Target

Carmen Xia Martínez Espinosa, Natalia Gutiérrez López

Target

¿Qué ha pasado en la empresa? 2

¿Cómo se relaciona el ataque con la transformación digital que sufre una empresa? ¿Cuáles fueron los puntos débiles por los que lo atacaron? 2

Analiza y define como fue la reacción de Target a corto y largo plazo ante este hecho 3

Análisis cronológico de la evolución de la tipología de ciberataques producidos. 3

La empresa Target, es una empresa minorista de mercaderías que vende productos mediante sus tiendas y canales digitales. Sus tiendas ofrecen una variedad de alimentos; perecederos, comestibles secos, lácteos y productos congelados.

¿Qué ha pasado en la empresa?

En diciembre del año 2013, esta empresa sufrió un ciberataque a través de un malware PoS.

Debido a este malware, sus dispositivos y una cifra de 70 millones de clientes quedaron afectados. Información personal como correos electrónicos, números de teléfonos, nombres, direcciones y datos bancarios quedaron comprometidos.

El malware PoS, perjudica a los lectores de tarjetas de crédito, débito y cajas registradoras. Este ataque se produjo en periodo previo a las compras de navidad.

¿Cómo se relaciona el ataque con la transformación digital que sufre una empresa? ¿Cuáles fueron los puntos débiles por los que lo atacaron?

Una empresa, cuando pretende transformarse digitalmente, cumple unos pasos a seguir; cambia la cultura empresarial y la organización interna de la empresa, busca nuevos objetivos y nuevas estrategias empresariales usando la nueva tecnología, por ello debe mejorar el departamento de inteligencia digital…

Deben hacer frente a los nuevos competidores y sobre todo ofrecer productos y servicios que les hagan diferenciarse de la competencia.

El ataque se pudo haber producido debido al aumento de la dependencia de las nuevas tecnologías y la falta de medidas de seguridad.

Tras el ataque, la empresa ha aumentado considerablemente su sistema de seguridad, reduciendo así el riesgo a un nuevo ataque, pero no evitando completamente el riesgo de sufrirlo de nuevo.

En la actualidad, la empresa tiene un sistema de detección de malware “skimming web”, basado en un código abierto. Funciona de la siguiente manera: mediante un simulador, se realiza una compra en la página web y se identifican los códigos maliciosos que pretenden robar información de las tarjetas de crédito y débito de los clientes.

Pero, el principal debate que se nos presenta es, ¿porque se están produciendo más ataques cibernéticos a las empresas en pleno periodo de transformación digital? Tenemos varios puntos que pueden provocar un aumento de los casos de ataques a empresas.

1. Existe una mayor exposición, la pandemia ha acelerado el proceso de transformación digital. Las empresas han adoptado nuevas tecnologías y herramientas que aumentan su exposición en la red y a sus riesgos.

2. No hay la seguridad adecuada en las empresas para proteger sus sistemas y datos. Puede deberse a la falta de conocimientos o recursos o simplemente a la falta de atención.

3. Incentivos económicos, normalmente se produce un secuestro de datos y se extorsiona a las empresas para que den la cantidad requerida por los ciberdelincuentes. Con la transformación digital, las empresas están generando cada vez más datos valiosos y eso hace que se centren en el punto de mira para los delincuentes.

En resumen, la transformación digital ha aumentado la exposición y la complejidad de los sistemas de las empresas, lo que a su vez ha aumentado los riesgos cibernéticos y la necesidad de una seguridad adecuada. Es importante que las empresas tomen medidas para proteger sus sistemas y datos, incluyendo la implementación de medidas de seguridad y la capacitación de los empleados sobre los riesgos cibernéticos.

Analiza y define como fue la reacción de Target a corto y largo plazo ante este hecho

Target a corto plazo tomó grandes medidas para solucionar las consecuencias del ataque.

En primer lugar, se dio el anuncio del incidente para informar a sus clientes, de esta forma los clientes fueron capaces de detectar rápidamente si sus datos habían sido robados. El siguiente paso que Target llevó a cabo fue la investigación interna del suceso para así comprender lo ocurrido y detectar las vulnerabilidades para poder remediarlas. Tras detectar algunas de las vulnerabilidades, Target contrató expertos en ciberseguridad de una empresa externa. De esta forma se redujeron las vulnerabilidades y se mejoró la seguridad digital de Target. Y además, hubo una compensación a los clientes, ofreciendo un servicio de monitoreo del crédito así como indemnización económica.

A largo plazo, Target principalmente aumentó su inversión en ciberseguridad. Hubo un cambio en el liderazgo, con la contratación de un nuevo CEO y director de seguridad de la información. Además, de la adopción de nuevas tecnologías.

Análisis cronológico de la evolución de la tipología de ciberataques producidos.

1. 2017: WannaCry Ransomware - Este ataque afectó a más de 300,000 dispositivos en todo el mundo. Fue un ransomware que explotó una vulnerabilidad en el sistema operativo Windows. Los ciberdelincuentes exigían el pago de un rescate en Bitcoin para liberar los sistemas.
2. 2017: Equifax Breach - Este ciberataque afectó a la compañía de informes de crédito Equifax. Los ciberdelincuentes accedieron a la información personal de 147 millones de personas, incluyendo nombres, direcciones y números de seguridad social.

3. 2018: Facebook Cambridge Analytica Scandal - Este escándalo involucró la recopilación y explotación de datos de millones de usuarios de Facebook por parte de Cambridge Analytica, una firma de consultoría política. Los datos se utilizaron para influir en las elecciones presidenciales de EE. UU. de 2016.
4. 2018: Marriott Breach - Este ciberataque afectó a la cadena hotelera Marriott International. Los ciberdelincuentes accedieron a la información personal de 500 millones de clientes, incluyendo nombres, direcciones y números de pasaporte.
5. 2019: Capital One Breach - Este ciberataque afectó al banco Capital One. Los ciberdelincuentes accedieron a la información personal de más de 100 millones de clientes, incluyendo nombres, direcciones y números de seguridad social.
6. 2020: SolarWinds Supply Chain Attack - Este ataque afectó a una empresa de software llamada SolarWinds. Los ciberdelincuentes utilizaron una técnica de cadena de suministro para comprometer la seguridad de sus clientes, incluyendo varias agencias gubernamentales de EE. UU.
7. 2021: Colonial Pipeline Ransomware Attack - Este ataque afectó a la compañía de transporte de combustible Colonial Pipeline. Los ciberdelincuentes utilizaron un ransomware para bloquear el acceso a los sistemas de la empresa y exigieron un rescate en Bitcoin.