Jorge Iván Ramos Murgas

Taller Laboratorio:

Paso 1:

Recibimos un ataque de Phishing, entre los primeros signos que pudimos encontrar es un ordenador que funcionaba de mala manera, intentos de inicio de sesión de manera no autorizadas, alertas de inicio de sesión, viendo el correo del empleado podemos encontrar un correo de una cuenta que se hizo pasar por una entidad legitima y este correo contenía un archivo adjunto pdf, a la hora de pasar este pdf a un antivirus nos pudimos dar cuenta que este archivo contenía un malware

Paso 2:

Entre los logs que se deberían de buscar los logs de autenticación, las alertas de seguridad y los intentos de cambio de contraseña en el dispositivo, se deben inspeccionar de detenida manera los intentos de inicio de sesión de manera fallida, también cuando se desactiva la verificación en dos pasos, o cuando se realizan cambios de contraseña en un periodo corto de tiempo.

Paso 3:

Lo que se debería hacer en estos casos seria desconectar de la red al equipo que fue afectado para no comprometer los otros equipos que se encuentran conectados a la red, luego revisar que los equipos que se encontraban conectados a la red no se encuentren afectados para saber el alcance que tuvo el malware, también revisar y evaluar el impacto que puede tener este dispositivo infectado en la empresa

Paso 4:

Para poder prevenir que el ataque se expanda lo mejor seria desconectar de la red al equipo para evitar que se expanda, realizar una actualización del sistema con el fin de poder corregir las vulnerabilidades del equipo para evitar que vuelva a suceder, también se deberían de realizar el cambio de las credenciales del equipo afectado cambiando la contraseñas, activando la verificación en dos pasos y quitando las sesiones que se encuentren activas.

Como plan de recuperación de los datos lo ideal seria restaurar todo mediante la copia de la seguridad, verificar que el equipo se encuentre en optimas condiciones y no se encuentre afectada y realizar una evaluación post incidente con el fin de que no vuelva a suceder.

Este hecho debería de ser comunicado a los altos mandos de la empresa y también a los empleados que trabajan en dichos equipos con el fin de poder tener conciencia sobre lo sucedido y poder llegar a evitar que se pueda repetir.