Universidad de Buenos Aires

Facultad de Ciencias Económicas,
Ciencias Exactas y Naturales e Ingeniería

Carrera de Especialización en
SEGURIDAD INFORMÁTICA

TRABAJO FINAL

Título:

"**Descripción y análisis de Brechas de Seguridad que han sufrido empresas privadas en los últimos 5 años**"

Autor: Lic. Diego Hernán VITUZZI
Tutor: Mg. Darío RIZZO

Mayo 2022
- Cohorte 2021 –

Declaración Jurada del origen de los contenidos

Por medio de la presente, el autor manifiesta conocer y aceptar el “Reglamento de Trabajos Finales” vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

FIRMADO

……
Diego Hernán VITUZZI

DNI 24.591.042

Resumen

En el ámbito de la ciberseguridad la fuga de información se ha convertido en un aspecto central, posicionándose cada vez más como uno de los mayores problemas que deben afrontar las empresas, ya que de ello dependerá la continuidad de sus operaciones, es decir que dependiendo del tipo de compromiso que afecte a su información, será el impacto que le ocasione al negocio.

Existe un interés creciente en los últimos 5 años en lo que respecta a la protección del activo más valioso de las organizaciones, y que es la manera de como protegen su infraestructura tecnológica de cualquier intrusión que pueda afectar a la confidencialidad, integridad y disponibilidad de su información, sea esta en formato digital, impresa, tangible o intangible.

Las amenazas externas avanzan y evolucionan constantemente junto a las tecnologías, transformándose en un gran desafío para los profesionales de la Ciberseguridad para mantenerse formados y actualizados de manera constante.

Durante el año 2020 el costo de los ciberataques rompió los récords en todo el mundo, se estima que las pérdidas económicas a alcanzado a superar el trillón de dólares, contabilizando un promedio de U$S 3.9 millones de dólares por cada brecha de seguridad.

El presente trabajo consiste básicamente en describir y analizar el impacto que han sufrido las empresas producto de una fuga de información. De los 8 casos planteados se procederá a ordenarlos de acuerdo con su criticidad, sea esta por su impacto económico o reputacional, entre otros.

Se describirán las amenazas cibernéticas más frecuentes que ponen en jaque a las organizaciones y como deben gestionar una fuga de información. Para finalizar se realizará una conclusión en la cual se expondrán desde mi punto de vista que se debe hacer para que las brechas de seguridad no sucedan o al menos generen el menor impacto posible.

Contenido

Resumen **2**
1. Introducción **5**
2. Objetivo y Alcance **6**
3. Casos analizados de acuerdo con su criticidad **7**
3.1 Caso Equifax **8**
Descripción 8
Análisis del hecho: 9
Impacto 11
3.2 Caso British Airways **12**
Descripción 12
Análisis del hecho 12
Impacto 16
3.3 Caso Yahoo! **18**
Descripción 18
Análisis del hecho 18
Impacto 20
3.4 Caso Hotel Marriot **21**
Descripción 21
Análisis del Hecho 21
Impacto 23
3.5 Caso Facebook **24**
Descripción 24
Análisis del Hecho 24
Impacto 28
3.6 Caso Disney Plus **29**
Descripción 29
Análisis del hecho 30
Impacto 33
3.7 Caso Cencosud **34**
Descripción 34
Análisis del hecho 34
Impacto 39
3.8 Caso Mercado pago **40**
Descripción 40
Análisis del hecho 41

Impacto 43
4. Criterio de ordenamiento de acuerdo con la criticidad del hecho 43
5. Tipos de amenazas Cibernéticas 45
Amenaza 1: Phishing 45
Amenaza 3: Estafas de PDF 46
Amenaza 4: *Malware* y *Ransomware* 46
Amenaza 5: Exposición de la Base de Datos 47
Amenaza 6: Denegación de Servicio (DoS) 47
6. Como mitigar una fuga de información 48
7. Conclusión General 51
8. Bibliografía 55

1. Introducción

En los últimos 5 años se ha notado una tendencia en alza de las brechas de seguridad que afectan a las empresas privadas u Organismos Gubernamentales de todo el mundo, cualquiera sea su actividad y tamaño, y que han puesto en jaque a la seguridad de uno de sus activos más valiosos, la información.

