Imagen que contiene Texto

Descripción generada automáticamenteCOMENTARIOS LECTURA #2

Fundamentos Avanzados Ciber Seguridad

Daniel Alejandro Olarte Ávila

Universidad Sergio Arboleda

Universidad Sergio Arboleda Cl. 74 #14-14

Bogotá, Colombia

Correo: [daniel.olarte01@correo.usa.edu.co](mailto:daniel.olarte01@correo.usa.edu.co)

Escuela de Ciencias Exactas e Ingeniería

Profesor: Juan Carlos Galindo Piraquive

06/02/2022

**“El ciclo de vida de un ciberataque basado en Ingeniería Social”**

La lectura en general me pareció muy interesante, este tema que es relativamente nuevo para mi me llama mucho la atención y cualquier cosa relacionada a esta me hace leer más artículos como este, y seguir investigando por mi parte, lo que me parece interesante de esta lectura es el cómo resalta un montón de aspectos nuevos que normalmente la gente no conoce sobre esto, dándonos a entender lo vulnerables que somos y en la cantidad de riesgos que podemos estar sin darnos cuenta.

El artículo es interesante debido a que además de mostrar una forma de cómo nos pueden sacar información personal como cuentas, contraseñas, fechas, etc. (Ingeniería Social). También nos cuentan de cómo podemos actuar para que todo eso no suceda, dando consejos para estar alerta a este método de hackeo el cual es tan peligroso debido a que se hace de forma clandestina. Y todo esto con fuentes confiables como el del Instituto Nacional de Ciberseguridad (INCIBE), el cual es el único organismo español en la recepción de vulnerabilidades de ciberseguridad.

Me parece muy interesante como comienza esta lectura, ya que nos empieza hablando de que es la ingeniería social, y nos habla un poco de Pishing (tema que ya hemos visto y ya nos hemos informado) lo que me dio curiosidad es un nuevo termino “Spoofing” el cual me hizo investigar por mi parte a que se refería este termino y luego llegar a buscar la diferencia entre Spoofing y Phishing.

Aparte de este nuevo termino, la lectura empieza directo con un dato muy importante el cual es el ciclo de vida de un ciberataque, el cual dice que cada ciberataque es único, pero aun así todos comparten características al cual lleva el ciclo de vida, este ciclo esta conformado por 4 fases los cuales son:

1. **Recolección de la información:**

La fase de Footprinting, la cual es la fase previa al engaño trata del intento de acumular toda la información posible para así poder estar informado de sus relaciones, interacciones, y demás cosas.

1. **Relación de confianza:**

Esta fase es la que sigue de la recolección de datos, en donde el ciberdelincuente se acerca a la victima a entablar una relación más cercana.

1. **Manipulación:**

La fase de la manipulación Psicológica, todo gracias a la confianza que se obtuvo en la fase anterior con la víctima. Una vez con confianza lo que busca el atacante es sacar todo tipo de información confidencial que sea necesaria para el ingreso al sistema necesario, o convencer a la víctima que realice determinada acción.

1. **Salida:**

Esta fase es sobre como ya extraída toda la información, se hace el intento de no dejar ningún tipo de sospecha que pueda recaer contra el atacante, todo esto para en un futuro seguir actuando por el mismo camino que se utilizo con todo el proceso sin ningún problema.

Lo más interesante es leer como nos da esos consejos para no caer en un hackeo simple, para que podamos actuar de diferente forma y evitar posibles riesgos que ya estamos sufriendo. En la lectura habla de como el INCIBE tiene iniciativas gratuitas para garantizar la seguridad de las compañías, las cuales me parecen muy interesantes, que van desde la concienciación hasta videos e interacciones para hablar sobre como actuar frente a un ataque de estos.