Совершенствование методов обнаружения аномалий в области компьютерной безопасности с помощью проектов координированных исследований

Родни Буским э Силва и Андреа Рахандини

Выявление аномалий в работе компьютерных систем, контролирующих критически важные функции ядерной и физической безопасности, требует высокой квалификации, а необходимые меры, чтобы быть эффективными, должны быть протестированы, проанализированы и скорректированы.

«Обнаружение аномалий играет важную роль в оперативной оценке потенциальных опасностей, угрожающих компьютерным системам на ядерных и радиологических установках, — говорит Скотт Первис, начальник Секции управления информацией Отдела физической ядерной безопасности МАГАТЭ. — Обычно для обнаружения аномалий используется искусственный интеллект, в том числе машинное обучение, методы, основанные на статистике и знаниях, а также другие технологии». Такие технологии используются для выявления отклонений от ожидаемых параметров сетевых коммуникаций или показателей, которые могут быть первым признаком того, что злоумышленникам удалось преодолеть защиту компьютерной системы; они способны обеспечивать обнаружение кибератак в режиме реального времени.

Эти технологии важны потому, что злоумышленники могут внедрить вредоносное ПО, способное подорвать функции безопасности и защиты цифровой системы и сфальсифицировать данные, которые датчики и сенсоры передают оператору. Таким образом оператор не сможет узнать о злоумышленных действиях и первое время будет реагировать исходя из показателей приборов в диспетчерской, то есть предпринимать неверные действия. Оператор может быть правильно проинформирован только благодаря автоматизированному обнаружению мельчайших аномалий, проявляющихся в ходе такой кибератаки.

Для охвата этой важной области работы и решения других проблем компьютерной безопасности МАГАТЭ в 2016 году запустило специальный проект координированных исследований (ПКИ).

Исследования и разработки в рамках ПКИ — неотъемлемая часть деятельности МАГАТЭ в области компьютерной безопасности в целях обеспечения физической ядерной безопасности. В рамках таких проектов проводятся исследования и делаются практические выводы, которые дополняют текущие усилия МАГАТЭ по расширению возможностей стран по предотвращению и выявлению инцидентов в области компьютерной безопасности, реагированию на них и восстановлению после них, которые могут прямо или косвенно повлиять на ядерную и физическую безопасность ядерных и радиологических установок.

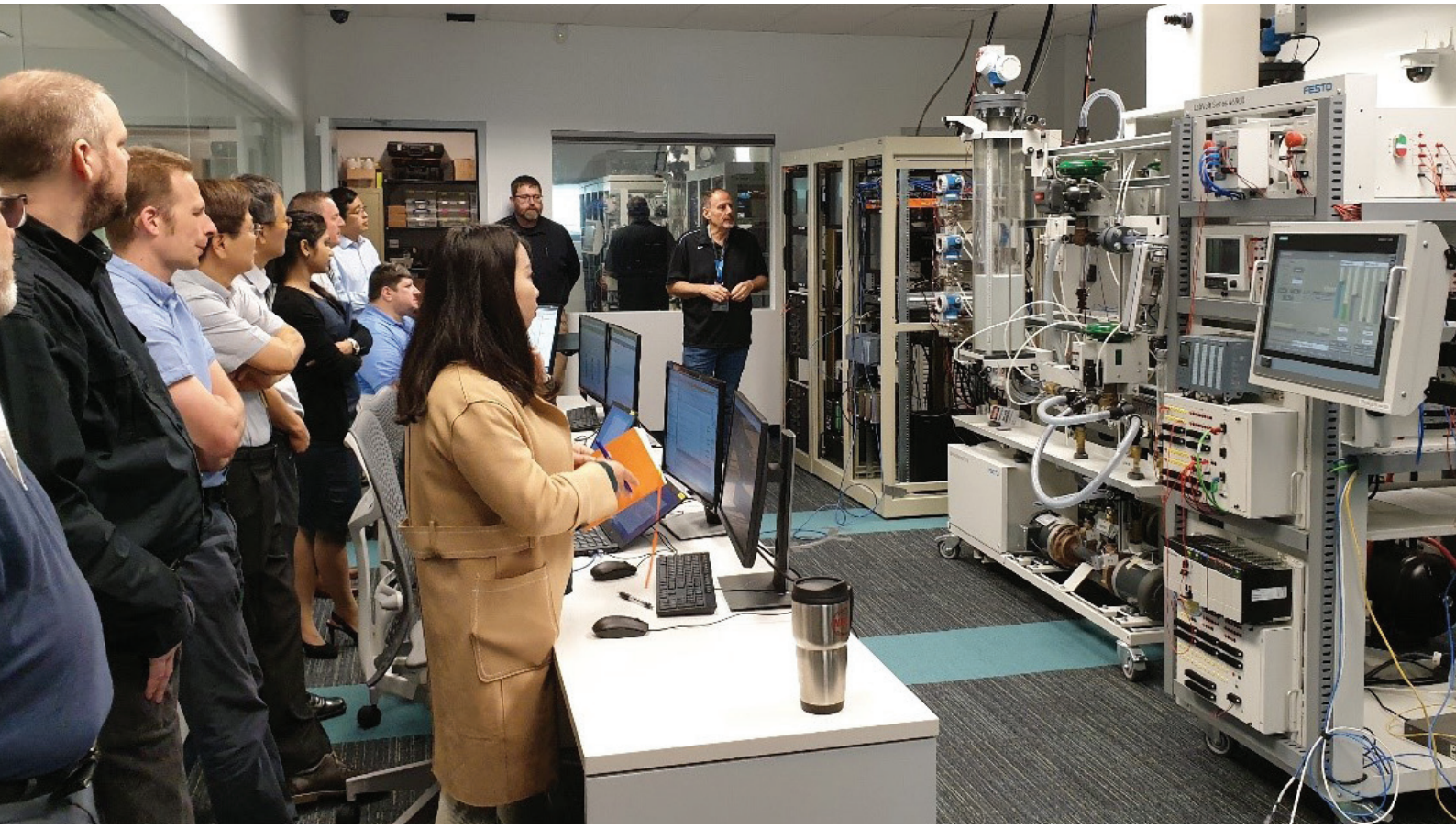
«Профессиональный уровень противника растет, и их кибервозможности создают все больше проблем при разработке средств обнаружения аномалий, — отмечает Первис. — Разработка методов выявления аномалий требует доступа к реалистичным и физически сопоставимым данным сети и технологических процессов на объекте для обучения и тестирования моделей обнаружения».

