КИБЕРАТАКИ НА ПРОМЫШЛЕННЫЕ ОБЪЕКТЫ В 2019 ГОДУ

Е. ПИТОЛИН,
управляющий директор Kaspersky в Казахстане,
Центральной Азии и Монголии

Республика Казахстан, 050010, г. Алматы, Казыбек би, 20а

За последние несколько лет мишенью кибер-преступников становились больницы, аэропорты, поезда, компьютеры банков и государственных учреждений. Затем настала эра эпидемий WannaCry, ExPetr и BadRabbit – они распространялись как лесной пожар, грозя множеству компаний по всему миру убытками и помехами в работе. Казахстан, напоминаю, в 2017 году занял пятое место в мире по количеству зараженных WannaCry компьютеров, включая заражения объектов КВОИКИ и нефтегазового сектора.

В последние двенадцать месяцев атак такого масштаба не наблюдалось, и мир расслабился. Однако 19 марта 2019 года начался новый отчет в эпохе промышленных киберугроз. Норвежский промышленный гигант Hydro, один из крупнейших производителей алюминия в мире, объявил, что попал под удар программы-вымогателя, и эта кибератака колоссально повлияла на всю компанию. В компании работает около 35 000 человек, и заражение затронуло немалую их часть.

Принадлежащие Hydro электростанции не пострадали, потому что были изолированы от основной сети, – и это правильный подход к критической инфраструктуре. Однако плавильные заводы изолированы не были, а степень их автоматизации за последние годы значительно выросла. В результате шифровальщик поразил ряд заводов, расположенных в Норвегии. Неспособность подключиться к основным системам вызвала проблемы на производстве и временные остановки на нескольких заводах. Вредоносные программы зашифровали данные на компьютерах с Windows, выведя их из строя.

Читайте далее в журнале «Нефть и газ», №4, 2019 г.