Buenos Aires, 27 de septiembre de 2021

Sr. Matías Videla
Gerente General
Cencosud S.A.

Ref: Informe sobre Ciberataque de 2020

De mi consideración,

Tengo el agrado de dirigirme a Usted, con la finalidad de enviarle el informe titulado “Ciberataque a Cencosud del año 2020: impacto de la filtración de datos en los clientes”.

En el mismo se brinda información detallada sobre las implicancias de la obtención de información por los autores del ataque, principalmente el peligro que representa el robo de identidad. En adición, se presentan las problemáticas actuales de seguridad de los canales de comunicación tradicionalmente utilizados.

Espero que este informe sea de utilidad y cumpla con sus expectativas. Le agradezco por su tiempo y atención en la lectura del mismo. Quedo a su disposición ante cualquier comentario o consulta.

Saluda atentamente,

Sergio Calderón

Ciberataque a Cencosud del año 2020: impacto de la filtración de datos en los clientes

Calderón, Sergio Leandro

bs.sergiocalderon@gmail.com.ar

Av. Leandro N. Alem 1067 – Piso 9 – Buenos Aires

Índice

Resumen 1

Palabras clave 1

Introducción 1

Usurpación de datos 2

Implicaciones de la información patrimonial 2

Implicaciones de la información de contacto 3

Discusión 4

Conclusiones 4

Bibliografía 5

Glosario 5

Resumen

En el contexto pandémico, la dependencia de dispositivos electrónicos ha aumentado considerablemente, reflejado en aspectos como las compras online y el trabajo desde casa. A raíz del ciberataque producido a Cencosud en el año 2020, se filtró información muy comprometedora de los clientes. En este informe se detalla una clasificación de los datos almacenados en empresas comerciales, destacando el grado de privacidad normal de los mismos, y se analiza el grado de alcance que ha ocasionado y puede ocasionar su conocimiento por parte de terceros. Principalmente se explica su utilización para entrar en contacto con las personas, a través de medios tradicionales, y realizar una suplantación de su identidad. También se identifican los principales errores por parte de la empresa luego de producirse el robo de datos, y cómo ciertas acciones quedan completamente en manos del usuario.

Palabras clave

Filtración de datos, ingeniería social, privacidad, spam, suplantación de identidad.

Introducción

En la última década, los ataques cibernéticos han aumentado en frecuencia e ingenio. El bajo costo y el riesgo mínimo que conllevan estos delitos han sido factores clave en su crecimiento. Con el simple uso de una computadora y el acceso a Internet, los ciberdelincuentes pueden causar daños enormes mientras permanecen relativamente anónimos (Urrutia, 2020).

En seguridad informática, se define como ingeniería social a la práctica de obtener información confidencial mediante la manipulación de usuarios legítimos. Entre las formas de ataque más utilizadas se encuentra la suplantación de identidad por medio del *phishing* (ver glosario), que requiere de datos certeros de la empresa y el cliente.

A partir del inicio de la pandemia de COVID-19, se produjo un incremento notable de ciberataques a empresas en todo el mundo. Concretamente, en América Latina los países del Cono Sur son los más atractivos para los hackers, por su capital, gran población y adoptación rápida de tecnologías, aunque, a la vez, aún muy detrás del resto del mundo respecto a mecanismos de ciberdefensa y políticas de cumplimiento general (Wright, 2020).

El objetivo del presente informe es informar sobre el caso de ciberataque a la empresa Cencosud ocurrido en noviembre de 2020 y analizar sus consecuencias, con especial énfasis en el peligro que representa la suplantación de identidad y el envío de mensajes falsos a los clientes de la empresa víctima del ciberataque.

Usurpación de datos

Las empresas de carácter multinacional, en general, cuentan con una gran base de datos tanto de sus clientes como empleados. Al efectuarse un ciberataque existe gran probabilidad de que los atacantes involucrados logren tener acceso a una parte considerable de dicha información, que puede ser cifrada[1], difundida y/o usada para realizar phishing.

Asimismo, en la mayoría de los casos, los datos filtrados resultan muy variados en importancia y contenido, por lo tanto, su uso puede tener diferentes implicaciones. A continuación, se presenta una clasificación de los datos almacenados en una empresa comercial.

