Seminario de Redacción de Textos Profesionales

Trabajo Práctico N°4

1. Redactar la sección ***"Introducción"*** detallando los antecedentes del tema a abordar en el informe. Incluir las citas bibliográficas (Autor, Año), algunas de las definiciones escritas en la actividad de la Unidad N°3 y los objetivos del informe que se plantearon en la Unidad N°1.

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 con economías más potentes son los más atractivos para los hackers, ya que tienen capital, gran población y están adoptando las nuevas tecnologías rápidamente, aunque, a la vez, aún están muy por detrás del resto del mundo a la hora de implantar mecanismos de ciberdefensa y políticas de cumplimiento de forma generalizada (Wright, 2020). Un claro ejemplo es la implementación y regularización del uso de facturas electrónicas en reemplazo a las facturas en papel, siendo el correo electrónico el medio ampliamente utilizado para el envío de las mismas, que si bien presenta muchas ventajas también suma nuevos riesgos para los usuarios.

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.

2a. Redactar un *borrador preliminar* sobre el tema en investigación, teniendo en cuenta la organización del diagrama de flujo de la Unidad N°2. Ilustrar con 2 gráficos, con sus correspondientes leyendas. Antes de la redacción, escribir el 1er título del cuerpo del informe.

Usurpación de datos

Las empresas de carácter multinacional, en general, cuentan con una gran base de datos tanto de sus clientes como así también de sus empleados. Al efectuarse un ciberataque existe una gran probabilidad de que los atacantes involucrados logren tener acceso a una parte considerable de dicha información. Según los propósitos de los ciberdelincuentes, la información usurpada 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.

