Universidad del Caribe
2000 CANCUN, QUINTANA ROO, MÉXICO
CONOCIMIENTO Y CULTURA PARA EL DESARROLLO HUMANO

20 AÑOS
CRECIENDO CON EL SIGLO

"TAREA #998"

Alumno: Kanxoc Ay Cesar David

Matricula: 200300581

Materia: Tópicos Selectos para Ingeniería.

Docente: Ismael Jiménez Sánchez

El hack de eBay

Casi todo el mundo conoce eBay por ser una empresa gigantesca de comercio electrónico que permite que cualquiera pueda vender sus productos. En mayo de 2014 las bases de datos que contenían nombres de usuarios, contraseñas, direcciones físicas y números de teléfonos fue atacada por un grupo de hackers llamado “The Syrian Electronic Army“. Este mismo grupo es culpable de atacar sitios como Twitter, The New York Times, LinkedIn y varias cuentas de Twitter prominentes.

A pesar de que el grupo no hizo nada con la información obtenida de eBay, la empresa no actuó de la manera más abierta posible. De hecho, tuvieron la suerte de que el problema no empeoró porque tardaron más de tres meses en anunciarlo (pidiendo a sus usuarios que cambiaran las contraseñas) y se vieron potencialmente afectados unos 145 millones de personas.

La base de datos fue vulnerada utilizando solo nombres de usuarios y claves del personal, eso significa que eBay no está valorando nuestra información personal tanto como debería.

Cuándo pasó: En mayo de 2014 las bases de datos que contenían nombres de usuarios, contraseñas, direcciones físicas y números de teléfonos fue atacada.

Cómo lo solucionaron: Pidiendo a sus usuarios que cambiaran las contraseñas, como primer paso, en lo que ellos investigaban a fondo el problema.

Qué datos se expusieron: Bases de datos que contenían nombres de usuarios, contraseñas, direcciones físicas y números de teléfonos.

Quién fue el atacante: un grupo de hackers llamado “The Syrian Electronic Army”.

Impacto de la brecha: Se vieron potencialmente afectados unos 145 millones de personas. Por lo tanto se considera como una de las brechas de seguridad más grandes de la era digital.

Recomendaciones para prevenir brechas de seguridad: Se puede prevenir bastante realizando copias de seguridad de tus archivos y usando contraseñas seguras para todas tus cuentas en línea.

Lamentablemente el usuario no tiene manera de saber si una empresa en la que confía se ha visto afectada por un problema de seguridad de este tipo, y si algo

demuestran estos ejemplos es que no es sino hasta que el problema es tan grande que no puede ser escondido por más tiempo, que termina saliendo la verdad a la luz. La moneda de cambio en la red es la información, y siempre habrá personas con malas intenciones intentando obtenerla por el medio que sea. Da mucho que reflexionar que algo tan grave como Heartbleed no fue descubierto hasta que tenía más o menos dos años afectándonos.