Информационная безопасность на критически важных объектах: от проблем к возможностям

В текущих реалиях информационная безопасность – это непрерывный процесс, который идет от создания объекта до вывода его из эксплуатации. Для критически важных объектов (КВО) ИБ – это неотъемлемая часть полноценного функционирования, к которой необходим грамотный подход на всех этапах

Александр Поздняков
Профессор
РГУ нефти и газа (НИУ) им. И.М. Губкина, д.т.н.

Информационная безопасность является неотъемлемой частью полноценного функционирования нефтегазового комплекса

В начале 2018 г. прошли важные изменения в правовом регулировании в сфере ИБ на объектах нефтегаза – вступил в силу ФЗ-187 и уже к весне появились его подзаконные акты. Это очень большой шаг в вопросе обеспечения безопасности КВО, так как данные нормативно-правового акта являются более зрелыми, чем все, что было до этого. И, в отличие от предыдущих, новые документы ратуют за реальную безопасность и направлены на отражение реальных угроз, а не просто на соблюдение буквы закона.

Ключевые тренды

Одной из основных тенденций развития ИБ видится объединение подсистем и их нацеленность на защиту от так называемых направленных атак, или атак "нулевого дня", – специально спланированных для поражения конкретного предприятия и являющихся на сегодняшний день самыми опасными.

Объединение систем ИБ проявляется в том, что сейчас на рынке нет продуктов, которые выполняют, скажем, только функции межсетевого экранирования или только антивирусную защиту. Кроме того, в сфере антивирусов и систем обнаружения вторжений наметилась тенденция к уходу от сигнатурного анализа в сторону поведенческого анализа.

Приоритетные задачи

Как бы странно это ни звучало, но на первый план выходят обучение персонала и повышение общей грамотности в вопросе ИБ. Мы можем построить любую систему защиты, но все равно самым слабым звеном в этой цепи будет человеческий фактор. И единственное, что может помочь, – это повышение осведомленности.

Расширение интеграции

Если говорить с точки зрения пользы, то взаимное проникновение технологий положительно влияет на информационную безопасность. Такое объединение позволяет строить эффективные системы безопасности с использованием минимального количества продуктов и является наиболее эффективным способом борьбы с направленными атаками.

К примеру, благодаря этому взаимному проникновению появился такой продукт, как "песочница", которая представляет собой объединение антивирусной системы и систем виртуализации, обнаружения и предотвращения вторжений. В связи с этим стало возможно проверять любой файл или любую активность на возможные негативные последствия для КВО.

Конвергенция логического и физического доступа

Сделано очень много положительных шагов в направлении объединения службы физической безопасности помещений и логической безопасности информационных систем. На нашем рынке появилось много продуктов, которые затрагивают обе эти стороны и тем самым являются связующим звеном. Это и электронные карточки, которые одновременно являются и пропуском, и частью системы идентификации на АРМ. Это и системы контроля мобильных устройств, навязывающих политики безопасности в зависимости от того, в каком помещении находится данное устройство.

А мешает этой взаимной интеграции устаревшее мнение, что ИБ существует отдельно от службы корпоративной защиты. Должно быть специализированное подразделение в службе корпоративной защиты – это логично с организационной точки зрения. В противном случае подразделения АСУТП изолируются от проблемы ИБ извне – их устраивает интегрированная система зарубежного вендора.

Отечественные vs импортные продукты

К сожалению, российских решений по ИБ в нефтегазовой отрасли нет (имеется в виду функционал объекта, АСУТП). Есть неплохие встроенные системы ИБ разных зарубежных производителей, но центры их компетенции и удаленный доступ находятся за рубежом, причем не всегда в дружественных странах.

В целом российский рынок ИБ очень сильно отстает от западного. В первую очередь из-за того, что у нас нет своей собственной производственной базы. Даже отечественные программно-аппаратные комплексы базируются на железе иностранного производства. Кроме того, очень сильно отстает функциональность систем защиты, взять те же самые межсетевые экраны. Крупнейшие нефтяные компании используют МЭ только иностранных производителей, так как они дают не только эффективную защиту, но и являются гибкими в настройке, что также положительно сказывается на информационной безопасности в целом.

Конечно, есть продукты, которые никак не заменить иностранными, – это оборудование криптографической защиты. Но, к сожалению, их незаменимость продиктована не их бесспорной эффективностью, а скорее требованиями регуляторов, не допускающими использование иностранных алгоритмов шифрования.

Будущее информационной безопасности объектов нефтегаза

В будущем на критически важных объектах я вижу наличие систем без включения в Интрасет зарубежного вендора SCADA-систем (сканер-системы). А если наступит долгожданный момент использования российских SCADA-систем, то туда можно будет интегрировать много российских наработок. ■

Ваше мнение и вопросы по статье направляйте на ss@groteck.ru