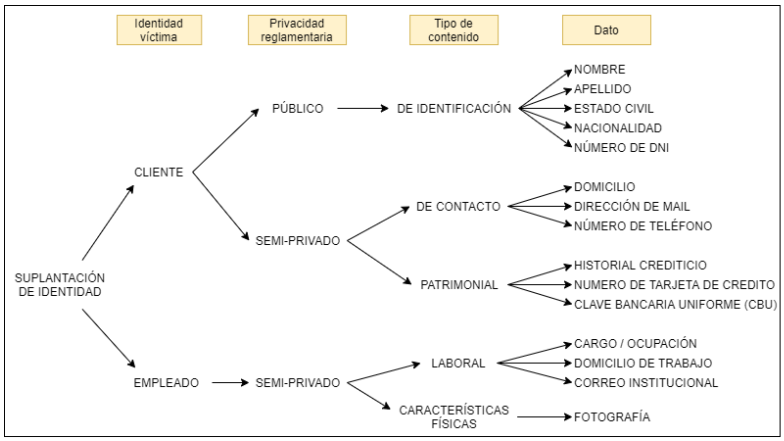

Figura 1. Clasificación de los datos almacenados en una empresa de comercio

Como se puede observar en la Figura 1, existen dos grupos que se encuentran bien diferenciados según el nivel reglamentario de privacidad. En general, las consecuencias más graves ocurren cuando se filtran los datos semiprivados[2] de clientes. En el ataque cibernético a Cencosud, se difundieron hasta 38 GB de datos que incluían este tipo (Monastersky, 2020).

Implicaciones de la información patrimonial

La empresa Cencosud ofrece una tarjeta de crédito propia a los clientes de los 5 países donde opera. Esta característica compromete una mayor cantidad de datos de carácter financiero de cada cliente, por ejemplo, número de tarjeta y movimientos de compra.

La posesión de esta información por terceros facilita la suplantación de identidad del cliente para realizar operaciones no autorizadas, como compras y solicitud de préstamos. Esto último tiene consecuencias muy perjudiciales para la economía del titular de la tarjeta, especialmente si la empresa no se responsabiliza por los daños ocasionados.

[1] Se convierten los datos de un formato legible a uno codificado, solo se pueden leer luego de descifrarlos.
[2] Se trata de información concreta cuyo conocimiento o acceso debe resultar de interés únicamente para el titular y un sector específico de una organización.

Cencosud negó en un principio la filtración masiva de datos (Monastersky, 2020) y no hubo comunicados oficiales que alertaran a sus usuarios para que efectuaran un seguimiento de las compras practicadas en sus tarjetas y denunciaran cualquier situación anormal.

Implicaciones de la información de contacto

Toda organización requiere de una vía de comunicación con sus usuarios para que ambas partes estén en contacto ante cualquier novedad o inconveniente. Para ello, se cuenta con el número de teléfono y una dirección de correo electrónico del cliente. Estos medios tradicionales son aprovechados para realizar diferentes ataques de phishing debido a la dificultad que puede presentar la correcta identificación del emisor (ver Apéndice A1).

Los servicios de correo disponen de filtros para bloquear los correos fraudulentos y con virus informáticos (ver glosario). Sin embargo, los ataques de phishing son cada vez más sofisticados y consiguen burlar dichas barreras. A continuación, se muestran las categorías de organizaciones más afectadas por el uso de estas prácticas de ingeniería social.

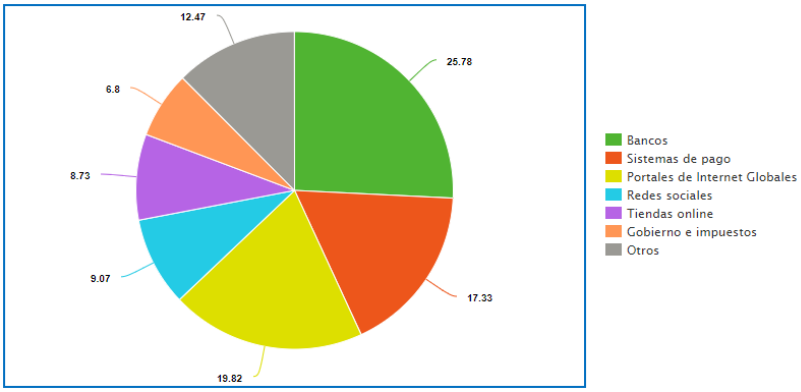

Figura 2. Distribución de organizaciones cuyos usuarios fueron atacados por phishers (Kaspersky, 2019)

