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.

Конечно, полностью восстановить работу в штатном режиме получится нескоро. Да и расследование инцидента займет очень много времени, как у самой компании, так и у норвежских правоохранительных органов. Хотя анализ происшествия все еще ведется, уже можно говорить о том, что Hydro сделала правильно, а что неправильно до инцидента и во время его.

Правильно:

- станции энергоснабжения были изолированы от основной сети;
- компания оперативно смогла отсоединить от сети плавильные заводы;
- сотрудники могли нормально взаимодействовать даже после инцидента;
- есть резервные архивы, с помощью которых можно восстановить хотя бы частично зашифрованные данные;
- есть киберстраховка, которая должна покрыть хотя бы часть ущерба от инцидента.

Неправильно:

- сеть не была должным образом сегментирована со стороны департамента АСУ;
- установленное Hydro защитное решение не сумело перехватить шифровальщик, так как не взаимодействовало с промышленной сетью и было не предназначено для защиты таких сетей;
- периметр безопасности можно было дополнить специализированным продуктом по защите от вымогателей.

Подтвержденные компанией оценки ущерба от атаки на NorskHydro – 40 млн долл в первом квартале, до 25 млн ожидается по итогам второго квартала.

Также, за этот период произошло еще несколько крупных атак на мировую промышленность. Так, седьмого июня один из крупнейших в мире производителей авиационных деталей, компания ASCO Industries (занимается производством некоторых компонентов корпусов для гражданских и военных самолётов), подверглась атаке вымогательского ПО, которая привела к временному закрытию четырех заводов.

Подробностей об атаке известно немного: представители ASCO очень неохотно делятся информацией. По данным бельгийской телевещательной компании VRT, для расследования инцидента привлекли полицию и сторонних экспертов по информационной безопасности.

Компания приостановила производство на своих заводах в Бельгии, Германии, Канаде и США. Затронула ли атака их все, остается неизвестным, как неизвестны и масштабы ущерба. По данным СМИ, заражение произошло на бельгийском заводе в Завентеме. Однако компания приостановила производство также в Германии, Канаде и США. Связано ли это решение с распространением вредоносного ПО на другие заводы, или же является мерой предосторожности, пока неясно.

В апреле стало известно, что швейцарская компания AebiSchmidt, производитель тяжелой строительной и дорожной спецтехники, в частности – снегоуборочных машин для аэропортов и автомагистралей, стала очередной жертвой атак с использованием зловредов-шифровальщиков. Производственные процессы оказались парализованы из-за масштабного компьютерного сбоя, вызванного заражением вредоносным ПО. Инцидент затронул также систему внутренней электронной почты компании. В результате рабочие были отправлены по домам, а части из них

пришлось даже уйти в неоплачиваемые отпуска. Представитель AebiSchmidt Томас Шисс подтвердил факт инцидента и уточнил, что производственные процессы в процессе восстановления, а системы компании, использующие ОС Windows, «затронуты вирусом». Шисс также добавил, что часть незатронутых атакой систем была отключена, чтобы избежать распространения инфекции.

Из описания этих трех атак мы видим, что риски для промышленности, энергетики, финансовой среды крайне типичны – блокировка производственных процессов, дорогостоящие простои производства, вынужденные отпуска сотрудников, миллиардные убытки. К счастью для нефтегазового сектора, атаки первого полугодия были направлены пока на другие сегменты промышленности. Однако идентичность построения технологических сетей, схожие принципы и подходы к киберзащите, и увы, общая для всех отраслей кадровая проблема в ИБ говорит о том, что передышка у нефтянки небольшая, и чисто техническая. Как свидетельствуют статистические данные аналитического центра Kaspersky ICS CERT, с киберугрозами сталкивается значительное число промышленных компаний, и в 2018 году атакам вредоносного ПО подвергся практически каждый второй (47%) компьютер в технологической среде предприятий. В таких условиях инфраструктура нефтегазового сектора нуждается в особой защите. При этом крайне важно использовать специализированные решения для индустриальных сред, поскольку традиционные защитные продукты не всегда совместимы с оборудованием индустриальных предприятий и, следовательно, не столь эффективны.

Существует распространенное убеждение, что кибербезопасность – это черная дыра, которая требует огромных денег, но ничего не дает взамен. Однако недавнее исследование одного из ведущих в мире аналитических агентств Форрестер показало, что на самом деле кибербезопасность можно рассматривать как область инвестиций с солидными преимуществами как с точки зрения эффективности, так и финансов.

В следующий раз, когда ИБ-специалисты принесут вам план защиты промышленной сети от кибератак, а АСУ ТП отдел начнет рассказывать, как у них все хорошо и безопасно, и независимо от мировых угроз – просто вспомните этот текст.