El proceso de transformación digital como lo es la Big Data, la automatización de marketing, aprendizaje automático, entre otros, se debió mayormente al crecimiento y avance tecnológico de los últimos tiempos, por el cual las empresas se han reinventado buscando nuevas formas de reducir sus costos, optimizar sus procesos y mejorar los servicios que brindan a sus clientes. Por tal motivo esta transformación no es una alternativa, sino una necesidad importante para que las empresas sobrevivan y se vuelvan más competitivas en relación con sus competidores. (Médico, 2020).

Además, no solo se debe enfocar en la transformación digital, sino también en las organizaciones criminales, ya que estas actúan sin límite de fronteras, poseen todos los recursos y tiempo necesario para lograr su cometido, haciendo que las empresas vean como sus datos se encuentran expuestos en la internet profunda “Dark Web” y puestas a la venta del mejor postor, por ende, esto ha provocado el crecimiento de los delitos.

Uno de los vectores de ataques más utilizados es mediante el empleo de técnicas de ingeniería social, a través del cual los atacantes han encontrado una puerta de acceso a los datos de las empresas por intermedio de sus empleados.

Desde las áreas de ciberseguridad existe preocupación sobre la

sofisticación que emplean las organizaciones criminales para lanzar sus ataques empleando *exploit* con infección de *malware*, que muchas veces no son detectados por las herramientas de seguridad con las que cuentan.

La seguridad no es absoluta, pero lo que sí sabemos es que debemos aplicar seguridad en profundidad, con el fin de reducir los riesgos a un valor aceptable para la empresa. De esta forma se evitará, dentro de lo posible, dejar expuesta información de la empresa o en el peor de los casos información sensible de sus clientes, como ser, datos personales, datos de tarjetas de créditos, entre otros, quedando vulnerables y blanco fácil para que los ciberdelincuentes lancen y empleen distintas técnicas de ingeniería social a partir de los datos robados.

2. Objetivo y Alcance

Este documento tiene como objetivo principal comprender como y porqué las empresas sufren ataques que provocan la filtración de sus datos.

Como objetivos específicos, se tomará en cuenta los siguientes factores:

- Analizar casos de empresas privadas que sufrieron ataques entre 2016-2022.
- Elaborar un índice de criticidad basado en el efecto que tuvo el incidente.
- Identificar cómo se produjo la fuga de información.
- Describir los casos estudiados según el índice de criticidad.
- Analizar qué elementos deben tener en cuenta las empresas para evitar fuga de información según lo detectado en el índice de criticidad.

Es importante tener en cuenta y entender cuáles son las técnicas y

amenazas cibernéticas recientes, es decir, las más empleadas por los atacantes para lograr su cometido, es por eso por lo que se dedicará un apartado para describir cada una de ellas.

Para finalizar se desarrollará una conclusión general, explicando la importancia del por qué las empresas deben contar con un Plan de Gestión de Seguridad de la Información para evitar la fuga sus datos, que no solo se enfoque en la implementación de tecnologías de vanguardia, sino también destacar la importancia que tiene la concientización y/o capacitación de los empleados en materia de ciberseguridad.

3. Casos analizados de acuerdo con su criticidad

A continuación, se describen las ocho empresas que se han tomado como caso de estudio para entender la problemática que sufrieron al ocasionarse la filtración de sus datos, estas son:

1. Equifax
2. British Airways
3. Yahoo!
4. Hotel Marriot
5. Facebook
6. Disney Plus
7. Cencosud
8. Mercado Pago

3.1 Caso Equifax

Descripción

La compañía Equifax es una agencia multinacional de los Estados Unidos de Norteamérica que se dedica a generar informes de crédito al consumo. Es una de las tres agencias más grandes a nivel mundial, junto con Experian y TransUnion, conocidas en conjunto como los “Tres Grandes”. La empresa recopila información de más de 800 millones de consumidores individuales y más de 88 millones de empresas en todo el mundo.

