EL INCIDENTE CRITICO

JESUS DAVID DE LA HOZ PEÑA

UNIVERSIDAD POPULAR DEL CESAR

VALLEDUPAR

2025

Paso 1: Identificar el vector de ataque inicial

El 22 de febrero de 2020, se detectó una actividad sospechosa en la cuenta de Facebook de un empleado administrativo. Se observó que alguien había accedido a la cuenta, ingresado a diversas carpetas y descargado información. Sin embargo, ese día el empleado se encontraba de vacaciones, lo que levantó sospechas sobre la seguridad de su cuenta. Al investigar, el trabajador descubrió que había recibido un correo electrónico que, aparentemente, provenía de Facebook, con un enlace que dirigía a una página muy similar a la oficial de la plataforma. Sin sospecharlo, el empleado ingresó sus datos en ese sitio, lo que permitió que su información fuera robada. Esto sugiere que el incidente fue el resultado de un ataque de phishing, en el cual un atacante engañó al usuario para que proporcionara sus credenciales en un sitio web falso.

Paso 2: Analizar los logs del Sistema para Encontrar Evidencias de Actividad Maliciosa

Los logs fueron revisados en el visor de eventos, los cuales nos mostraban que un usuario entró a las 2 am de la mañana a la cuenta del propietario original, otro log que mostraba que carpetas confidenciales pertenecientes a Facebook fueron abiertas varias veces, un log que mostraba que todos estos archivos anteriormente fueron descargados y finalmente otro log seria el correo enviado, a pesar de que tenía la misma apariencia que la página de Facebook, tenía diferente link lo cual se podría decir que no era la página legitima.

Paso 3: Determinar el Alcance del compromiso y los sistemas afectados

Una vez se mira el sistema comprometido, hay que mirar que datos han sido robados, en este caso descargaron varios datos importantes de Facebook en la cuenta del usuario, por parte de la disponibilidad se ha violado debido a que si el usuario no está en horarios laborales el sistema no debería estar disponible,

en la integridad podría decirse que sí, ya que solo la persona que es autorizada debería poder descargar los archivos, para eso debería haber otra verificación, y también fue violada la confidencialidad ya que el atacante pudo ver toda la información secreta de esa cuenta.

Paso 4: Proponer medidas de contención inmediatas

Una vez se detecta el sistema comprometido, lo ideal es desconectarlo de la red, en este caso también se podría bloquear la cuenta para que no se pueda volver a entrar y luego cambiar las credenciales, además en caso de que se haya dado permiso a otras aplicaciones externas revocar estos permisos, en este caso solo descargaron datos y no se alteró más nada, además de esto implementar medidas de verificación de 2 pasos en todas las cuentas administrativas para que no vuelva a suceder y bloquear el usuario que ha enviado el correo de phishing, por ultimo revisar una vez mas que no haya alterado nada, en caso de esto se hace por medio de la copia de seguridad, una vez validado todo correctamente se vuelve a habilitar la cuenta para el propietario original.

Finalmente, se le debe informar de la situación al departamento de seguridad de la empresa (Facebook) para que planeen estrategias como mejor capacitación a los trabajadores, mejorar la seguridad a los sistemas como por ejemplo con verificación 2 pasos y además investigar a fondo el responsable y que no se hayan perdidos datos en toda esta situación