Под защитой

«Лаборатория Касперского» сосредоточится на кибербезопасности крупных промышленных объектов

Андрей Духвалов
Руководитель департамента перспективных технологий «Лаборатории Касперского»

Тема киберзащиты индустриальных объектов, в том числе топливно-энергетического комплекса, — относительно новое направление деятельности для «Лаборатории Касперского», крупнейшей частной компании в сфере информационной безопасности. За последние четыре года ее эксперты создали ряд технологий и сервисов, предназначенных для того, чтобы сделать эксплуатацию крупных ответственных промышленных объектов более безопасной. Среди предприятий — крупнейший в Татарстане нефтехимический комплекс «ТАНЕКО».

Ключевые слова: Лаборатория Касперского, кибербезопасность, ТАНЕКО.

Спикеры пресс-конференции «Кибербезопасность АСУ ТП: время действовать»

Тема безопасности АСУ ТП (автоматизированных систем управления технологическим процессом) актуальна уже много лет, и для этого есть причины. С одной стороны, сегодня промышленные системы становятся все более связанными внутри корпорации и с внешним миром, а значит, повышается их уязвимость. С другой стороны, именно инфраструктурные и промышленные предприятия все чаще оказываются в фокусе внимания киберпреступников. В последние годы в число наиболее уязвимых попадают большие промышленные объекты, в том числе в сфере ТЭК.

Вот лишь два примера. В 2012 году одна из крупнейших нефтедобывающих компаний мира — Saudi Aramco, являющаяся национальным предприятием Саудовской Аравии, подверглась кибератаке. Заражение произошло через электронную почту, в результате атаки были уничтожены данные на 35 тыс. компьютеров предприятия. Отгрузка нефти была полностью приостановлена, и на 17-й день простоя корпорация начала поставлять нефть бесплатно всем, кто заявлял о своих правах, веря им на слово. Другой пример гораздо ближе к нам. В декабре 2015 года была зафиксирована кибератака на украинскую сеть распределения электроэнергии. В результате пострадало более 230 тыс. потребителей, и это не только частные лица, но и промышленные предприятия, которые столкнулись с отключением электроэнергии. В автоматизированной системе управления распределением ресурсов (АСУ РР) была предусмотрена возможность ручного управления, поэтому удалось через шесть часов восстановить подачу электроэнергии потребителям. На полное восстановление АСУ РР потребовалось три месяца.

Подобных реальных инцидентов на производствах становится все больше и больше. Именно поэтому одним из основных направлений деятельности «Лаборатории Касперского» является разработка решений по защите критической инфраструктуры. К понятию «критическая инфраструктура» относится все то, что может влиять на дееспособность бизнеса и даже на жизнеобеспечение граждан. Для нас это прежде всего промышленные компании, нефтеперерабатывающие заводы, компании, производящие и доставляющие электроэнергию, заводы по производству химических материалов, предприятия тяжелого машиностроения, другие крупные промышленные компании, остановка или перерыв бизнеса которых влияют на экономику или жизнь за пределами отдельной компании.

Помочь, а не навредить

Поскольку речь идет о защите индустриальных объектов, а это, как правило, объекты, которые связаны с повышенным риском, применять те технологии, которые индустрия безопасности накопила к настоящему моменту, нельзя. При разработке необходимых мер защиты нужно понимать специфику как технологического процесса, так и самого промышленного объекта. По этой причине «Лаборатория Касперского» разработала специализированные технологии, предназначенные именно для защиты критических инфраструктур.

В отличие от традиционных компьютерных систем здесь мы имеем дело с киберфизической системой. Киберфизические системы — это промышленные системы, объединяющие в себе производственное оборудование и информационные процессы. Кибер — компьютерное решение, наличие вычислительной инфраструктуры, включающей серверы и компьютеры, плюс программное обеспечение (ПО), управляющее логикой работы исполнительных механизмов. Если взять, например, трансформатор, то это «железо», но не только. Современными трансформаторами можно управлять с помощью специализированных компьютеров. Это уже получается киберфизическая система. Физической частью такой системы может быть конвейер заводов, турбина гидроэлектростанции и так далее. Чтобы анализировать правильность проходящих процессов, нужно понимать не только информационную часть, но и физическую. Это означает, что одни и те же информационные процессы могут быть в одной ситуации нормальными, а в другой ненормальными. Чтобы понять, какие процессы нормальные, нужно работать в сотрудничестве с инженерами той отрасли, для которой разрабатываются средства обеспечения кибербезопасности.