Con sede en la ciudad de Georgia Atlanta, Equifax opera con inversiones es 24 países de América, Europa y Asia. Cuenta con un plantel de más de 10.000 empleados en todo el mundo y tiene un ingreso anual de más de 3100 millones de dólares. (EQUIFAX, 2022).

Imagen obtenida del sitio web de Equifax
Fuente: https://www.soluciones.equifax.com.ar/acerca-de-equifax/perfil-de-la-empresa

Sucursales:

- Estados Unidos
- Arabia Saudita
- Argentina
- Australia
- Brasil
- Camboya
- Canadá
- Chile
- Costa Rica
- Ecuador
- El Salvador
- España
- Honduras
- India
- Malaysia
- México
- Nueva Zelanda
- Paraguay
- Perú
- Portugal
- Reino Unido
- República Dominicana
- Rusia
- Singapur
- Uruguay

Imagen obtenida del sitio web de Equifax
Fuente: https://www.soluciones.equifax.com.ar/acerca-de-equifax/perfil-de-la-empresa

Análisis del hecho:

Durante el año 2017, la compañía Equifax sufrió uno de los ataques cibernéticos más relevantes de la época. Este incidente le ocasionó el robo de información confidencial de aproximadamente 143 millones de usuarios, en su mayoría residentes de los Estados Unidos, Canadá y del Reino Unido.

Como resultado de la investigación, se llegó a la conclusión que la intrusión se llevó a cabo por la explotación de una conocida vulnerabilidad de la aplicación web para abrir una *ShellWeb* que corría en un servidor (Apache Server) y que, por falta de actualización y configuración deficiente, fue aprovechada por los atacantes durante 3 meses. Para ello lograron conseguir el acceso a distintas bases de datos de la compañía y de esta forma robar la información almacenada. (ABC.ES, 2017).

La gravedad de este hecho fue la filtración del tipo de información que maneja la compañía respecto de sus clientes, como ser el historial crediticio, nombres completos, direcciones, números de teléfonos, números de tarjetas de créditos, fecha de nacimiento, números de seguridad social y hasta licencias de conducir.

De acuerdo con las fuentes analizadas, los directivos de la compañía admitieron que se cometieron muchos errores, entre ellos tener una lista desactualizada de los administradores de los sistemas, ya que la empresa hizo circular un aviso para instalar un parche de seguridad que corregía la vulnerabilidad detectada en el aplicativo del software y sus servidores, pero el mensaje nunca llegó a todos los referentes técnicos. Este error es típico de la falta de comunicación entre las áreas involucradas.

A raíz del incidente de seguridad sufrido por la empresa, el Departamento de Justicia de los EE. UU anunció en su momento la acusación de cuatro miembros del Ejército Popular de Liberación de China (PLA por su acrónimo en inglés) por su presunta participación del hackeo a las bases de datos de la firma Equifax. (FBI.GOV, 2020).

Los cuatro imputados -Wang Qian, Xu Ke, Liu Lei y We Zhiyong

Imagen obtenida del sitio web: www.fbi.gov

Cargos que se le imputa: *conspiración para cometer fraude informático, conspiración para cometer espionaje económico y conspiración para cometer fraude electrónico.*

La empresa nunca se percató que los intrusos se interesaron en sus bases de datos y analizaron todas las variables posibles para obtener la información durante más de 6 semanas. Para lograr el objetivo, los atacantes

explotaron la vulnerabilidad antes descripta y una vez dentro de la red, los hackers pudieron descargar y filtrar datos de Equifax a computadoras fuera de los Estados Unidos, según lo reportaron autoridades responsables de la investigación. (INFOBAE, 2020).

