12 октября 2021 года **ПРЕСС-РЕЛИЗ**

ТМК и Группа Синара провели первые кросс-отраслевые корпоративные киберучения в промышленности на Национальном киберполигоне

«Ростелеком-Солар» совместно с Корпоративным университетом ТМК2U организовали для сотрудников Трубной Металлургической Компании (ТМК) и Группы Синара масштабные кросс-отраслевые корпоративные учения на Национальном киберполигоне. Это первые в России киберучения, охватывающие отработку всех ключевых процессов служб информационной безопасности – от анализа защищенности и выстраивания системы комплексной безопасности инфраструктуры до выявления и отражения хакерских атак.

Киберучения прошли в рамках международного корпоративного форума ТМК и Группы Синара «Горизонты» и длились три дня, в течение которых семь команд, состоящих из ИТ- и ИБ-специалистов компаний, боролись за первенство в выявлении, отражении и расследовании кибератак. В последний день мероприятия был проведен разбор сценариев кибернападений и тактик реагирования команд защитников. Прямые включения в корпоративном мобильном приложении Mobi2U комментировали Руководитель направления кибербезопасности ТМК Антон Кокин и руководитель Лаборатории Кибербезопасности автоматизированных систем управления технологическим процессом (АСУ ТП) компании «Ростелеком-Солар» Андрей Кузнецов.

В первый день киберучений команды должны были провести максимально полную инвентаризацию инфраструктуры, специально созданной на базе промышленного сегмента киберполигона. Затем им необходимо было выполнить поиск уязвимостей в ней и настроить источники событий в SIEM-системе. На данном этапе оценивались полнота и точность данных от каждой команды.

Во второй день команды противостояли целенаправленным атакам, и на этом этапе ключевым показателем стала скорость обнаружения инцидента и реагирования на него. По итогам каждой атаки команды предоставляли отчеты с описанием как цепочки шагов злоумышленника, так и мер, необходимых для того, чтобы избежать повторения инцидента.

В заключительный день киберучений были подведены общие итоги, а также проведен подробный разбор сценариев учебных кибератак и действий команд. Наилучший результат по отражению кибератак продемонстрировала команда управляющей компании ТМК, второе место заняла сборная Первоуральского новотрубного и Челябинского трубопрокатного заводов (ПНТЗ и ЧТПЗ), третье место — у команды Северского трубного завода (СТЗ).

«Киберучения – это отличная возможность объективно оценить уровень своих компетенций и отработать практические навыки реагирования на инциденты информационной безопасности, а формат соревнования привнес в них элемент азарта. Важно, что в ходе мероприятия отрабатывались сценарии, близкие к жизни, релевантные именно для промышленных предприятий. Подобный формат используется впервые в металлургической отрасли. Результаты учений подтвердили

высокий профессионализм нашей команды кибербезопасности», – подчеркнул директор по информационным технологиям ТМК Дмитрий Якоб.

«Безопасность промышленных предприятий – тема, значимость которой остается недооцененной. Ее сложность связана с необходимостью очень специфических компетенций от защитников, будь то внутренний ИБ-департамент или сервис-провайдер, особенностями функционирования технологических сегментов и одновременно – максимально недопустимыми рисками от успешной хакерской атаки. Поэтому мы очень рады тому, что ТМК и Группа Синара так тщательно прорабатывают вопросы киберустойчивости предприятия, используя максимум инструментов для ее проверки и повышения», – отметил вице-президент «Ростелекома» по информационной безопасности Игорь Ляпунов.

Национальный киберполигон создан по поручению Минцифры России в рамках программы «Цифровая экономика». Целью его создания является отработка процессов выявления и реагирования на компьютерные атаки на уровне отраслей и ключевых организаций России. К настоящему моменту «Ростелеком» на базе ресурсов дочерней компании «Ростелеком-Солар» создал три первых сегмента киберполигона, которые представляют собой цифровые копии типовых ИТ-инфраструктур, существующих в организациях ключевых отраслей экономики.

ТМК (*www.tmk-group.ru*) — глобальный поставщик стальных труб, трубных решений и сопутствующих сервисов для нефтегазового сектора. Компания обладает производственными активами в России, Румынии, Казахстане и Чехии. Наибольшую долю в структуре продаж ТМК занимают нарезные нефтегазовые трубы, отгружаемые потребителям более чем в 80 странах мира. Компания также поставляет специальные трубы и трубопроводные системы для атомной энергетики, продукцию для химической промышленности, машиностроения, строительства и других отраслей. ТМК сочетает поставки продукции с широким комплексом сервисных услуг по термообработке, нанесению защитных покрытий, нарезке премиальных соединений, складированию и ремонту труб. Компания совершенствует свои научно-технические компетенции и ведет разработку инновационной трубной продукции на базе научно-технического центра (НТЦ) в Сколково и Русского научно-исследовательского института трубной промышленности (РусНИТИ) в Челябинске. Акции ТМК обращаются на Московской бирже.

ТМК в Facebook* * *ТМК в Twitter* * *ТМК в Youtube* * *ТМК в Flickr

Пресс-служба ПАО «ТМК»: тел. +7 (495) 775-76-00, e-mail: pr@tmk-group.com

«Ростелеком-Солар» — компания группы ПАО «Ростелеком». Национальный провайдер сервисов и технологий для защиты информационных активов, целевого мониторинга и управления информационной безопасностью.
В основе наших технологий лежит понимание, что настоящая информационная безопасность возможна только при непрерывном мониторинге и удобном управлении системами ИБ. Этот принцип реализован в наших продуктах и сервисах.

Контакты для СМИ: Наталья Лезина, +7 926 527 1992, n.lezina@rt-solar.ru