INCIDENTES DE CIBERSEGURIDAD

Unidad 1. Actividad 3

17 DE OCTUBRE DE 2023

CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

Ejercicio 1.

IDEALIZA CASOS DE CIBERINCIDENTES PARA CADA UNO DE LOS NIVELES DE IMPACTO DESCRITOS POR EL INCIBE .-

PARA ELLO UTILIZA LA CLASIFICACIÓN DE CIBERINCIDENTES DADA POR EL INCIBE .-

Los incidentes se asociarán a alguno de los siguientes niveles de peligrosidad: CRÍTICO, MUY ALTO, ALTO, MEDIO, BAJO.

Crítico

Una serie de ciberataques que utilizaban un exploit de Día Cero (Un exploit de día cero es un fallo de seguridad no descubierto previamente en tu software o hardware que los hackers pueden aprovechar para penetrar en tus sistemas) para instalar el troyano Hydrag, destinado a robar información. Google fue la primera empresa pero hubo otras como bancos , compañías eléctricas …

Investigaciones de McAfee pusieron de manifiesto que el objetivo inicial del ataque era ganar acceso y modificar el código fuente de los repositorios de las víctimas.

Muy alto

Uber pagó cien mil dólares a dos hackers para eliminar los datos robados y ocultar el ciberataque, manteniéndolo en secreto. El ataque tuvo lugar en octubre de 2016 -un año antes de su publicación- e incluyó la exposición de nombres, correos electrónicos y números de teléfono de 57 millones de clientes en todo el mundo, así como la información personal de 7 millones de conductores de esa empresa de transporte.

Alto

La empresa Equifax, una de las principales agencias de informes de crédito en los Estados Unidos, sufrió un importante ataque de phishing que llevó a una violación de datos masiva.

En este caso, los atacantes aprovecharon una vulnerabilidad en una aplicación web de Equifax y engañaron a los empleados para que proporcionaran credenciales de acceso. La brecha de seguridad resultante expuso la información personal y financiera de millones de personas.

Medio

El caso de "Target" en 2013, los atacantes comprometieron las credenciales de un proveedor de servicios de HVAC (calefacción, ventilación y aire acondicionado) de Target y utilizaron esas credenciales para acceder a la red de la empresa. Una vez dentro, los ciberdelincuentes pudieron moverse lateralmente por la red, ganar acceso a sistemas sensibles y finalmente robar datos de tarjetas de crédito de millones de clientes.

Este ataque de suplantación de identidad resultó en una violación masiva de datos y tuvo un impacto significativo tanto en Target como en los clientes afectados.

Bajo

Hace un par de meses, en la empresa de Interalmeria, recibió un ataque de spam a través de sus redes sociales. Este problema vino desde una plataforma llamada socialmedia donde publicaban desde ahí los post diarios y semanales. El problema se soluciono a las horas cambiando de contraseñas en cada una de las redes sociales