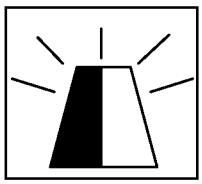

ПРОБЛЕМНАЯ СТАТЬЯ

БИТ

E. Kaspersky
general director «Laboratory of Kaspersky»

Automation Hostage: How to Protect the Industry Againts Cyber Attacks

Keywords: automated systems, security, technological process, vulnerability.
Humanity depends too much on automated systems whose vulnerability could to bring the world to the disaster at any moment.
All who are responsible for the operation of industrial facilities, as a rule are very serious about their security. Various means are used: barbed wire, security service, the pass office, video cameras, fire-protection systems, a Geiger counter, etc. This allows to increase the level of security of critical devices and hosts againts intruders and just idly walking citizens. Under normal circumstances, a person from the street can not get into a Nuclear power plant's control center or car factory's conveyor, because he can disrupt the technological process, arrange the economic and/or environmental catastrophe.

Е. Касперский
генеральный директор «Лаборатории Касперского»

В ЗАЛОЖНИКАХ У АВТОМАТИКИ: КАК ЗАЩИТИТЬ ПРОМЫШЛЕННОСТЬ ОТ КИБЕРАТАК[1]

Человечество слишком сильно зависит от автоматизированных систем, уязвимость которых может в любую минуту поставить мир на грань катастрофы.

Все ответственные за эксплуатацию промышленных объектов, как правило, очень серьезно относятся к их безопасности. В ход идут различные средства: колючая проволока, служба охраны, бюро пропусков, видеокамеры, противопожарные системы, счетчик Гейгера и т. д. Это позволяет повысить уровень защищенности критически важных устройств и узлов от злоумышленников и просто праздношатающихся граждан. В нормальной ситуации человек с улицы не может попасть в центр управления блоком АЭС или на конвейер автомобильного завода, потому что он может нарушить технологический процесс, устроить экономическую и/или экологическую катастрофу.

[1] Подробнее см. в первоисточнике на РБК:
http://www.rbc.ru/opinions/business/12/09/2016/57d2947d9a7947bd5adb221c?from=newsfeed

Тотальная автоматизация

Приблизительно с 1970-х годов в системах управления промышленностью, транспортом и инфраструктурными объектами огромное внимание начали уделять автоматизации технологических процессов. Она позволила существенно повысить как производительность труда, так и эффективность бизнеса в целом. Происходило создание и развитие информационных сетей, связанных с управлением производством, погрузкой-разгрузкой, доставкой и вообще любыми процессами, которые можно автоматизировать. Однако развитие автоматизированных систем управления технологическими процессами (АСУТП) традиционно происходило «за забором»: это были физически и информационно изолированные системы.

При этом промышленная и офисная информатизации шли каждая своей дорогой, каждая решала свои задачи. В промышленности первоочередной целью было, условно говоря, добиться максимально эффективного безаварийного управления турбиной, всем процессом производства и передачи электроэнергии.

В офисной сфере решались задачи по автоматизации бухгалтерии, ускорению и упрощению документооборота, повышению эффективности бизнеса. Офисные информационные технологии стали бурно развиваться на фоне взрывного роста использования интернета частными лицами и появления огромного количества публичных сетевых сервисов.

Именно в этом сегменте IT-мир столкнулся с эпидемиями вредоносного ПО, целевыми шпионскими атаками, немыслимыми грабежами банков. Здесь действуют сотни международных банд, распространяющих троянцев-шифровальщиков. И именно в этой реальности выросла традиционная отрасль информационной безопасности, включая мою компанию.

В мире АСУТП тоже происходили изменения. Выяснилось, что производительность труда и доходность бизнеса растут тем скорее, чем эффективнее информационные бизнес-процессы взаимодействуют друг с другом. Менеджмент получает возможность в реальном времени отслеживать и управлять тем, сколько и какой продукции производится. Упрощаются и ускоряются многие процессы – управление запасами, планирование, реакция на любые рыночные изменения. Повышается надежность оборудования и удобство его обслуживания.

Производители, например, турбин могут в реальном времени получать телеметрические данные с изготовленных ими устройств и моментально фиксировать любое их нештатное поведение. Все это ведет к тому, что оборудование работает лучше и становится безопаснее.

Однако вся эта информационная взаимосвязанность, в том числе критически важного оборудования, означает, что забор и системы видеонаблюдения, охраняющие процесс от внешнего вмешательства, становятся все менее эффективными. Компьютерные сети, оставаясь физически изолированными, перестали быть изолированными информационно. Колючая проволока не спасает от проникновения в информационную сеть, управляющую технологическим процессом, особенно если та соединена с внешним миром.

Глобальная уязвимость

До определенного момента информационные угрозы для АСУТП были исключительно теоретической проблемой. Физическая изоляция представлялась достаточной защитой от любого вторжения. Разработчики стремились к повышению устойчивости в аварийных ситуациях. Защищенность программного обеспечения и индустриальных

протоколов не была приоритетом. При этом почти всегда такие объекты являлись и являются очень чувствительными и значимыми как для экономики, так и для экологии. Любые аварии и нештатные ситуации могут угрожать человеческим жизням, не говоря уж об экономическом ущербе.