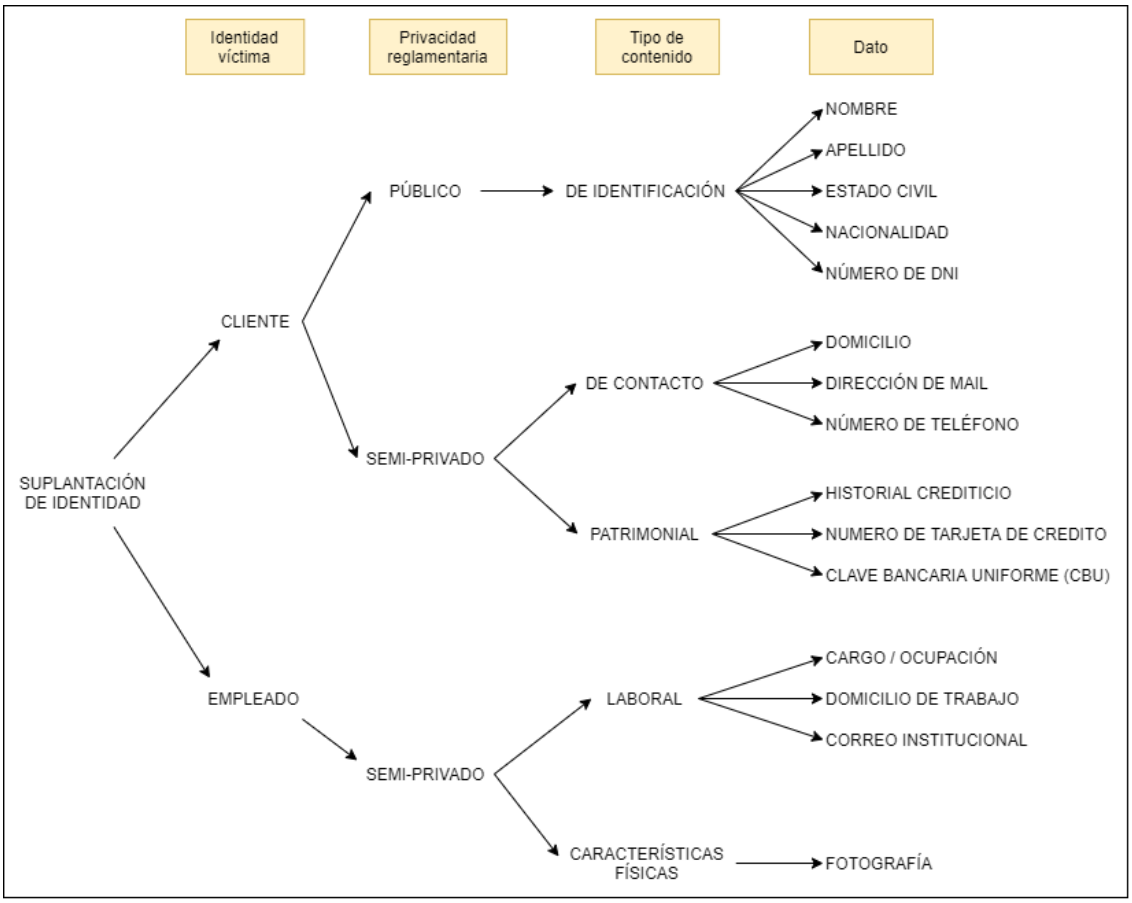

Figura 1. Clasificación de los datos almacenados en una empresa de comercio

[1] Se convierten los datos de un formato legible a uno codificado, solo se pueden leer luego de descifrarlos.

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 otras palabras, la información patrimonial y de contacto. En el ataque cibernético a Cencosud, se difundieron hasta 38 GB de datos que incluyeron dichas categorías (Monastersky, 2020).

Implicaciones de la información patrimonial

La empresa Cencosud ofrece una tarjeta de crédito propia a los clientes de los 5 países latinoamericanos donde opera. Esta característica compromete una mayor cantidad de datos de carácter financiero de cada cliente, por ejemplo, los detalles específicos de la tarjeta y los movimientos de compra que se hayan realizado recientemente.

La posesión de este tipo de información por terceros facilita la suplantación de identidad del cliente al momento de 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.

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.

En general, las empresas de tarjetas de crédito realizan llamados telefónicos para notificar sobre una deuda existente y/o envían un correo electrónico cuando se realiza una compra en línea. Estos medios tradicionales son aprovechados para realizar diferentes ataques de phishing debido a la dificultad que puede presentar la correcta identificación del emisor.

Los servicios de correo más frecuentemente utilizados disponen de filtros para bloquear los correos fraudulentos. Sin embargo, los ataques de phishing son cada vez más sofisticados y consiguen burlar dichas barreras, por ejemplo, mediante direcciones de mail similares a los oficiales de la empresa o la mención de información acertada de una transacción reciente.

[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.

A continuación, se muestran las categorías de organizaciones más afectadas por el uso de estas prácticas de ingeniería social.

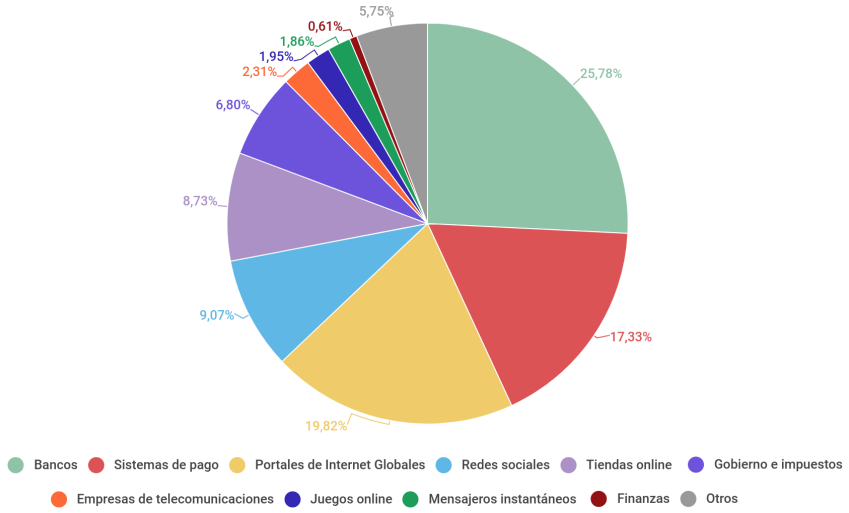

Figura 2. Distribución de organizaciones cuyos usuarios fueron atacados por phishers (Kaspersky, 2019)

Cencosud forma parte de las empresas de sistemas de pago y tiendas online, que representan el 17.33% y 8.73% respectivamente de los casos de phishing, siendo en su conjunto más del 25%, en función de lo observado en la Figura 2. Considerando además la posesión, por parte de los atacantes, de datos concretos sobre movimientos de compra en la empresa, los clientes resultan muy perjudicados por la invasión de spam (mensajes falsos).

