ПРОБЛЕМЫ КИБЕРАТАК НА АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМ ПРОЦЕССОМ В НЕФТЕГАЗОВОЙ ОТРАСЛИ

Евгений ПИТОЛИН,
управляющий директор

KasperskyLab в Казахстане, Центральной Азии и Монголии
050010, Республика Казахстан, г. Алматы, Казыбекби, 20а

Современные предприятия нефтегазовой отрасли давно перешагнули черту, отделяющую физический мир машин и агрегатов от виртуального, превратившись, по сути, в киберфизические системы. Эти системы строят с использованием IT-технологий и объединяют при помощи каналов связи. Это многократно упрощает их эффективное использование, но делает их уязвимыми перед угрозой компьютерных атак.

Какие факторы оказывают значительное влияние на ландшафт угроз, на разработку, внедрение и использование организационно-технических мер защиты объектов нефтегаза?

Эволюция технологических процессов – необходимость производить новую, более сложную, продукцию изменяет требования к системам автоматизированного управления.

Изменение процессов управления производством – подъем функций мониторинга и управления на более высокие уровни иерархии (от технологической установки внизу в кабинет главного инженера наверху и далее).

Постоянно возрастающая техническая сложность систем управления технологическим процессом – как следствие – переход на новые технологии при разработке систем автоматизированного управления, которые

- разрабатываются третьей стороной;
- заимствуются из IT;
- используются большим количеством производителей.

Уменьшение времени жизни систем управления – это приводит к уменьшению длительности цикла разработки и поддержки продуктов для АСУ ТП, что накладывает дополнительные ограничения на возможные затраты для обнаружения и решения проблем кибербезопасности продуктов на стороне производителя.

Повышение степени автоматизации, избавление от ручного труда.

- Рост и развитие общего количества систем автоматизации и прочих информационных систем на производстве.
- Внедрение новых систем и технологий, позволяющих унифицировать мониторинг и управление ранее несвязанными объектами и системами.
- Увеличение количества поставщиков и подрядных организаций.

Увеличение уровня защищенности «традиционных» жертв киберпреступников.

- Рост количества и качества используемых средств зашиты от традиционных атак, увеличение осведомленности потенциальных жертв и зрелости процессов обеспечения безопасности.
- Рост уровня экспертизы органов делает традиционные кибератаки все более рискованным видом нелегальной деятельности.
- Киберпреступники все более настойчиво ищут новые, менее защищенные цели.

Отсутствие очевидной повседневной угрозы – функциональной (технологическому процессу, оборудованию) и физической (людям и окружающей среде) безопасности, бизнесу нефтегазовых организаций.

- Многие организации при планировании и ведении своей деятельности из всего многообразия последствий кибератак учитывают только те, что потенциально ведут к уже смоделированным авариям с оцененным риском.
- Матрица этих рисков складывалась, как правило, под прессингом со стороны законодательно-нормативной базы и в условиях сложившейся во многих отраслях промышленности традиции.

Определяющее воздействие на список рисков предприятия и конкретного подразделения внутри предприятия оказывает также разделение ответственности между вертикалями управления на одном предприятии и между предприятиями в отрасли. При этом, как правило, речь идет об оцененных рисках возникновения критических ситуаций при случайном стечении негативных обстоятельств – исходя из теоретических обоснований и опыта практической эксплуатации оборудования. Таким образом, свести полностью планирование и реализацию организационно-технических мер киберзащиты к традиционным практикам функциональной и физической безопасности принципиально невозможно.

К сожалению, эту реальность большинство промышленных организаций принять пока не могут или не хотят. Целевые атаки на системы автоматизированного управления в нефтегазовой отрасли, в том числе и в РК, уже далеко не экзотика; при этом атаки, нацеленные на кражу денег, равно как и атаки вымогателей, также

становятся все более частыми. Так, системы «Лаборатории Касперского» автоматически исследуют и обрабатывают более 300 000 новых экземпляров подозрительного и вредоносного ПО ежедневно.

Угроза таких атак часто остается недооцененной представителями промышленных организаций, которые с ними не сталкивались на личном опыте, однако статистика предотвращенных попыток заражений промышленных систем автоматизации, которую мы публикуем в наших отчетах по РК и миру в целом, явно свидетельствует о том, что системы технологической сети нефтегаза доступны для массовых атак и случайных заражений, и, следовательно, могут быть целями злоумышленников, рассчитывающих получить выкуп за разблокировку.

Информация о проблемах информационной безопасности, обнаруженных уязвимостях, атаках и инцидентах во многих случаях считается конфиденциальной на всех уровнях экосистемы промышленного производства, поэтому доступ к такой информации для рядовой организации часто затруднен.Как следствие, недостаток информации, скрытность целевых атак, направленных на системы автоматизации, излишняя вера в системы противоаварийной защиты и неприятие объективной реальности (например, отрицание факта доступа в интернет или наличия случайных заражений компонентов АСУ ТП) сказываются негативно на оценке уровня угрозы владельцами и операторами промышленных предприятий и их персоналом.

Появившиеся в большом количестве производители новых специализированных средств защиты систем промышленной автоматизации (зачастую не имеющие достаточного практического опыта в разработке и применении средств защиты от традиционных IT-угроз) создали продукты, защищающие, возможно, не столько от реальных повседневных атак, сколько от синтетических сценариев.

Таким образом, в индустрии сложилась опасная, на наш взгляд, ситуация, когда усилия и бюджеты производителей и потребителей средств кибербезопасности могут тратиться не на решение первоочередной задачи – защиту от реальных (и все более частых) атак, а на защиту от синтетических сценариев и атак воображаемого будущего, измышленного производителями средств защиты без исследования объективной картины ландшафта повседневных угроз.