ГК Innostage представила платформу обучения кибербезопасности

Тематика: **IT и телекоммуникации**
Корпоративные новости

Дата публикации: 22.09.2022

Дата мероприятия / события: 22.09.2022

г. Москва

В рамках международного форума «Kazan Digital Week 2022» ГК Innostage представила новую платформу обучения кибербезопасности, развернула работу виртуального киберполигона и провела практическое обучение ИБ-специалистов по выявлению реальных компьютерных атак.

Платформа обучения кибербезопасности представляет из себя виртуальный киберполигон, на котором сымитирована типовая инфраструктура предприятия и развернуты средства защиты информации, такие как Positive Technologies NAD, Positive Technologies SIEM, Positive Technologies AF, Positive Technologies Sandbox. При этом такой цифровой двойник хранит следы хакерских атак, сценарии и тактики которых взяты из реальных инцидентов, количество которых, начиная с февраля 2022 года, выросло в кратном размере.

«Чтобы противостоять современным компьютерным атакам, сегодня уже недостаточно просто пройти курс, прочитать форум или найти ответ в книге. Эти источники не дают специалисту по ИБ реального опыта. Сегодня мы представили платформу обучения, уникальную для специалистов по информационной безопасности. Она позволяет проводить практическую подготовку по выявлению и противодействию современным компьютерным атакам. Здесь сымитировано больше 90 процентов всех компьютерных атак, которые произошли в последние полгода — это подмена информации на сайтах, внедрение программ вымогателей и шифровальщиков. Чтобы защититься от этих угроз, нужен реальный опыт. А к этому, к сожалению, никто не готовит, опыт можно получить только ''в бою'', и здесь мы готовы его дать», — отмечает **Алексей Воронцов, директор департамента сервисов киберзащиты ГК Innostage.**

Обучение проходит на примере реальных цепочек из самых распространённых атак — deface сайта, внедрение шифровальщиков, шпионского ПО, майнеров и фишинг. В основе заложены актуальные сценарии и тактики, которые сейчас применяются хакерами для атак на российские информационные системы.

На «Kazan Digital Week 2022» состоялся релиз платформы и учебного киберполигона. Специалисты по ИБ смогут прокачать свои компетенции по оперативному реагированию на атаки и эффективной настройке средств защиты информации. В конечном итоге они смогут оценить защищенность собственной инфраструктуры, посмотрев на нее глазами хакера.

«Спрос на практический опыт сейчас огромен. В вопросах обеспечения информационной безопасности сместился акцент. Если раньше компании следовали «бумажной» безопасности, пытаясь соответствовать правилам от регулятора, то сегодня бизнесу нужна практическая кибербезопасность, чтобы выстоять под натиском хакерских атак. Фактически, мы находимся в состоянии реальной кибервойны. Каждое предприятие в нашей стране – это легитимная цель для любого хакера. Государство принимает меры – вводит персональную ответственность за ИБ, оборотные штрафы за утечку персональных данных, ограничивает использование иностранного ПО. Все это вкупе с санкциями обостряет давнюю проблему – нехватку кадров. Мы готовы ее решать с помощью платформы обучения кибербезопасности», - резюмировал **Айдар Гузаиров, генеральный директор ГК Innostage.**

В дальнейшем Innostage планирует проводить подобное обучение на регулярной основе, в очном и дистанционном формате под контролем наставников - специалистов компании.

О группе компании? Innostage *(https://innostage-group.ru/)*
Группа компании? Innostage специализируется на решении задач в области кибербезопасности. В рейтинге CNews Security компания занимает 12 место, а также 4 позицию среди ИБ-интеграторов. Ключевые направления

деятельности: информационная безопасность, внедрение средств защиты информации, системная интеграция, безопасность АСУ ТП и комплексных инженерно-технических средств. Офисы расположены в Казани, Москве, Краснодаре, Иннополисе.

Среди клиентов компании: ПАО «НК «РОСНЕФТЬ», ПАО «Россети», Госкорпорация «Росатом», ПАО «Газпром», ПАО «Транснефть», ПАО «Интер РАО», ПАО «СИБУР Холдинг», АО «Газпромбанк», ПАО «АК БАРС» БАНК, Правительство г. Москвы, Правительство Республики Татарстан.

На базе ГК Innostage функционирует Центр предотвращения киберугроз CyberART, отвечающии? за мониторинг и быстрое реагирование на инциденты ИБ. Специалисты проводят анализ защищенности и тестируют компании на проникновение злоумышленников. CyberART является центром ГосСОПКА и обеспечивает безопасность объектов критической информационной инфраструктуры.

Постоянная ссылка на материал: http://www.smi2go.ru/publications/146751/