



**U**niversidad  
**del C**aribe

2000

CANCUN, QUINTANA ROO, MEXICO

CONOCIMIENTO Y CULTURA PARA EL DESARROLLO HUMANO

## **Ingeniería en Datos e Inteligencia Organizacional**

### **Brecha de seguridad**

#### **Profesor:**

Ismael Jiménez Sánchez

#### **Alumnos:**

Chi Huchim Emily Rubi

### **Tópicos selectos en ingeniería en datos**

En el 2014 Home Depot afirmó experimentar una brecha de seguridad, el siguiente párrafo muestra lo dicho por la empresa en ese entonces:

“El pasado martes 2 de septiembre revelamos que estábamos investigando una posible brecha en nuestros sistemas de datos de pago. Queremos que sepan que hemos confirmado que esos sistemas, en efecto, han sido comprometidos, lo cual podría impactar en cualquier cliente que haya usado su tarjeta de pago en nuestras tiendas de Estados Unidos y Canadá, desde abril en adelante. No tenemos evidencia de que la brecha haya impactado tiendas en México o clientes que compraron online en HomeDepot.com”

La información robada permite a los delincuentes crear copias falsas de tarjetas de crédito y débito, que pueden ser usadas para comprar. Pero si quienes compran tarjetas robadas logran cambiar el PIN de las cuentas, pueden incluso utilizarlas para sacar dinero de cajeros automáticos.

La puerta de entrada de los cibercriminales parecería ser una débil autenticación en los sistemas de la compañía, y malware que se instaló en la red o en los dispositivos de Punto de Venta o Point of Sale (PoS). Ya hemos visto qué amenazas atacan contra estas terminales.

En ese sentido, ya que las empresas del sector comercial están orientadas a garantizar la satisfacción del cliente, no pueden permitirse que ciertos episodios como los anteriormente mencionados, fuga de información o ataques dirigidos a su operación normal dañen su imagen, o la calidad del producto que ofrecen.