Об открытии центра промышленной безопасности Kaspersky Lab ICS-CERT стало известно во время конференции «Кибербезопасность АСУ ТП 2016: время действовать вместе», которая в эти дни проходит в Иннополисе.

Напомним, ранее в Иннополисе компания открыла центр компетенции, который, по словам самого Евгения Касперского, занимается «консалтингом, помощью в проектировании решений по защите индустриальных систем». Планируется, что в центре компетенции в Иннополисе будет работать до десяти специалистов, но пока их меньше.

Однако центр промышленной безопасности — это нечто другое. Пока центр «физически никуда не привязан», то есть существует лишь в виде сайта, куда могут обратиться компании, у которых возникли проблемы с кибербезопасностью.

Планируется, что ICS-CERT будет координировать действия производителей систем автоматизации, владельцев и операторов промышленных объектов, а также исследователей в области информационной безопасности. Центр также будет собирать данные об уязвимостях, атаках и возможных угрозах, на основе которых будет давать рекомендации по защите индустриальных и критически важных инфраструктурных объектов. Все данные, кроме конфиденциальных, будут доступны публично в обезличенном виде. Информация об уязвимостях в индустриальном ПО и оборудовании будет публиковаться при взаимодействии с производителями согласно политике ответственного разглашения.

Ожидается, что основными клиентами центра станут производители компонентов автоматизированных систем управления технологическим процессом (АСУ ТП), национальные CERT и промышленные предприятия, работающие в энергетике, машиностроении, транспорте, металлургии, нефтегазовом секторе, производстве строительных материалов и т. д.

Несмотря на то, что центр промышленной безопасности пока существует лишь виртуально, у него уже есть несколько крупных клиентов. По словам Касперского, один из них — татарстанское нефтеперерабатывающее предприятие «ТАНЕКО». «Естественно, мы наработали некоторый опыт по защите подобных объектов, который хотим применять дальше», — сказал глава Kaspersky Lab.

Как стало известно «Хайтеку», в число компаний — заказчиков решений по информационной безопасности «Лаборатории Касперского» также входит латвийская компания Vars (терминал перевалки нефтехимических продуктов с железнодорожного транспорта на водный — прим. авт.). Также «Лаборатория Касперского» оказывает услуги по анализу текущей защищенности череповецкого металлургического комбината «Северсталь».

Опасения крупных компаний, заботящихся о цифровой безопасности, не напрасны. В последнее годы в мире киберпреступлений, связанных с атаками на критические индустриальные объекты, прослеживается определенная тенденция: взломав систему, все чаще злоумышленники не просто ее отключают, а предпочитают сохранить к ней доступ, создавая тем самым некую бомбу замедленного действия, которую могут «взорвать» впоследствии в любой удобный для себя момент. В качестве примера можно привести успешную атаку хакеров на украинские электроподстанции в декабре 2015 года, в результате которой без

света остались 230 тысяч жителей Ивано-Франковской области. Как выяснилось уже после инцидента, доступ к подстанциям взломщики получили еще за два года до их отключения.

Вот еще пара примеров: о вирусе NetTraveler стало известно в 2013 году, тогда как он был активен с далекого 2004 года, а компьютерный червь Stuxnet, по некоторым предположениям являющийся специализированной разработкой спецслужб Израиля и США, был обнаружен лишь в 2010 году, хотя работал с 2005 года.

Менеджер по развитию решений по безопасности критической инфраструктуры «Лаборатории Касперского» Антон Шипулин рассказал «Хайтеку» о результатах исследований, в рамках которых на заранее смоделированные электроподстанции, как в ловушку, заманивались взломщики — исследования проводились для изучения поведения хакеров.

«Большинство атакующих были организованы, захватывали управление над системами и сохраняли себе доступ, не спеша побыстрее отключить или разрушить систему, — рассказал Шипулин. — То есть, если сейчас какие-то инциденты не происходят, это не значит, что объекты безопасны и неуязвимы. Многие просто не знают, что они уже под контролем».

По словам Шипулина, лучшая защита — это обеспечение безопасности на уровне производителя промышленного оборудования, когда автоматизированную систему управления разрабатывают, изначально закладывая в нее механизмы безопасности с проверкой исходного кода, выявлением уязвимостей и т. д.

«С этого года замечена тенденция, что сами производители промышленного оборудования начинают закладывать криптографию внутрь, осуществлять проверку исходного кода, то есть ситуация меняется, — говорит Шипулин. — Но проблема в том, что огромная часть промышленного оборудования до сих пор работает на старых, уязвимых системах. И эту проблему нужно решать. Для этого „Лаборатория Касперского“ разрабатывает свое решение по мониторингу целостности технологического процесса».

В 2016 году «Лаборатория Касперского» зафиксировала 2,2 млн срабатываний антивирусного программного обеспечения на компьютерах, установленных на производстве. Из них 104 тысячи были вызваны вредоносным ПО.