Imagen que contiene Texto

Descripción generada automáticamenteCOMENTARIOS LECTURA #4

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

22/02/2022

**“Así ha evitado Microsoft el robo de millones de contraseñas”**

La lectura en general me pareció muy interesante, este tema que ya llevamos viendo desde el principio del semestre 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. (Phishing) y otros métodos de robos de contraseña (Fuerza Bruta). También nos cuentan de cómo podemos actuar para que todo eso no suceda, dándonos consejos para evitar y estar alerta a este método de hackeo el cual es tan peligroso debido a que se hace de forma clandestina, y como principal objetivo ilustrarnos de como una empresa tan conocida como Microsoft ha llegado a proteger millones de contraseñas.

Me parece muy interesante como comienza esta lectura, ya que nos empieza hablando como los clientes de servicios de Microsoft como Office 365 y Azure AD, constantemente están siendo parte de un intento fallido de robos de sus contraseñas, donde ya Microsoft ha evitado miles de millones de estos intentos de Phishing y Fuerza Bruta, dándonos estadísticas como que de 2021 bloquearon mas de 25600 millones de ataques por fuerza bruta contra Azure AD, y otros 35700 millones de ataques de Phishing a través de Office 365, dando así un total de mas de 61300 ataques bloqueados de forma exitosa.

La lectura resalta que Microsoft cuenta con soluciones de seguridad muy avanzadas que le permite reducir e incluso evitar este tipo de ataques que se ven todos los días en sus servicios y en cualquier lado de Internet. Todo esto gracias al conocimiento previo, de grandes bases de datos que les permite detectar todas estas amenazas.

Algo fundamental que nos cuenta el artículo, es de como aun que llegan a evitar estos millones de ataques aun así no son lo suficiente, debido a que se siguen viendo como varios ataques de Fuerza Bruta o Phishing se cuelan de forma clandestina escabulléndose de las medidas de seguridad planteadas, ahí es donde entra el usuario de que deben saber a defenderse y saber cómo actuar ante esos casos, los cuales nos cuentan varias medidas a tomar en cuenta para estar preparados a la hora de recibir uno de estos intentos de ataque y robo.

De las medidas a tomar en cuenta que nos aconseja Microsoft para evitar estos ataque están más allá de la autenticación de 2 pasos (que aun así sirve bastante), en donde podemos encontrar el actualizar a las últimas versiones ya sea del sistema operativo o de cualquier programa que se usa, debido a que normalmente cada actualización se lanza para resolver algún fallo o para mejorar algún tema de seguridad que tenía el Software anteriormente.

Otro aspecto muy importante es contar con firewalls o programas de seguridad, debido a que un buen antivirus puede detectar todos los malwares que ponen en riesgo el equipo, manteniendo que no se descargue ni se hagan procesos sospechosos de ataques para poder navegar de cierta forma segura en el equipo, sin estar preocupado de un posible malware ingresando por el equipo.