KASPERSKY lab

Kaspersky Security Bulletin:

ПРОГНОЗЫ ПО РАЗВИТИЮ УГРОЗ В СФЕРЕ ПРОМЫШЛЕННОЙ БЕЗОПАСНОСТИ НА 2019 ГОД

Последние несколько лет были богаты на инциденты, связанные с информационной безопасностью промышленных систем. Экспертам удалось обнаружить новые уязвимости и векторы угроз, а также выявить немало случайных заражений промышленных систем и продуманных целевых атак. В прошлом году мы проанализировали результаты поисков и исследований и сформулировали прогноз для промышленной безопасности на 2018 год, где описали ряд тенденций, развития которых, по нашему мнению, можно было ждать в ближайшем будущем.

Ландшафт кибербезопасности промышленных систем более устойчив к переменам, чем ландшафт IT-безопасности в целом, а потому развивается значительно медленнее. Атаки на системы управления технологическими процессами сложнее монетизировать. Промышленные организации все еще не входят в область интересов большинства киберпреступников: даже для тех, кто уже начал атаковать АСУ ТП, эти системы — относительно новая мишень. Злоумышленники все еще адаптируют инструменты и тактики, которые использовали ранее, к новым атакам. Поэтому большинство тенденций, ожидаемых в текущем году, сохранятся и в следующем, хотя некоторые прогнозы сбылись уже сейчас.

Специалисты «Лаборатории Касперского» в течение нескольких лет исследовали ландшафт киберугроз для промышленных организаций, стараясь применять накопленный опыт и использовать свои разработки в OT-средах. Этот процесс пока далек от завершения: нам еще предстоит разобраться со многими сложностями и решить немало проблем. Мы постоянно консультируемся с исследователями из других организаций, занимающихся безопасностью, а также с первопроходцами в области защиты АСУ ТП из промышленных компаний. В ходе обсуждений выяснилось, что с некоторыми трудностями сталкиваемся не только мы, но и вся индустрия. Разрешив их, мы сделаем весь мир безопаснее.

Итак, хотя судьба некоторых предсказаний на 2018 год пока туманна, мы решили рассказать вам о проблемах, которые будут в приоритете у профессионалов по защите промышленных систем в 2019 году.

ЧЕТЫРЕ ГЛАВНЫЕ ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ, С КОТОРЫМИ СТОЛКНУТСЯ ПРОМЫШЛЕННЫЕ КОМПАНИИ В 2019 ГОДУ

1. Растущая поверхность атаки

Число автоматизированных систем растет, средства автоматизации становятся все разнообразнее, все больше организаций и отдельных сотрудников имеют прямой или удаленный доступ к АСУ ТП, появляются коммуникационные каналы для мониторинга и удаленного контроля ранее независимых объектов — все это дает киберпреступникам больше возможностей для планирования и осуществления атаки.

2. Растущий интерес киберпреступников и спецслужб

Сокращение прибыльности и увеличение риска атак, направленных на традиционных жертв, заставляет киберпреступников искать новые цели, в том числе среди промышленных организаций.

Параллельно спецслужбы многих стран, а также другие организованные группы, движимые коммерческими, внутренними или внешними политическими интересами, активно участвуют в разработках техник шпионажа и кибертеррористических атак на промышленные объекты.

Принимая во внимание сложившийся геополитический контекст, тенденции в разработке АСУ ТП, а также повсеместный переход на новые процессы управления, модели производства и экономической деятельности в ближайшие годы кибердавление на промышленные компании будет только нарастать.

3. Недооценка общего уровня угроз

Сегодня у широкой публики отсутствует доступ к сведениям о проблемах информационной безопасности в промышленных компаниях. К тому же целевые атаки на АСУ ТП относительно редки, а в организациях превалирует вера в системы аварийной защиты и отрицание объективной реальности существующих угроз. Все это негативно влияет на то, как владельцы и управляющие промышленных компаний, а также их персонал, оценивают степень опасности.

4. Неправильное понимание специфик угроз и далекий от оптимального выбор вариантов защиты

Несколько масштабных инцидентов, ставших результатами целевых атак против крайне ограниченного числа жертв, породили определенные представления о потенциальной угрозе в мире промышленной информационной безопасности — как среди ИБ-исследователей и разработчиков защитных средств, так и среди потенциальных пользователей защитных решений.

Однако большинство профессиональных отчетов об этих инцидентах оказались слишком сложными для понимания потенциальными пользователями и не содержали важных подробностей об OT-системах. В промышленных средах не нужно ежедневно отражать атаки, направленные на АСУ ТП, и сформировавшееся в этих условиях информационное поле привело к тому, что разработчики начали создавать продукты, которые скорее всего будут лучше защищать от искусственных сценариев, придуманных самими экспертами, чем от реальных повседневных угроз. Сложившаяся ситуация может повысить уязвимость систем промышленных предприятий к реальным атакам, будь то случайные заражения или целенаправленные кампании, организованные киберпреступниками.