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).

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 web de la empresa, con campos para rellenar datos de interés que permiten la recolección de suficiente información para efectuar una suplantación de identidad del cliente.

Implicaciones de la información de empleados

Las organizaciones almacenan datos de identificación y seguimiento de cada una de las personas que pertenecen a la misma. El conocimiento de esta información por parte de terceros permite efectuar la suplantación de identidad de un empleado. Esto es aprovechado en los ciberataques para enviar correo electrónico con archivos adjuntos que contienen virus informáticos (ver glosario) a distintos sectores de la empresa. Si el mismo es puesto en funcionamiento, de forma accidental, se inicia así un nuevo ciclo de usurpación de datos.

2b. Redactar la sección de ***Discusión*** donde se explique el significado de la información y se exponga a la audiencia una propia visión crítica sobre el tema desarrollado.

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).

A partir de los avances tecnológicos cada vez más dominantes en la sociedad, en los últimos años se ha incrementado el porcentaje de empresas que disponen de una aplicación móvil oficial para diversos sistemas operativos. Mediante el uso de la misma se puede garantizar un entorno de navegación seguro por el sitio de la organización, incluyendo las funcionalidades que se consideran necesarias para los usuarios.

Cencosud posee aplicaciones para su tarjeta y sus supermercados, sin embargo, no han tenido la recepción adecuada debido a varios fallos reportados. Por ejemplo, los movimientos de compra y los resúmenes de cuenta se muestran desactualizados, y por dicho motivo algunos usuarios optan por la desinstalación de la app y regreso al correo electrónico.

La implementación de un software completo con el mantenimiento adecuado es una solución objetiva a la problemática. Para disminuir considerablemente las 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.

3. Redactar las ***"Conclusiones"*** de su informe destacando los hallazgos más importantes del tema abordado. Las mismas deben estar en concordancia con los objetivos planteados.

Conclusiones

- Más de un cuarto de los correos fraudulentos usuales están dirigidos a usuarios de organizaciones de la misma categoría que Cencosud, intentando suplantar la identidad de la misma para transmitir una falsa confianza a sus clientes.
- El conocimiento de datos de identificación, como el nombre, apellido y DNI, en adición con los datos patrimoniales, como el número de tarjeta de crédito, permite la realización de compras y solicitudes bancarias no autorizadas por el titular.
- Cencosud no ha demostrado una preocupación relevante por proteger la integridad de los datos de las personas. Aunque el ocultamiento de la situación puede mantener la imagen empresarial en un principio, la misma se ve afectada por ataques futuros a sus clientes usando la información filtrada, como sucedió con el spam de Easy en marzo de 2021.
- 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, como la modificación de sus claves o la baja inmediata de las cuentas afectadas.
- Los filtros antispam no siempre son capaces de identificar aquellos mensajes que no corresponden a la dirección oficial de la empresa, 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, como el uso completo de aplicaciones oficiales, colabora en cierta medida a la expansión de la ingeniería social por el gran uso de medios tradicionales para la comunicación empresa – cliente, cuya principal desventaja es el reconocimiento de la verdadera identidad del emisor.

4. En base a las citas mencionadas en la Introducción y a la búsqueda bibliográfica realizada, confeccionar una lista de las fuentes consultadas. Seguir el formato de escritura de la ***"Bibliografía"***, ya que luego formará parte de esa sección.

Bibliografía

- Urrutia, F. D. (6 de julio de 2020). Reporte de ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe. Banco Interamericano de Desarrollo; Organización de los Estados Americanos. p 12.
- 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. [@identidadrobada]. (24 de noviembre de 2020). *Finalmente difundieron la información comprometida de Cencosud (38.8 GB)*. Twitter. Disponible en internet en: https://twitter.com/identidadrobada/status/1331354457678942211
- 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.