Сценарий кибератаки для наращивания потенциала

Начатый в 2016 году ПКИ на тему «Совершенствование анализа инцидентов в сфере компьютерной безопасности на ядерных установках» принес значительные результаты, в частности, способствовал дальнейшему исследованию целевых инструментов и методов, которые ранее было невозможно исследовать без риска раскрытия конфиденциальной информации, связанной с ядерными и радиологическими установками.

Участвующие в реализации ПКИ исследователи из 13 стран и 17 организаций разработали виртуальную модель объекта (АЭС «Ашера»), а специалисты из Университета Сан-Паулу создали на основе этой модели тренажер (ANS). Вместе они разработали реалистичные сценарии кибератаки на ядерный объект. Эти сценарии позволили изучить и оценить эффективность мер компьютерной безопасности, а также потенциальные последствия несанкционированного доступа к цифровым активам для эксплуатации установки. Кроме того, специалисты работали над сбором и анализом данных, разработкой и тестированием методов обнаружения кибератак.

«Мы создали и с помощью ANS наполнили хранилище данных для обучения моделей машинного обучения и оценки их эффективности. В рамках ПКИ МАГАТЭ объединило усилия международных партнеров для проведения исследований и способствовало получению



В Университете Сан-Паулу был разработан тренажер на базе виртуальной АЭС «Ашера». (Фото: МАГАТЭ)

новых знаний в этой области, — говорит Рикардо Маркес, профессор политехнической школы при Университете Сан-Паулу (Бразилия). — Сотрудничество между участниками ПКИ было принципиально важно для подтверждения результатов проделанной работы».

Кроме того, результаты ПКИ использовались для обучения и подготовки большого числа аспирантов и ученых в различных дисциплинах. Это способствовало дальнейшему развитию исследований и подкрепило усилия, направленные на постоянное укрепление компьютерной безопасности на ядерных и радиологических установках.

«Часть моих исследований в аспирантуре проводилась с использованием ANS и его человеко-машинного интерфейса (ЧМИ) — интерфейса, который позволяет пользователю взаимодействовать с тренажером, разработанным в рамках ПКИ МАГАТЭ», — рассказывает Си Вэнь, аспирант Университета Цинхуа (Китай). «Мои исследования касались методов обнаружения аномалий, и ANS был необходим для получения данных для обучения и оценки алгоритма обнаружения, разработанного для АЭС. Без сотрудничества между всеми участвующими учреждениями и инструментов, разработанных в рамках ПКИ, мое исследование по кибербезопасности цифровых систем АЭС было бы невозможно провести», — добавляет она.

Результаты ПКИ — ANS, инструменты и руководящие материалы — доступны для заинтересованных исследовательских институтов по всему миру. Их можно получить, подав в МАГАТЭ через соответствующий национальный орган форму запроса, которая размещена на портале МАГАТЭ по физической ядерной безопасности (NUSEC).

Совсем недавно, в 2023 году, МАГАТЭ приступило к реализации нового ПКИ по теме «Укрепление компьютерной безопасности применительно к системам обнаружения излучения» для исследования методик и способов повышения компьютерной безопасности оборудования для обнаружения излучения. В рамках нового ПКИ, в котором примут участие 12 организаций (включая национальные лаборатории, университеты и национальные исследовательские институты) из 11 стран, будут проводиться исследования, направленные на использование новых цифровых технологий, таких как облачные вычисления, а также дальнейшее изучение и разработка инновационных методов обнаружения аномалий.