Для этого привлекаются специалистов той или иной области и совместно с ними изучает инфраструктуру системы. Далее определяются возможные векторы угроз и к каким последствиям может привести с физической точки зрения воздействие на ту или иную часть информационного процесса. После этого совместно со специалистами промышленного предприятия формализуются модели правильного поведения. Эти модели закладываются в информационную систему.

При разработке технологий защиты мы руководствуемся главным требованием: сохранить непрерывность работы производственного процесса, что крайне важно для предприятий, ведь любой простой может привести к огромным убыткам. Защитные программы не должны вмешиваться в производственный процесс и тем более останавливать его. Система работает в пассивном режиме, ее можно быстро развернуть без необходимости что-то менять в существующем оборудовании, и она тут же начнет анализировать происходящее в сети, выявляя критически важные события.

UNDER THE AEGIS

Kaspersky Laboratory will focus on the cyber security of large industrial facilities

The cyber protection of industrial facilities, including the fuel and energy sector, is a rather new avenue of activity for Kaspersky Laboratory, the largest private company in the domain of IT security. Over the past 4 years, its experts have created a series of technologies and services aimed at enhancing the operational security of large crucial industrial facilities. The petrochemical complex TANECO, the largest in Tatarstan, is included in such enterprises.

Keywords: Kaspersky Laboratory, cyber security, TANECO.

Andrey Dukhvalov

Технологии разработаны таким образом, что анализируется не сама информация, которая циркулирует внутри информационных систем, а ее копия. То есть для анализа берутся объекты, которые продолжают функционировать, — работа ведется с копией этой информации. Мы анализируем ее на предмет совпадения с правильными моделями поведения. В случае если находятся какие-либо отклонения, отправляется уведомление обслуживающему персоналу объекта анализа о том, что система вышла из стабильного состояния.

Наше решение анализирует весь трафик внутри промышленной сети, отслеживает все запускаемые программы и подключаемые устройства и наблюдает за их работой. Защита распространяется на все ключевые компоненты: АСУ ТП, рабочие места операторов, РЗА, контроллеры, элементы индустриальных сетей, рабочие станции. Фактически система постоянно мониторит технологический процесс и не только, выявляет подозрительные действия, связанные с информационными системами, но и отслеживает нелогичные, несвоевременные или потенциально опасные команды внутри технологического процесса.

Главное — человеческий фактор

Стоит отметить, что система защиты промышленных предприятий «Лаборатории Касперского» — не блокирующая технология. Информация о сбоях передается обслуживающему персоналу предприятия. И здесь есть проблема, с которой мы иногда сталкиваемся: персонал не знает, что с этой информацией делать. Тема кибербезопасности производственных объектов — абсолютно новая. В крупных компаниях порой недооцениваются потенциальные риски, при этом многие специалисты, отвечающие за производственные системы, продолжают убежденно верить, что их система изолирована и самое главное для них — надежность оборудования и функциональная надежность SCADA-систем, которые они эксплуатируют. Они не подозревают, насколько легко перехватить управление такой системой удаленно,

«ТАНЕКО» под защитой

«ТАНЕКО», крупнейший нефтехимический комплекс Татарстана, является одним из первых партнеров «Лаборатории Касперского» в области обеспечения кибербезопасности предприятий. Сотрудничество началось в 2015 году. Увеличение степени автоматизации производств, а также активное проникновение технологий, разработанных для бизнес-структур, в индустриальную инфраструктуру значительно повышают риски, связанные с кибератаками на промышленные объекты. Именно поэтому «ТАНЕКО» поставила задачу провести обследование состояния информационной безопасности железнодорожной платформы по сливу вакуумного газойля.