Cencosud forma parte de las empresas de sistemas de pago y tiendas online, siendo en su conjunto más del 25%, en función de lo observado en la Figura 2; por lo tanto, los clientes resultan muy perjudicados por la invasión de spam (mensajes falsos) luego de la filtración.

Los mensajes generalmente contienen un enlace web, es decir, un “elemento” donde el usuario puede hacer clic para abrir otro contenido. La página de redirección puede tener un diseño similar al sitio de la empresa, con campos para rellenar datos que permiten la recolección de suficiente información para efectuar una suplantación de identidad del cliente.

Discusión

En resumen, con la información proporcionada en la sección anterior, se distinguen problemas de seguridad prominentes entre la empresa y sus clientes. La falta de acciones por parte de Cencosud para impedir la difusión de los datos tuvo como consecuencia un nivel de exposición alto, muchas personas tienen acceso a los mismos. En adición con información filtrada de otras empresas, se crean nuevos perfiles para realizar ilícitos (Stranieri, 2021).

En los últimos años se ha incrementado el porcentaje de empresas que disponen de una aplicación móvil oficial para diversos sistemas operativos, que garantizan una navegación segura a través de las funciones. Cencosud posee apps para su tarjeta y sus supermercados, sin embargo, no han tenido la recepción adecuada debido a varios fallos reportados.

La implementación de un software completo con el mantenimiento adecuado es una solución objetiva a la problemática. Para evitar el uso de llamadas telefónicas y el uso de correo electrónico, la aplicación puede proveer un sistema de atención al cliente personalizado, un sistema de cobros integrado, un rápido acceso a los comprobantes y un fácil seguimiento de las operaciones en tiempo real, sumado de una interfaz de usuario amigable.

Conclusiones

- Más de un cuarto de los correos fraudulentos usuales están dirigidos a usuarios de organizaciones de la misma categoría que Cencosud.
- El conocimiento de datos patrimoniales, en adición con los datos de identificación, permite la realización de compras y solicitudes bancarias no autorizadas por el titular.
- La inexistencia de un comunicado oficial es una ventaja para los atacantes debido a que los clientes de la empresa no toman los recaudos necesarios para su protección personal.
- Los filtros antispam no son 100% efectivos, entonces la distinción de su veracidad queda en manos del usuario. Si el contenido es creíble, la persona posiblemente accederá a las solicitudes del atacante, resultando realmente perjudicada por el robo de datos.
- La incapacidad de un traspaso definitivo a nuevas tecnologías colabora en cierta medida a la expansión de la ingeniería social por el gran uso de medios tradicionales, cuya principal desventaja es el reconocimiento de la verdadera identidad del emisor.

Bibliografía

- Urrutia, F. D. (6 de julio de 2020). Reporte de ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el Caribe. Organización de los Estados Americanos.
- Wright, C. (8 de abril de 2020). Latin America under threat of cybercrime amid Coronavirus. Disponible en internet en: https://insightcrime.org/news/analysis/threat-cyber-crime-coronavirus. 16 de septiembre de 2021.
- Monastersky, D. (25 de noviembre de 2020). Hackeo a Cencosud: se filtró la información. Disponible en internet en: https://www.iproup.com/innovacion/18582-hackeo-a-cencosud-se-filtro-la-informacion. 18 de septiembre de 2021.
- Azzolín, H. (21 de marzo de 2021). Alertan sobre una nueva modalidad de estafas por correo electrónico. Disponible en internet en: https://lacapitalmdp.com/alertan-sobre-una-nueva-modalidad-de-estafas-por-correo-electronico. 19 de septiembre de 2021.
- Kaspersky Lab (15 de mayo de 2019). Spam y phishing en el primer trimestre de 2019. Disponible en internet en: https://securelist.lat/spam-and-phishing-in-q1-2019/88830. 20 de septiembre de 2021.
- Stranieri, S. (19 de marzo de 2021). Hackeo a Cencosud: malestar de los clientes por estafas. Disponible en internet en: https://www.iproup.com/innovacion/21432-hackeo-a-cencosud-malestar-de-los-clientes-por-estafas. 21 de septiembre de 2021.

