LABORATORIO 3 CYBERSEGURIDAD

1. A varios trabajadores de mi empresa comenzaron a llegarles correos muy extraños y con un patrón muy común del mensaje, incluso a uno de los trabajadores ingreso al enlace del correo e informo que desde que recibió este correo su computadora se apago repentinamente y no pudo encenderla, lo cual claramente se trata de un ataque de phishing.

2. Para identificar que fue un ataque de phishing revisamos lo correos de los trabajadores y notamos que los enlaces no eran los mismos y aparte notamos que cada correo tenía un enlace similar al que se envió lo que significa que exactamente este ataque fue por el correo ya que no hubo ningún otro fallo en general.

3. Solo a un trabajador se le infecto el computador, por lo tanto, a este fue el que se le dio prioridad para solucionar el problema del virus para que ah si no pueda infectar más dispositivos y de puede perjudicar a la empresa dentro de los 3 pilares de la seguridad se debe analizar lo siguiente:

   Disponibilidad: Identificar que los equipos no hayan sido afectados por el virus y eliminar todos los posibles correos de phishing para no tener otro inconveniente como este.
   Integridad: Identificar si algún dato sensible dentro de la empresa se ha modificado o eliminado, y mas que todo cambiar la dirección de todos archivos en eso
   Confidencialidad: En esta toca analizar si el virus llego a interferir en el acceso de inicio de sesión del trabajador, y de ser el caso lo mas probable es que toque darle otro dispositivo al trabajador para que ah si pueda trabajar sin ningún problema.

4. Con lo sucedido lo primero que se hizo fue desconectar la red del dispositivo infectado, para que ah si no pueda comprometer a los demás dispositivos de la empresa, a la computadora afectada se aisló para ah si estudiar el virus y poder eliminarlo, también se pudo recuperar la información comprometida del trabajador mediante la copia de seguridad y gracias a esto, parte del trabajo que hizo el trabajador no fue perdida, y como ultimo se le notifico al Administrador del servidor de lo que ocurrido para que ah si pueda tomar medidas sobre el servidor y proteger la información comprometida frente al virus.

Curso de Cisco