ПРЕСС-РЕЛИЗ

Екатерина Куценко
Пресс-служба
«Делойт», СНГ
Тел.: +7 (495) 787 06 00
Email: ekutsenko@deloitte.ru

Согласно новому отчету международной сети «Делойт» нефтегазовым компаниям необходимо укреплять подход к обеспечению кибербезопасности

Новые риски, угрожающие корпоративным системам управления производственными процессами, требуют разработки надежных, гибких и готовых к кибератакам механизмов защиты.

- *На фоне растущего осознания последствий кибератак необходимость принятия мер для подготовки к ним становится все более очевидной.*
- *Надежная платформа при обеспечении кибербезопасности — это необходимое условие для повышения операционной эффективности*

Москва, 29 мая 2017 года. Сегодня международная сеть «Делойт» опубликовала новый отчет «Интегрированный подход к управлению киберрисками*: обеспечение безопасности операционной деятельности в нефтегазовом секторе*». Он посвящен необходимости повышения уровня безопасности систем управления производственными процессами (ICS) на фоне трудностей, которые создают новые технологии. Исследование содержит результаты анализа, проведенного в ходе оказания различным нефтегазовым компаниям содействия в обеспечении не только материальной, но и информационной безопасности их ICS-систем.

В отчете говорится о том, что, несмотря на масштабное распространение инновационных методов работы, таких как роботизированные системы, цифровые решения и Интернет вещей (IoT), в вопросах кибербезопасности нефтегазовый сектор по-прежнему отстает от других отраслей. Для обеспечения безопасности и гибкости операционных процессов и их готовности к возможным угрозам нефтегазовые компании должны объединить усилия в двух сферах — технической и информационно-технологической, а также применять специализированные технические решения, которые не всегда легко защитить от кибератак.

Пол Зонневельд, руководитель Международной группы по предоставлению консультационных услуг в области управления рисками предприятиям энергетики и добывающей промышленности «Делойта»в Канаде, комментирует: «Постоянное совершенствование методов, применяемых киберпреступниками, ведет к росту риска возникновения катастроф и увеличению масштаба их последствий, которые проявляются в виде повышения затрат, нарушения безопасности, нанесения ущерба репутации компаниям и финансовых потерь. До сих пор нефтегазовому сектору удавалось избегать крупных производственных катастроф. Но если они не расширят свои программы по управлению киберрисками, это везение может вскоре закончиться».

Понимание рисков

При создании ICS-систем не предполагалось их дальнейшее объединение в сети, однако сегодня происходит именно это. Дигитализация операционных процессов в нефтегазовом секторе привела к тому, что перед компаниями открываются новые возможности для повышения производительности и сокращения затрат.

В то же время слияние производственных и бизнес-процессов также делает организации уязвимыми

Deloitte.

для новых киберрисков. В отчете рассматриваются нижеследующие возможные сценарии изменения ландшафта киберрисков.

- **Использование незащищенного удаленного доступа для осуществления взаимодействия** позволяет киберпреступникам получить контроль над системой, управляющей производственными процессами, и вызвать ее перегрузку.

- **Некорректное тестирование информационных систем перед их развертыванием** приводит к полному отказу систем и, как следствие, к сбоям или остановке производственных процессов.

- **Неэффективные методы обеспечения безопасности, применяемые сторонними контрагентами**, позволяют вирусам проникнуть в производственную программную среду, что приводит к остановке ключевых систем диспетчерского управления и сбора данных (SCADA).

- **Приобретение технологических продуктов без проведения полноценного предварительного тестирования и исправления ошибок** делает предприятие уязвимым и позволяет враждебно настроенным лицам получить удаленный доступ к системам.

«Приведенные примеры показывают, что существует множество источников киберугроз, в том числе в лице сотрудников компании, стремящихся организовать диверсию на производстве; и конкурентов, желающих нанести ущерб бренду компании; а также третьих лиц, заинтересованных в остановке ее работы, — говорит г-н Зонненвельд. — И пусть не все риски можно минимизировать, важно понимать, какие виды контрольных процедур существуют в организации и над чем еще необходимо работать».

Компании должны найти способ использовать противоположные точки зрения на информационные системы и операционные процессы. Полезным инструментом для преодоления этого непонимания может стать анализ типа bowtie — популярная концепция, широко используемая в инженерно-технической области для оценки отказов оборудования. Для защиты ICS-систем также можно применять нижеследующие дополнительные меры.

- **Оценка зрелости существующих средств обеспечения контроля.** Данная мера предполагает проведение инвентаризации активов и оборудования, а также оценку их значимости для организации; определение наличия/отсутствия в работе ключевых активов и оборудования детально изученных уязвимостей, которыми можно воспользоваться; оценку зрелости средств обеспечения контроля с целью упреждающего управления указанными угрозами.

- **Разработка единой программы.** Централизованная программа обеспечения кибербезопасности в нефтегазовом секторе может быть разработана и внедрена путем проведения многолетней работы, направленной на комплексное преобразование ICS-систем. При этом на каждом этапе трансформации необходимо помнить о самой главной цели — совершенствование процессов управления операционными процессами для создания безопасной, готовой к работе и защищенной контрольной среды.

- **Внедрение ключевых контрольных процедур.** Несмотря на то что показатели готовности к рискам разнятся от компании к компании, существует несколько основополагающих средств обеспечения контроля за киберрисками, которые должна иметь в своем наличии практически любая нефтегазовая компания. К ним относятся проведение информационно-разъяснительной работы среди сотрудников, осуществление контроля за доступом, обеспечение безопасности коммуникационной сети, ограничение использования и проверка переносных носителей информации, а также разработка регламента реагирования в случае возникновения угроз.

Deloitte.

- **Обеспечение эффективных механизмов управления** Внедрение программ информационной безопасности при управлении операционными процессами сопряжено с дополнительными сложностями, связанными с управлением кадровыми ресурсами. Организации должны разработать программу проведения информационно-разъяснительных мероприятий, чтобы преодолеть непонимание между ИТ-специалистами и специалистами по ICS-системам, а также обеспечить возможности карьерного роста для тех сотрудников, которые желают специализироваться в области информационной безопасности ICS-систем.

###