Компании же, работающие в сфере информационной безопасности (ИБ), традиционно разрабатывали свои решения, не особо учитывая специфику производства. Три главные цели классической ИБ-модели – конфиденциальность, целостность и доступность данных. Традиционно для офисных сетей и для персональных пользователей главной целью считалась именно конфиденциальность, то есть гарантия, что информация не попадет в руки посторонних.

Для промышленных объектов целостность и доступность данных, то есть непрерывность технологического процесса, гораздо важнее конфиденциальности. Даже для компаний, которым конфиденциальность важна (например, если у них есть какие-то секретные рецептуры), целостность и доступность потоков данных, как правило, важнее, потому что, если они нарушены, что-то может просто взорваться.

Управление технологическими процессами – задача очень сложная. Именно поэтому привычный подход в промышленности: «работает – не трогай». И обычно специалисты по промышленной автоматизации подозрительно относятся к любым мерам по IT-защите их систем. Надо признать, у них есть для этого основания: любое обновление ПО – потенциальная угроза технологическому процессу. И поэтому есть еще много мест, где продолжают работать системы на базе Windows NT и даже MS-DOS, которые давно не поддерживаются, не обновляются и обладают массой известных уязвимостей.

Но давайте посмотрим на проблему с другой стороны. Сегодня огромное количество промышленных систем подключено к интернету. В нашем исследовании мы насчитали в глобальной сети более 200 тыс. таких подключенных систем, из них более 30 тыс. – это программируемые логические контроллеры (ПЛК), то есть устройства, непосредственно управляющие технологическими процессами. Мы не знаем, где конкретно они стоят и что именно они делают, но это компьютерные устройства, они подключены к сети, и многие из них уязвимы для кибератак. Существует исследовательский проект, в рамках которого был создан червь, живущий в таких ПЛК, – ему вообще не нужны персональные компьютеры для распространения.

При этом даже изоляция от интернета хоть и помогает делу безопасности, но не является панацеей. Червь Stuxnet, который считается первым примененным кибероружием, и который был, предположительно, создан для физического саботажа работы центрифуг по обогащению урана, достиг своей цели через зараженные USB-флешки и подрядчиков.

Долгий путь к безопасности

Надо принять: человечество слишком сильно зависит от автоматизированных систем, которые пронизывают практически все сферы нашей деятельности. И уязвимость этих систем для кибератак может в любую минуту поставить мир на грань катастрофы, поэтому конвергенция промышленной и информационной безопасности неизбежна.

Американский ICS-CERT (United States Computer Emergency Readiness Team, Компьютерная группа реагирования на чрезвычайные ситуации. – РБК), орган, целью которого является защита критической инфраструктуры США, фиксирует все больше киберинцидентов в промышленной среде. В 2015 году их было 295 только по статистике, собранной этой организацией. По другим регионам цифр пока нет, потому что до

недавних пор компании не были обязаны сообщать о такого рода авариях. Подозреваю, что бóльшая часть подобных инцидентов остается неизвестной для широкой публики, регуляторов и ИБ-специалистов, поскольку компаниям проще не выносить сор из избы и не становиться героями плохих новостей.

При этом хакерские атаки уже становятся причинами серьезных и болезненных сбоев. Недавний пример – отключение электроэнергии на западе Украины в декабре 2015 года, когда сотни тысяч людей остались без электричества. Есть данные об атаке с помощью вирусов-вымогателей на американскую энергосбытовую и водоснабжающую компанию, расположенную в штате Мичиган. Правда, в этом случае успели отключить зараженные участки в корпоративной офисной сети и вредоносное ПО не достигло сети промышленной. В подпольном интернете появляются предложения о продаже удаленного доступа к системам управления технологическими процессами. Все чаще жертвами вредоносных программ становятся учреждения здравоохранения.

И хотя большинство крупных промышленных компаний находится еще только на этапе осознания проблемы, по моим ощущениям, видна положительная динамика. Мы действительно движемся к более безопасному и устойчивому миру.

О проблеме промышленной кибербезопасности все больше говорят, во многих странах появляются новое законодательство и требования к защите таких систем. Выходят требования к сертификации решений в области промышленной кибербезопасности, уже есть специализированные продукты и решения. И есть случаи их успешного внедрения.

Самое большое препятствие на пути конвергенции промышленной и IT-безопасности – скорость принятия решений о внедрении систем безопасности. Это понятно: крупным организациям требуется время для оценки рисков и разработки проекта. Увы, на другой стороне решения принимаются иначе. Злоумышленники – а это чаще всего небольшие хакерские группы, иногда криминальные, иногда связанные со спецслужбами, – по определению быстрее и мобильнее, они не скованны ни моральными ограничениями, ни обязательствами выполнять требования закона.

Новый рынок защитных решений для промышленных систем – это большой вызов для компаний сектора информационной безопасности, потому что в промышленности требуются абсолютно другие подходы. Я боюсь, что потребуются десятилетия, чтобы сделать промышленные системы во всем мире устойчивыми к кибератакам. Но делать это надо. На сегодняшний день самое страшное, что может случиться в сфере IT-угроз, – это именно атака, выводящая из строя критическую инфраструктуру с разрушениями, экологическими катастрофами и человеческими жертвами. Наша задача – предотвратить такое развитие событий.