Glosario

- **Dato semiprivado:** información concreta cuyo conocimiento o acceso debe resultar de interés únicamente para el titular y un sector específico de una organización.
- **Phishing:** tipo de ataque de ingeniería social cuyo objetivo es engañar a un usuario, transmitiéndole una falsa confianza, para que luego comparta sus datos al atacante. El término deriva de la palabra *"fishing"*, en referencia a *"pescar víctimas"*. A su vez, se divide en 3 tipos: *"phishing tradicional"* (mediante correo electrónico), *"vishing"* (por llamado telefónico) y *"smishing"* (por SMS y mensajería instantánea).
- **Virus informático:** programa de apariencia inofensiva que pueda afectar potencialmente el funcionamiento de una computadora. Para efectuar su ataque, el usuario debe descargar el archivo, instalarlo y ejecutarlo. Luego, el programa puede replicarse e infectar otros archivos.

Apéndice A1: Caso de phishing en Cencosud

El correo electrónico es ampliamente utilizado por las organizaciones para el envío de recibos o notificaciones sobre acciones recientes hacia sus usuarios. Este hecho implica simultáneamente que se trate de una vía de comunicación vulnerable a los ataques de la ingeniería social, en particular, el *phishing tradicional*.

La posesión de información real que comprometa la actividad de los clientes de la empresa permite aumentar la probabilidad de que el receptor del mensaje sea engañado y manipulado para brindar aún más detalles de su información personal.

De hecho, en Argentina esta modalidad de estafa tuvo como victimas a clientes de compras online a Easy, a quienes se les informaba de un supuesto problema y se les solicitaba fotografías de ambas caras del DNI y tarjeta de crédito utilizada (Azzolín, 2021), como se muestra a continuación:

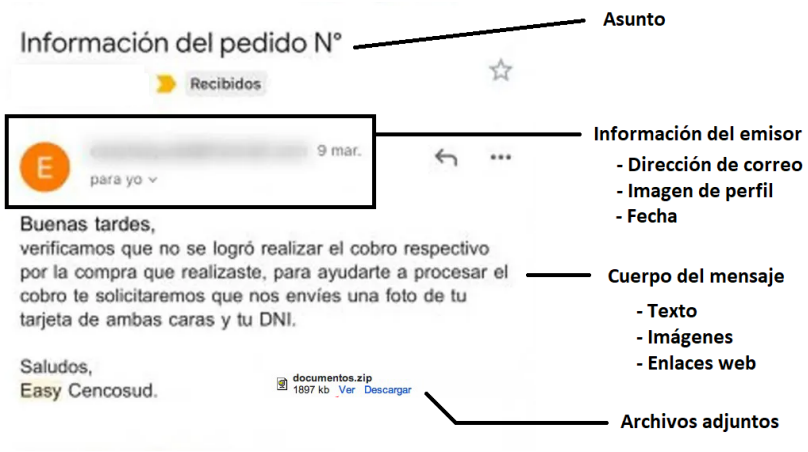

Figura A1: partición de un mensaje fraudulento con robo de identidad de Easy

Como se puede observar en la figura A1, aunque el número de pedido sea correcto, existen características distinguibles frente a un mensaje oficial de la empresa, principalmente en la información del emisor y en el cuerpo de mensaje. En primer lugar, la imagen de perfil y la dirección del emisor no se corresponden con la información pública de la empresa, por ejemplo, el logo corporativo. Por otra parte, respecto al cuerpo de mensaje, la ortografía en el texto y la ausencia de imágenes no brindan una apariencia formal.

Sin embargo, gran parte de la población no se encuentra informada sobre el tema, por ejemplo, los adultos mayores, o por falta de tiempo no presta atención a estos detalles.