Certified Tech Developer
The Ultimate Degree

Práctica integradora Equipo 8

Objetivo

Vamos a poner en práctica los conocimientos que hemos adquirido hasta el momento. Se crearán grupos, divididos en sus respectivas salas y realizarán la siguiente ejercitación.

Actividad

Deberán leer cada una de las noticias asignadas y responder en un documento de Google Presentations para todas las mesas, las siguientes consignas:

- ¿Qué tipo de amenaza es?

  Es una amenaza de tipo **Ramsomware-as-a-Service**

- ¿Cómo comienza y cómo se propaga esta amenaza?

  Un 7 de mayo del presente año un ataque del ransomware DarkSide impactó a Colonial Pipeline, la compañía de oleoducto más importante de Estados Unidos, provocando el corte del suministro de nafta, diesel y otros productos refinados para un tramo de aproximadamente 8850 kilómetros que va desde Texas hasta Nueva York. La compañía confirmó

al día siguiente el ciberataque y afirmó que para contener la amenaza tuvieron que desconectar algunos equipos.

Las consecuencias de este ataque a una infraestructura crítica tan importante como Colonial Pipeline llevó a que la Administración Federal de Seguridad de Autotransportistas (FMCSA, por sus siglas en inglés) declarara la emergencia regional en Alabama, Arkansas, Washington D.C., Delaware, Florida, Georgia, Kentucky, Luisiana, Maryland, Misisipi, Nueva Jersey, Nueva York, Carolina del Norte, Pensilvania, Carolina del Sur, Tennessee, Texas, y Virginia.

- ¿Hay más de una amenaza aplicada?

  Muchos grupos de ransomware han estado aprovechando —entre otras vías de acceso inicial— las conexiones remotas como el RDP para acceder a los sistemas de las víctimas. Se logra vulnerando la red mediante ataques de fuerza bruta a las credenciales del RDP.

- ¿Qué solución o medida recomendarían?

  Recomendamos tener actualizado el sistema operativo de la empresa así como todos los parches de seguridad para evitar los ataques que van surgiendo. No tener un único punto de fallo, mantener una ética anti-hacker presente e implementar un proceso de auditoría de seguridad informática diariamente.

Una vez resueltas, volveremos a la sala principal en la cual el grupo debe compartir sus respuestas a los demás compañeros y compañeras, exponiendo la problemática y el análisis que realizaron.