Desafío informático: aprenden de ciberseguridad en Hack@Tec 2023

Estudiantes del **Tec de Monterrey** participaron en **Hack@Tec 2023,** para adentrarse en el mundo de la **ciberseguridad y** ganar experiencia como **programadores competitivos.**

*“Esta edición se trata de un **ejercicio especializado en ciberseguridad,** para preparar a nuestros alumnos y que puedan ser **competitivos internacionalmente**”,* dijo Luis Muciño, encargado de cacería de amenazas de la institución.

*“Tuvimos personas desde primer hasta séptimo semestre. Fue una **experiencia muy variada** con gente de **tecnologías computacionales, electrónica, robótica y sistemas digitales**”,* agregó.

Conferencistas con experiencia en el campo de ciberseguridad se presentaron, entre ellos, **Francisco León, de la organización Palo Alto;** a la par de **Julio Santiago y Salvador Pulido, de Crowdstrike.**

Este evento se llevó a cabo el día 3 de noviembre en el Centro de Congresos, del campus Monterrey.


/> width="900" loading="lazy">

Ciberseguridad, una cacería de amenazas persistentes

Con la proliferación de **amenazas cibernéticas y la evolución de las tecnologías**, los ponentes recalcaron que la **formación en este campo es más crucial** que nunca.

*“La **ciberseguridad** es parte de nuestro día a día, de nuestras vidas, es algo que nos afecta a todos lo queramos o no”,* reflexionó Muciño.

*“Así como tenemos nuestro **sentido común en la vida real**, tenemos que tener ese mismo **sentido en la vida digital** y prepararnos en estos temas nos permite realizar todos los controles para llevar a nuestra **persona a un nivel más seguro**”*, añadió.

Siendo así, Pulido señaló a los estudiantes la **presencia de 250 adversarios cibernéticos (*hackers*) alrededor del mundo,** divididos por nombre, región, motivación, el tipo de táctica que utilizan, entre otros factores.

Igualmente, Salvador indicó que al menos **16 de los adversarios conocidos están trabajando activamente en México** y cuentan con la **capacidad de desestabilizar tanto al Estado** como a otros actores.

*“Ya no es como en la tecnología de antes. Aquí estamos hablando de **adversarios que son gente con muchísimas capacidades y recursos**, recursos que pueden venir hasta del mismo Estado donde operan”,* advirtió.

“*Cada vez se complica más el escenario con la transformación digital, esto hace que* ***tu superficie de ataque incremente muchísimo****, por lo que el valor de la sofisticación para la* ***contención de un ataque*** *cada vez sube más”,* añadió.

Esto ha generado un **aumento significativo en la demanda de capital humano con habilidades técnicas** capaces de hacer frente a ciberataques, particularmente en zonas como Latinoamérica, donde esta vulnerabilidad podría acabar con la empresa, mencionó.

“La ciberseguridad es parte de nuestro día a día, de nuestras vidas, es algo que nos afecta a todos lo queramos o no”.- Luis **Muciño**

/> width="900" loading="lazy">

Desplazarse en un entorno digital cambiante, el reto de los *hackers*

Como parte de la ponencia de Francisco León, los jóvenes fueron retados a **reflexionar sobre sus propias habilidades** en comparación con el trabajo de algunas de las **empresas de tecnología más conocidas.**

“Hay que ***conocer tus habilidades y las de tu enemigo*** *para que nunca te gane y te hagas mucho más fuerte. Podemos irnos preparando desde hoy,* ***no tienes que esperarte hasta estar en Apple*** *para sumergirte en el entorno”,* aconsejó León.

*“Es importante que **no vean los conceptos que no conocen cómo algo tan lejano o ajeno a ustedes**, porque les prometo que muchos de ellos ya los conocen y hasta los han ejecutado, solo que no lo sabían”,* reflexionó.

Dentro de esta nube de acciones y términos, el **conferencista invitado** utilizó como ejemplo el **“zero-day” (día cero)** término que se refiere al descubrimiento de una vulnerabilidad que aún no ha sido **corregida por su desarrollador.**

A pesar de que los alumnos rápidamente pueden identificar ejemplos de un **“zero-day” en productos como iPhones, carros e incluso drones**, León les animó a pensar cómo ellos ya habían sido parte de este concepto sin ser profesionales.

*“Todo mundo se **imagina un zero day como algo muy avanzado cuando realmente no lo es**, es algo que no se conoce, es algo desconocido”,* invita a la reflexión el ponente.

/> width="900" loading="lazy">

Los "*hackers*" del Tec triunfan ante un desafío común

La **prueba final** que enfrentaron los alumnos de este Hack@Tec reunió todos los elementos que aprendieron durante el día culminando en un **desafío digital que les pidió responder preguntas en torno a un simulador en ‘peligro’.**

Con más de **50 alumnos participando de manera individual y en equipos**, los jóvenes tuvieron menos de una hora para **detectar elementos 'malignos' en el escenario dado**, premiando a aquellos con el menor tiempo de respuesta.

*"Esta plataforma gira en torno al **tema del thread hunting, de estar buscando aquellos procesos maliciosos**, además de contestar información clave como: ¿Quién es el usuario?, ¿Quién es la máquina? Entre otras",* aclaró León.

*"El objetivo es que se pregunten: **¿De qué herramientas me puedo alimentar?** Al principio no va a haber muchas herramientas cuando lleguen a una **empresa o corporativo**, así que hay que defenderse con lo que tienen al alcance y adaptarse",* advirtió.

De este modo, **alumnos desde tercero a séptimo semestre** bajo los alias de "Satoshi Sakamoto" (participación individual), Energetic Lobster (equipo) y Blue Legend (equipo), obtuvieron los **primeros lugares en este desafío.**

Además de un premio sorpresa por parte de *Crowdstrike*, el **Departamento de Seguridad** del Tec ofreció a los alumnos **vacantes** dentro del área como parte de un *kickstart* para **impulsar su carrera en el área de ciberseguridad.**

*"En esto **no hay reglas tan estrictas,** pero en un escenario real donde no hay preguntas, no hay una guía y tienen que hacer este tipo de cuestiones en 10 minutos, **hay que ser muy bueno, practicar mucho y conocer de todo"**,* cerró Muciño.

TAMBIÉN TE PUEDE INTERESAR: