Instituto Tecnológico y de Estudios Superiores de Monterrey

Participación con Socio Formador, Miércoles 18 de Mayo de 2022

Juan Pablo Echeagaray González
A00830646

Análisis de Criptografía y Seguridad
MA2002B.300
Dr. Alberto F. Martínez
Dr.-Ing. Jonathan Montalvo-Urquizo

22 de mayo del 2022

Durante esta sesión con el Socio Formador Ing. Roberto Martínez, se nos introdujo a una nueva ideología enfocada a la ciberseguridad que todas las empresas deberían de adoptar. El ingeniero abrió la conferencia con la frase *Building out threat intelligence without action is about as valuable as not having intelligence at all*, haciendo referencia a que el campo de la ciberseguridad es un campo activo, en el que no basta con tomar medidas reactivas, uno debe de tomar acción para garantizar su seguridad.

La economía ya no puede funcionar de una manera local, el mundo globalizado necesita de una manera de conectarse; las tecnologías de la información son la herramienta de la que disponemos para hacer crecer nuestros negocios, pero hay que considerar, ¿a qué nuevos riesgos nos enfrentamos al depender de estas nuevas herramientas? Las nuevas amenazas que entran al campo de juego solamente pueden ser desarmadas por medio de herramientas de ciberseguridad, pensemos que la ciberseguridad tiene la tarea de cuidarle la espalda a nuestro negocio cuando nos conectamos a este nuevo mundo.

Ahora uno podría verse tentado a pensar que el uso de un buen antivirus y el uso de contraseñas seguras bastarían para asegurar la integridad de nuestras operaciones; la realidad es completamente diferente, al día de hoy no existe un sistema perfecto que nos defienda de todas las posibles amenazas que existen.

Cuando reconocemos que no existe una bala de plata en la ciberseguridad, debemos de definir qué ataques somos propensos a recibir, para nuestra suerte, la comunidad ya ha creado diversas bases de datos en las que se documentan los ataques sufridos por varios empresas; al día de hoy tenemos grandes fuentes de conocimiento en las que se registran identificadores de los atacantes, técnicas utilizadas, tipos de empresas atacadas y daños generados, con estos datos uno puede aproximar el rango de ataques a los que es propenso, para después analizar la arquitectura de su empresa en búsqueda de vulnerabilidades similares a las explotadas con anterioridad.

Otra técnica de defensa relativamente simple, pero de gran efectividad, es la aplicación de una *defensa en profundidad*, donde los archivos de una empresa se esconden por capas, poniendo en las capas inferiores los archivos más críticos; el motivo de ser de esta implementación es que haremos que el acceso a las últimas capas requiera de más recursos para los atacantes, reduciendo la rentabilidad de un ataque. A su vez, le daremos una mayor ventana de oportunidad a nuestras defensas, facilitando la tarea de identificación de vulnerabilidades.

La ciberseguridad es un campo dinámico, las estrategias implementadas ayer podrían no defenderme de las amenazas del mañana, siempre se debe de estar trabajando en fortalecer la arquitectura de nuestra red. Las empresas del presente deben pasar de una postura reactiva a una preventiva.