Федор ТРИФОНОВ:
«Повысить безопасность без расширения штата»

По мере цифровизации промышленности обязанности службы информационной безопасности (ИБ) существенно расширяются, поскольку увеличивается площадь атаки. Однако специалистов по защите промышленных объектов сейчас не очень много, поэтому компании вынуждены обходиться минимальными силами. Для этого необходимо повышать уровень автоматизации средств, находящихся в распоряжении службы ИБ. О возможностях интенсивного развития защиты мы поговорили с руководителем отдела технического сопровождения продаж компании InfoWatch ARMA Федором Владимировичем Трифоновым.

– С помощью каких технологий, по вашему мнению, можно обеспечить защиту сложных объектов минимумом персонала служб ИБ?

– Если говорить про безопасность АСУ ТП, то сейчас на рынке следующая ситуация: большая часть компаний не планирует расширять штат сотрудников для защиты промышленных объектов по требованиям Закона № 187-ФЗ или собирается увеличить его незначительно. Как следствие, на специалистов помимо задач, которые у них уже были – выдача прав, обновление антивирусного ПО, контроль подрядчиков, ложится еще ряд новых задач. Сначала это категорирование, потом составление организационно-распорядительной документации или контроль ее качества от исполнителя, интеграция СЗИ, затем ее эксплуатация. Вариантов качественного решения перечисленных задач всего два – либо создание выделенного подразделения, либо автоматизация этих процессов. Наша компания берет на себя задачу предоставить продукт, который будет автоматизировать деятельность специалиста по ИБ на протяжении всего жизненного цикла системы защиты информации. Мы создали систему продуктов, позволяющую категорировать объекты КИИ, создавать документы, обновлять их, настраивать продукты, контролировать политики, автоматизировать реакцию на инциденты и при этом сокращать их количество.

– С помощью каких инструментов можно обеспечить видимость сети? Насколько российским компаниям близка концепция Zero Trust?

– По моему мнению, сегодня в модель Джона Киндервага верит большинство российских компаний. Для специалиста в области информационной безопасности всегда важно сохранять данные в целости и сохранности, и если для этого необходимо внедрять дополнительный функционал, то почему бы и нет? Что касается инструментов, то у разных компаний разный подход. Мы за счет своих межсетевых экранов прослушиваем трафик и видим коммуникацию внутри сети, благодаря нашим агентам понимаем, подключались ли какие-то внешние устройства к рабочим станциям, не даем возможности использовать программы, которые не нужны на рабочих станциях, тем самым создавая полноценную замкнутую среду. На мой взгляд, этого достаточно, для того чтобы обеспечить базовый уровень безопасности промышленного сегмента АСУ ТП.

– Какие наиболее интересные проекты в области защиты АСУ ТП специалисты InfoWatch реализовали в прошедшем году?

– Если говорить об интересных исследованиях, то это анализ доступных из сети Интернет устройств АСУ ТП, который был проведен при помощи поисковой системы Shodan. В рамках этого исследования мои коллеги установили огромное множество АСУ ТП, имеющих открытый доступ в Интернет. Проект всколыхнул большое количество обсуждений в сети, но важно то, что перед публикацией статьи вся информация была передана в НКЦКИ, который провел работы по оповещению владельцев АСУ ТП в целях устранения найденных проблем. Данный проект помог многим организациям узнать, где у них есть болевые точки и как их нужно закрыть. Результаты нашей работы были опубликованы, кроме того, был проведен вебинар. ■