Evidencia 4 Ética y Deontología

Alumnos integrantes del grupo:

- Cortabarria, Joaquin.
- Aliendro, Javier.

Carrera: TS Telecomunicaciones 2023

Buscar y leer sobre algunos casos recientes de violaciones de seguridad que ocurrieron en Argentina

Las violaciones de seguridad se producen cuando individuos o programas intentan acceder de manera no autorizada a datos, aplicaciones, servicios o dispositivos. Los atacantes, ya sean infiltrados o no, buscan obtener información que les pueda proporcionar beneficios financieros u otras ventajas.

Cuadro comparativo

A continuación, un cuadro comparativo sobre la información encontrada de ataques recientes realizados en nuestro país.

Fecha incidente	Organización afectada	cantidad de víctimas	que fue tomado	tipo de ataque	Link
01/02/2023	La Segunda Seguros	todos los afiliados	información sensible de personas físicas	ransomware	ver
01/06/2023	Usuarios en general	mas de 20	identidad digital	SIM Swapping	ver
Mayo/2023	Policía de Córdoba	no especificado	accesos al servidor de correo electrónico	no confirmado, posible phishing	ver
en proceso ahora	Comisión Nacional de Valores	todos los usuarios del mercado de capitales	1,5 terabytes de documentos y bases de datos	ransomware	ver

Ataque a compañía La Segunda Seguros

Link:
https://www.ambito.com/informacion-general/ciberseguridad-una-aseguradora-argentina-sufrio-un-impotante-ataque-hackers-rusos-n5665636

El hecho sucedió en los primeros días de febrero cuando se desarrollo un incidente de violación de seguridad informática que involucra a una importante compañía de seguros. El grupo de hackers conocido como LockBit logró obtener información confidencial de los clientes de la compañía después de haber comprometido sus sistemas mediante un ataque de ransomware. En este tipo de ataque, los archivos y datos de la empresa son cifrados y los hackers exigen un rescate para desbloquearlos.
En respuesta al ataque, la compañía de seguros decidió no pagar el rescate exigido, alegando una postura firme en contra de las solicitudes ilegales. Sin embargo, los hackers cumplieron su amenaza y, el 3 de marzo, expusieron los datos en línea a través de un método conocido como Snap2HTML.
Los datos expuestos incluyen información personal sensible de los clientes, poniendo en riesgo la privacidad y la seguridad de las personas afectadas.

Allanamientos por SIM Swapping en Córdoba

Link:
https://www.cba24n.com.ar/cordoba/allanamientos-y-detenidos-por-sim-swapping-en-cordoba--que-es-y-como-prevenir-estafas_a64788340fe9094ac599135ed

El artículo informa sobre el allanamiento y la detención de tres hombres en la provincia de Córdoba por su participación en el delito de duplicación de chips de teléfono, utilizando la modalidad conocida como "SIM Swapping". La investigación se inició en diciembre del año 2022, y durante los allanamientos realizados en diferentes barrios, se confiscaron diversos elementos relacionados con los hechos, como 20 teléfonos celulares, tarjetas de débito y crédito, así como una suma considerable de dinero.
El "SIM Swapping" consiste en duplicar la tarjeta SIM de los usuarios de teléfonos celulares con el propósito de robar contraseñas de diferentes plataformas digitales, como redes sociales, billeteras digitales y correos electrónicos.
La Policía proporcionó una serie de recomendaciones para prevenir convertirse en víctima de este tipo de delitos. Estas incluyen el uso de contraseñas adicionales o autenticación de dos factores, evitar compartir información personal en línea, no proporcionar datos personales a través de llamadas telefónicas no confiables, no divulgar códigos PIN o contraseñas a nadie, utilizar contraseñas seguras en lugar de fechas o números fáciles de adivinar, solicitar a la empresa de telefonía celular que refuerce la seguridad de las operaciones realizadas en nuestro nombre y evitar el uso de plataformas bancarias que validen contraseñas a través de SMS.

Venta de accesos a correos electrónico de la Policía de Córdoba

Link:
https://www.cba24n.com.ar/sucesos/ciberseguridad--denuncian-la-venta-de-accesos-a-correos-electronico-de-la-policia-de-cordoba_a64637cb70f5cce2f64dc2625

Se expone un incidente de seguridad cibernética en el que se están vendiendo accesos al servidor de correo electrónico de la Policía de Córdoba y se han filtrado credenciales de otras instituciones. Esto plantea serias preocupaciones éticas en términos de privacidad, seguridad y responsabilidad institucional
Según un analista de seguridad informática, un usuario de Internet está vendiendo accesos al servidor de correo electrónico de la Policía de Córdoba, así como una lista de credenciales de diversas instituciones, incluyendo el Banco Central, municipios, INTA, INDEC y otras 500 entidades.
Existiria aqui una clara violación de la privacidad y la seguridad de los datos de la Policía de Córdoba y las demás instituciones involucradas. El acceso no autorizado a cuentas de correo electrónico y la posibilidad de crear cuentas falsas con dominio oficial podrían permitir la suplantación de identidad para la realización de actividades ilegales.
La Policía de Córdoba debe tomar medidas para investigar cómo se produjo esta filtración y cómo se puede evitar en el futuro. También se destaca la importancia de la seguridad cibernética y la actualización de los sistemas para proteger la información sensible. En cuanto a la recomendación de seguridad planteada por el analista, se destaca la importancia de la conciencia y el sentido común al tratar con correos electrónicos sospechosos o que soliciten pagos o transferencias de dinero. Esto refuerza la necesidad de que los usuarios sean conscientes de los posibles riesgos y estén atentos a posibles intentos de estafa o phishing.}

Hackearon la CNV

Link:
https://www.cadena3.com/noticia/internacionales/hackearon-la-cnv-y-exigen-us500000-para-no-revelar-documentos-del-organismo_360515

Actualmente la Comisión Nacional de Valores (CNV) ha sido hackeada por el grupo de ciberataque Medusa en una operación de ransomware. El grupo exige un rescate de 500.000 dólares para evitar la filtración de documentos y bases de datos. Se ha comprometido una gran cantidad de información y Medusa amenaza con publicarla si no se paga el rescate. La CNV se enfrenta a un dilema ético, ya que debe proteger la información y mantener la integridad de los mercados financieros, pero ceder al chantaje podría tener consecuencias negativas a largo plazo.