Impacto

Como consecuencia de la fuga de información, producto del ciberataque, la compañía Equifax pagó una multa de u$s 700 millones de dólares. Acuerdo que se hizo con el Gobierno de los Estados Unidos, de los cuales 425 millones se destinaron mayormente para las indemnizaciones a los clientes afectados, es decir, con el fin de ofrecerles servicios gratuitos de control de crédito y de restauración de su identidad, además de entregarles dinero por su tiempo o reembolso de ciertos servicios. Sin embargo, debido a que tantas personas habían efectuado reclamos, los funcionarios informaron que algunos consumidores obtendrían menos que los montos elegibles debido a lo establecido por el fondo común del acuerdo.

Podemos ver la gravedad del caso ya que la información filtrada correspondía a datos sensibles, como los informes crediticios y los números de la seguridad social, y números de tarjetas de crédito. Por ello, la empresa ofreció a los clientes afectados un importe de **u$s 125** hasta **u$s 20.000** de acuerdo a la gravedad de los casos, como ser para afrontar los gastos de honorario de abogados y contadores y cualquier gasto que sea devengado en sus tarjetas de crédito que sea desconocido por los usuarios.

En este caso puntual, el impacto económico que sufrió la compañía fue uno de los más altos en los últimos tiempos, ya sea por el pago de la multa, el resarcimiento económico a sus clientes por los perjuicios ocasionados, sumado a la mala reputación de la empresa y desconfianza de sus clientes.

La compañía a raíz del incidente tuvo que habilitar oportunamente un portal web para que sus clientes puedan verificar si sus cuentas habían sido comprometidas.

3.2 Caso British Airways

Descripción

La compañía British Airways (BA) es una aerolínea de bandera del Reino Unido. La misma tiene su sede en la localidad de Waterside (Inglaterra), cerca de su principal base de operaciones aéreas en el aeropuerto de Londres-Heathrow.

Es una empresa que transporta aproximadamente 40 millones de pasajeros por año, entre los vuelos de cabotaje e internacionales que realiza. Sus ganancias llegaron a alcanzar los 360 millones de dólares anuales.

En el año 2010 la compañía se fusionó con la empresa Iberia de nacionalidad española. Es una empresa que tiene una antigüedad de 100 años de servicio y cuenta con más de 30.000 empleados en todo el mundo.

Análisis del hecho

La compañía British Airways sufrió una fuga de información durante el mes de septiembre del año 2018. La misma admitió que dicho incidente de seguridad se debió a un ataque cibernético que comprometió datos de sus clientes e información de pago de al menos unos 380.000 usuarios de la plataforma web que se encuentran registrados en el portal de la empresa para efectuar las reservas y/o compra de los pasajes aéreos.

Según se pudo comprobar en la investigación, el ataque se originó

por una mala configuración del código del sitio web que emplea el sistema magneto para efectuar los pagos de manera online a través de su página o mediante el uso de aplicativos móviles.

El ataque se lo atribuyen a una Organización criminal denominada Magecart que son grupos de ciberdelincuentes que se interesan por los sistemas de pago online que emplean el sistema magneto para robar los datos de las tarjetas de crédito y/o débito que utilizan los clientes a través del empleo de aplicaciones de terceros.

Con el avance de la investigación se logró determinar el rastreo de las operaciones detectando un script con una versión modificada perteneciente a la biblioteca Modernizr JavaScript 2.6.2, el cual fue cargado de manera malintencionada mediante una técnica de inyección XSS en el apartado de información de reclamo de equipaje en el sitio web oficial de la Compañía British Airways.

