроля безопасности для защиты систем.

Обнаружение

Существует вероятность того, что вторжение произойдет даже после внедрения множества средств защиты. Организации должны иметь систему, способную осуществлять раннее обнаружение и снижающую область распространение атаки.

Реагирование

Это ключевой этап, на котором процессы и мероприятия четко определяются, планируются и доносятся до сотрудников. Эти процессы и процедуры создаются и осуществляются для реагирования на все инциденты в киберпространстве. Это позволяет организации ограничить воздействие инцидента, связанного с кибербезопасностью, до минимального уровня.

Восстановление

Этот этап включает в себя внедрение процессов и процедур восстановления после инцидента в киберпространстве. Это позволяет организациям быстро восстановить функционирование ИТ-систем после киберинцидента. Создание и поддержание процедур непрерывности бизнеса является обязательным для любой организации.

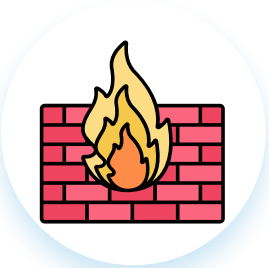
Дорожная карта кибербезопасности

Политики безопасности

Определение и установление политик безопасности, процедур и руководств для среды промышленных систем управления (ISC). Они должна охватывать такие области, как инвентаризация активов, контроль доступа, патч менеджмент, сетевая безопасность, обучение сотрудников, использования съемных носителей. управления инцидентами безопасности, резервное копирование, восстановление и т.д.

Видимость активов

Ведение инвентаризации активов с подробным описанием всех активов, атрибутов, типов и местоположений. Проведение периодических проверок. Обеспечение полной видимости активов OT, включая системы SCADA и полевые устройства, а также мониторинг сети. Мониторинг обеспечивает автоматическое обнаружение, классификацию и управление активами. Он собирает расширенную информацию и детали обо всех устройствах, включая версии ОС и микропрограммного обеспечения, связанные с ними уязвимости и рекомендациями по их устранению.



Сетевая безопасность

Взаимодействие и доступ к среде ICS должны быть определены и приведены в соответствие с потребностями бизнеса. Сегментация сети и безопасные исходные показатели должны соответствовать передовым практикам. Использование соответствующих средства контроля безопасности и технологии, таких как брандмауэры, системы обнаружения и предотвращения вторжений (IDS/IPS) и VPN. Блокирование всех коммуникаций из IT в OT или, если возможно, минимальное соединение через брандмауэр.

Мониторинг

Внедрение платформ безопасности для обеспечения круглосуточного централизованного мониторинга всех инцидентов и событий безопасности. Проведение мониторинга OT в режиме реального времени.

Управление безопасностью

Должна быть разработана, определена и реализована ответственность, функции и обязанности. Рамки обеспечения безопасности являются основой для создания жизнеспособной системы защиты. Настоятельно рекомендуется сосредоточить внимание на выявлении пробелов в управлении в таких областях, как управление доступом, роли и обязанности, управление деятельностью третьих сторон, управление инцидентами, управление исправлениями и уязвимостями, управление политикой и конфигурацией, а также в области резервного копирования и восстановления.

Контроль доступа

Доступ к ИТ-активам в среде ICS, будь то физический или логический, должен осуществляться только с надлежащей аутентификацией и авторизацией. Внедрение цифровых идентификационных данных, механизма привилегированного доступа, безопасного удаленного доступа и централизованного управления паролями может быть использовано для решения основных проблем безопасности в области управления доступом.

Обучение

Регулярные программы обучения и повышения осведомленности в область информационной безопасности должны быть организованы для специалистов каждого уровня, чтобы обеспечить безопасное и ответственное использование информационных систем и данных. Должны быть реализованы непрерывные интерактивные программы оценки и совершенствования знаний, основанные на передовом опыте в области безопасности, а также тренинги на основе симуляторов, демонстрирующих потенциальное воздействие нарушений безопасности в реальных условиях.

Управление инцидентами

Процессы управления инцидентами и реагирования на них должны разрабатываться и тестироваться. Необходимо интегрировать платформы безопасности в существующие централизованные SIEM-решения для разработки тестовых случаев и корреляции событий, связанных с инцидентами безопасности.

Патч менеджмент

Внедрение систематического, подотчетного и документированного процесса управления исправлениями и уязвимостям. Определите рамки управления уязвимостями. Выявите и оцените серьезность новых или существующих уязвимостей и их своевременного и эффективного устранения. Периодический обзор исправлений и уязвимостей должен проводиться для отслеживания состояния безопасности в ИТ-среде.

Чем мы можем Вам помочь?

ООО «НТЦ ЕВРААС», являясь многопрофильной коммерческой структурой, имеет все необходимые лицензии регуляторов рынка информационной безопасности, в том числе лицензии на осуществление работ с использованием сведений, составляющих государственную тайну.

Обладая фундаментальными знаниями и опытом в области защиты информации, эксперты НТЦ «ЕВРААС» предлагают новейшие комплексные разработки в сфере кибербезопасности.

Мы проектируем системы под конкретные нужды и специфику организаций, тем самым гарантируя, что система информационной безопасности комплексно решает все задачи и обеспечивает надежную круглосуточную защиту ваших корпоративных ресурсов и данных.

Контакты:

г. Москва, ул. Автозаводская 13/1

8 (495) 748-09-44

evraas@evraas.ru