Помимо этого, требовалось на пилотном проекте продемонстрировать возможность обеспечения кибербезопасности АРМ-операторов и SCADA-серверов, а также контроля целостности технологической сети и контроля ключевых параметров технологического процесса. В дополнение к этому предложенное решение не должно было оказывать никакого влияния на технологический процесс и требовать дополнительных настроек конфигурации АСУ ТП.

«Уже в первые месяцы работы решение по защите индустриальных объектов «Лаборатории Касперского» обнаружило несанкционированное подключение стороннего ноутбука к одному из контроллеров, а также попытку изменить параметры работы датчика», — рассказал начальник отдела АСУ ТП «ТАНЕКО» Марат Гильмутдинов.

«Результаты работы решения Kaspersky Industrial CyberSecurity превзошли все наши ожидания. Этот проект наглядно продемонстрировал возможность использования подобных решений на промышленных объектах. «ТАНЕКО» планирует и далее расширять свое сотрудничество с «Лабораторией Касперского» в области защиты индустриальных сетей», — сказал Гильмутдинов.

и сделать это может человек, месторасположение которого даже трудно определить. Или владельцы считают, что после установки межсетевого экрана сеть защищена. На самом деле межсетевой экран тоже уязвим, он не является панацеей. Поэтому была разработана программа образовательных тренингов с целью объяснить, как анализировать информацию, связанную с событиями кибербезопасности, и как действовать в подобных ситуациях. Мы предоставляем сервис, который поможет обслуживающему персоналу, владельцам информационно-индустриальных объектов понять, что произошло и как решить проблему в зависимости от ситуации.

Индивидуальный подход

С информационной точки зрения все промышленные объекты уникальны. Конечно, уникальность присутствует и в технологических процессах, которые часто имеют длительный срок эксплуатации. Как пример — сотрудничество с ФСК ЕЭС. Обсуждалась программа киберзащиты распределительных подстанций мощностью от 110 кВ и выше, которых в структуре предприятия около шестисот. В первую очередь необходимо было выяснить, какие типы подстанций существуют. Для того чтобы разработать средства защиты, нужно знать параметры каждого из них.

Когда подстанции ФСК были разнесены по определенным подтипам, при посещении объектов выяснилось, что даже объекты одного подтипа имеют некоторые отличия друг от друга. Ни одна подстанция не была точной копией другой, при этом на них применялось одинаковое оборудование и похожее программное обеспечение. Таким образом, чтобы разработать средства киберзащиты, необходимо понимать особенности каждого объекта.

Технологический процесс

В целом процесс применения защиты для разных объектов как определенная последовательность действий выглядит примерно одинаково. Сначала проводится обследование объектов с информационной точки зрения, в процессе которого собственники объектов часто узнают много нового о протекании информационных процессов на их предприятиях. На основании информации об обследовании «Лаборатория Касперского» разрабатывает модель угроз. Специалисты по информационной безопасности определяют слабые стороны той или иной системы. Затем начинается процесс взаимодействия для определения, какие из угроз с точки зрения владельца объекта могут привести к негативным последствиям, а какие можно игнорировать.

Далее необходимо определить, какие из этих угроз критические, а какие нет. Чтобы предотвратить любую из угроз, нужно оценить ее на предмет применения необходимых средств защиты. Эти средства могут быть как информационные, так и административные или даже физические. Например, ограничение физического доступа к серверу — это тоже мера защиты. «Лаборатория Касперского» концентрируется на мерах, которые лежат в информационной области, но тем не менее мы всегда проводим полноценный анализ и сообщаем заказчику о других возможных рисках и вариантах их предотвращения. Затем заказчик сам решает, с какими рисками и каким образом он будет работать.

Зачастую простые организационные меры повышают уровень устойчивости работы всей системы. Мы убеждены, что при решении той или иной задачи важен комплексный подход: это и использование технологий, и обучение персонала, и разработка рекомендаций по изменению внутренних регламентов, и сервисы, которые мы предоставляем сами или через партнеров.