A continuación de ilustra con una captura de pantalla el script modificado que se empleó para realizar el robo de los datos:

Imagen obtenida del sitio web Riskiq.com
Fuente: https://www.riskiq.com/blog/labs/magecart-british-airways-breach/

El cambio que se ha detectado fue en la parte inferior del script original, una técnica que a menudo se observa cuando los atacantes modifican los archivos de *JavaScript* para no romper su la funcionalidad del aplicativo web. Esa modificación despertó las sospechas de los analistas como se puede observar en la siguiente imagen:

La etiqueta de script sospechosa agregada por el grupo Magecart

Imagen obtenida del sitio web Riskiq.com
Fuente: https://www.riskiq.com/blog/labs/magecart-british-airways-breach/

Se encontró más evidencia en los encabezados del servidor web que fueron enviados, ya que cuando estos se envían lo hacen con la siguiente información: “Ultima modificación” que indica la última vez que se modificó un contenido estático. La versión limpia del script Modernizr tenía una marca de tiempo de diciembre del 2012, según se observa en la siguiente imagen:

Versión limpia del script

Imagen obtenida del sitio web Riskiq.com
Fuente: https://www.riskiq.com/blog/labs/magecart-british-airways-breach/

En la versión modificada Modernizr, se puede observar que la marca de tiempo difiere de la del script original, es decir fecha 18 de diciembre del 2012, respecto a la versión comprometida que figura como última modificación del script (21 de agosto del año 2018). De acuerdo con lo informado por la compañía afectada, las denuncias de sus clientes (Víctimas) fueron posteriores a dicha fecha.

Marca de tiempo de cuando comenzó la fuga de información

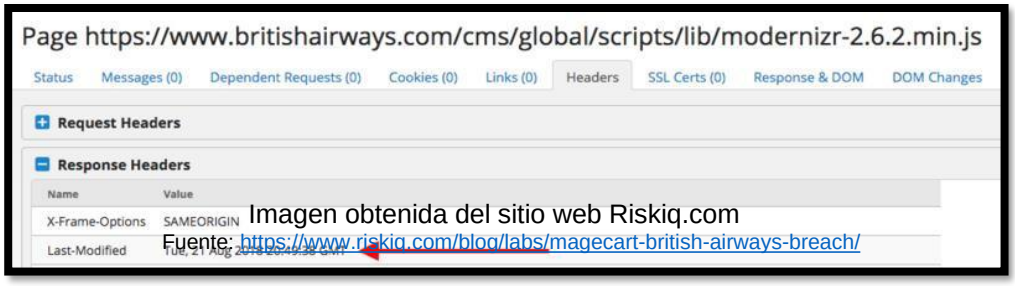


Imagen obtenida del sitio web Riskiq.com
Fuente: https://www.riskiq.com/blog/labs/magecart-british-airways-breach/

A continuación, se describe como con tan simple 22 líneas de código, los atacantes lograron concretar el grave incidente de seguridad que comprometiera los datos sensibles de las tarjetas de crédito y datos personales de los clientes de la empresa British Airways.

Script sencillo pero efectivo

```
window.onload = function() {
    jQuery("#submitButton").bind("mouseup touchend", function(a) {
        var
            n = {};
        jQuery("#paymentForm").serializeArray().map(function(a) {
            n[a.name] = a.value
        });
        var e = document.getElementById("personPaying").innerHTML;
        n.person = e;
        var
            t = JSON.stringify(n);
        setTimeout(function() {
            jQuery.ajax({
                type: "POST",
                async: !0,
                url: "https://baways.com/gateway/app/dataprocessing/api/",
                data: t,
                dataType: "application/json"
            })
        }, 500)
    })
};
```

Imagen obtenida del sitio web Riskiq.com
Fuente: https://www.riskiq.com/blog/labs/magecart-british-airways-breach/

Impacto

Como consecuencia del ciberataque la compañía debió afrontar una multa de 205 millones de euros por el robo de los datos sensibles de más de 380 mil clientes que involucró datos de sus tarjetas de crédito y/o débito.

La multa fue interpuesta por el Órgano responsable de la Protección de datos personales, sancionado a la empresa por no contar con las medidas de seguridad suficientes para evitar este tipo de robo de información evidenciando claramente la pérdida de confidencialidad de la información y la integridad de sus sistemas informáticos.

Con este tipo de incidente de seguridad sumado a la multa que debió afrontar la compañía, le ocasionó a la empresa un impacto negativo, no solo por la sanción económica, sino también por la mala reputación hacia sus actuales o futuros clientes.

