TARGET
A SECURITY NIGHTMARE?
Something to Ponder?

Dra. Isabel Maassardjian
Facultad de Ingeniería y Tecnologías
Universidad Católica del Urugay
Mayo 2014

BRECHA EN LA SEGURIDAD
VIERNES NEGRO

27 de noviembre al 15 de diciembre de 2013

HECHOS

- Cómo los intrusos llegaron a un sector interno de la red de los equipos de los puntos de venta, desde el sistema externo de facturación de Target?

- 40 millones de transacciones presenciales, con tarjetas de crédito y débito, con acceso a los datos asociados, bandas magnéticas
- 70 millones de clientes de quienes se sustrajeron nombres, emails, domicilios y teléfonos
- Acceso a cajeros automáticos, en caso de haber obtenido las claves de las tarjetas

TEORÍA DE UNA INTRUSIÓN…

- Los hackers ingresaron al sistema informático de Target a través de uno de sus proveedores: Fazio Mechanical Service
- Acceso para ayudar a ahorrar energía, pero la red no estaba debidamente aislada de la red de datos de ventas y pago
- Credenciales fueron robadas en un ataque de malware de correo electrónico a Fazio Mechanical Service enviado a los empleados
- Los atacantes fueron capaces de infectar los dispositivos de punto de venta de las cajas en las tiendas Target con un malware estableciendo un servidor de control dentro de la red interna de Target, que sirvió como un repositorio central de todos los registros infectados
- Error crítico: falta de aislamiento de los portales de sus proveedores de su red de pagos (separación entre cajas registradoras de sus tiendas, su climatización informatizada y los controles de refrigeración).

Fazio Mechanical Services

Fazio Mechanical is "Refrigeration"

Home | About | Services | Safety | Contact

- About Fazio Mechanical
- Fazio Services
- Safety Dedicated
- Directions to Fazio
- Contact Fazio

Fazio Mechanical is licensed in:

Pennsylvania
West Virginia
Maryland
Virginia
Ohio

View Fazio's Statement on Target Data Breach

At Fazio Mechanical we have a passion for design, engineering, installation, service and support and all while keeping a focus on saving energy. Learn more ...

Fazio Mechanical Services is a full-service mechanical contractor that specializes in the design, installation, and service of the most advanced, cost effective and environmentally-friendly supermarket refrigeration systems in the industry.

We service customers in Western Pennsylvania, Eastern Ohio, and parts of West Virginia, Maryland and Virginia. We bring the technical knowledge, experience, and proven performance that is "second-to-none" in the refrigeration industry.

"Fazio Mechanical is ..... Refrigeration"

FAZIO MECHANICAL SERVICES

- “Nuestra conexión de datos con el objetivo era exclusivamente para la facturación electrónica, la presentación de contratos y la gestión de proyectos, y Target es el único cliente para el que gestionamos estos procesos de forma remota. No hay otros clientes que se hayan visto afectados por la violación. Nuestras medidas de sistemas de TI y de seguridad están en plena conformidad con las prácticas de la industria.”

- Método principal de detección de software malicioso en su sistemas internos era la versión gratuita de Malwarebytes Anti-Malware

- La lista de clientes incluye grandes tiendas minoristas como Wal-Mart Stores, Inc. Costco Wholesale Corp. (COST), estaciones de combustible y restaurantes como Denny's Corp.

- Niega los reportes en blogs y portales en los cuales se dice que la empresa monitorea a distancia el sistema de aire acondicionado de Target

TARGET

- "La investigación forense actual ha indicado que el intruso robó las credenciales de un vendedor, que fueron utilizados para acceder a nuestro sistema“.
- Comunicado de prensa lamentando lo ocurrido y contacto con cada uno de los afectados
- Un año de monitoreo gratis de las cuentas y protección para el robo de identidad de quienes hayan comprando en sus tiendas
- Reconoció que los PIN fueron robados pero la empresa codifica los datos mediante un cifrado triple
- Los clientes de Target que hicieron compras en la tienda donde ocurrió la brecha deberían de comunicarse con sus bancos para solicitar una tarjeta de reemplazo y cambiar su número PIN
- A partir de mediados de enero, enfrenta más de 70 demandas, incluyendo demandas colectivas de los consumidores y los bancos

Y DESPUÉS QUÉ?.....

SISTEMA FINANCIERO

- Los bancos aseguran que han gastado dinero alertando clientes, reembolsándoles por cargos fraudulentos, reemplazo de tarjetas, cierre y apertura de cuentas, y advierten que sus pérdidas pueden ser mayores si terceros usan los datos robados

- Asociación de Banqueros para Consumidores y a la Asociación Nacional de Unión Crediticia tuvo un gasto de U$S 200 millones para cambiar las tarjetas de crédito y débito

- Buscan una compensación por los gastos incurridos

❖ **Actitud de los consumidores**:

- Demandas judiciales como la demanda colectiva presentada por el bufete de abogados Hagens Berman Sobol Shapiro LLP en California
- La demanda de Hagens Berman afirma que Target fue notificado acerca de las vulnerabilidades en sus sistemas en los puntos de venta de caja en 2007 y se califica como un caso de derechos del consumidor
- críticas a través de las redes sociales
- protestas fuera de algunas de sus tiendas

❖ **TARGET**:

U$S 61 millones de dólares es el costo que tuvo la empresa entre los gastos de la investigación del ciberataque, los costos legales, la contratación de más personal para su servicio de atención al cliente y nuevas medidas de seguridad para los medios de pago, si bien los seguros se hicieron cargo de U$S 44 millones

RESULTADOS…

- El Departamento de Justicia y el Servicio Secreto investigan el caso

- Varias personas en la frontera entre México y Estados Unidos usaron tarjetas con información de cuentas de clientes de Target del sur de Texas, con las cuales compraron cientos de productos en otras tiendas del área

- Otros datos robados podrían haber aparecido entre las 100 tarjetas requisadas en Texas

- Se advirtió a minoristas estadounidenses sobre eventuales ataques cibernéticos después de descubrir unos 20 casos de piratería en el último año que tuvieron el mismo tipo de software malicioso utilizado en contra de Target durante la temporada de compras navideñas.

LEGISLACIÓN

- El robo de datos en la cadena minorista Target Corp. ha puesto la atención en las leyes estatales de notificación a los consumidores, renovando la necesidad de contar con un estándar único en Estados Unidos, ya que varían según el Estado de que se trate.
- Los consumidores en un Estado podrían enterarse inmediatamente que ha sido expuesta su información personal, pero eso podría no ocurrir en otro Estado y los requerimientos de notificación para los negocios dependen en dónde están ubicados sus clientes.
- Dificultades para lograr un estándar: Grupos defensores de los consumidores no quieren debilitar las protecciones existentes en los estados con leyes más fuertes, mientras que las cadenas minoristas quieren leyes que sean menos trabajosas para acatar y dicen que demasiada notificación podría ocasionar que los consumidores no tomen en cuenta el problema.
- El Congreso analiza diferentes propuestas sobre cómo se tendría que aplicar cualquier estándar nacional y cuál tendría que ser el umbral antes de que se exija aplicar el requerimiento de notificación.