El impacto económico tuvo repercusión en el 1,5 % del ingreso total de las operaciones globales del año 2018. Lo destacable es que la sanción aplicada sufrió un atenuante dado que la compañía contaba con una serie de implementaciones de seguridad, sino la multa hubiese sido más severa cuanto ocurre este tipo de incidentes. (KLIJNSMA, 2018).

Cuando suceden estas brechas de seguridad, los organismos responsables de la protección de datos personales velan porque las empresas cumplan estrictamente con la privacidad de sus clientes ya sea en sus datos personales, sensibles y/o financieros.

Para este tipo de protección del e-commerce las empresas que ofrecen servicios de pago a través de sus sitios web, deben respetar lo que establecen las normas de seguridad de los datos del sector de Tarjetas de

Pago (PCI DSS*) "Payment Card Industry Data Security Standard".*

PCI DSS es un estándar exclusivo de seguridad de la información administrado por el consejo de Estándares de Seguridad de PCI, quien fuera fundado por American Express, Discover Financial Services, JBC International, MasterCard Worldwide y Visa Inc. que ayuda a reducir el fraude y las filtraciones de datos dentro de todo el ecosistema de pagos. Se aplica a toda organización que acepte o procese tarjetas de crédito y/o débito. (ACOSTA, s.f.).

Otro aspecto para destacar en la importancia de que los desarrolladores de los sitios web cumplan con las recomendaciones que establece el Proyecto OWASP por sus siglas en inglés (*Open Web Application Security Project*) para las buenas prácticas en la implementación y configuración de los sitios web.

OWASP TOP 10 (2017-2021)

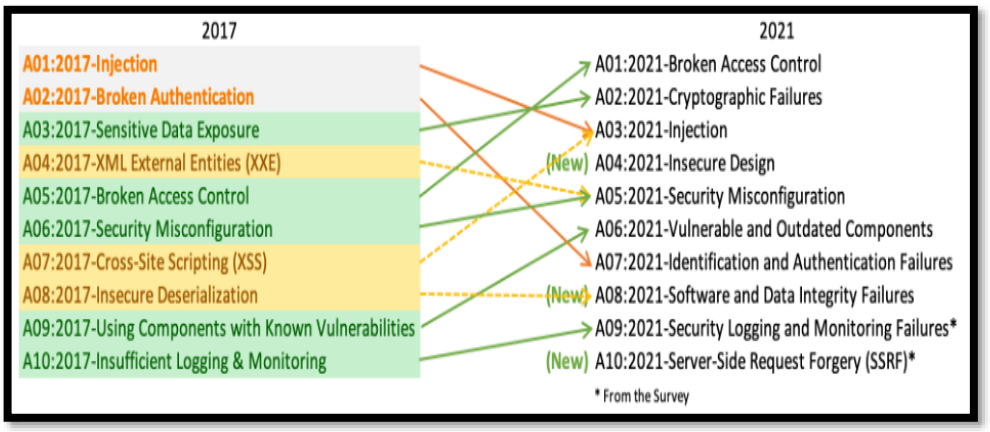


Imagen obtenida del sitio web OWASP.ORG

Como se observa en la imagen anterior, para este caso analizado se debería haber tomado en cuenta lo establecido en el apartado A09-2017 *Using Components with Know Vulnerabilidades*, es decir, lo que significa

que, para la implementación del script para el empleo de las transacciones comerciales, utilizaron componentes de terceros con vulnerabilidades conocidas.

3.3 Caso Yahoo!

Descripción

Yahoo es una empresa de medios de comunicación radicada en los Estados Unidos, brinda sus servicios a través de plataformas web, posee un portal de internet, un directorio web y varios servicios asociados, como el conocido correo electrónico entre otros. La compañía fue fundada en el año 1994 por dos estudiantes de posgrado de la Universidad de Stanford, Jerry Yang y David Filo.

El buscador web de Yahoo, el sitio de noticias y el servicio de correo fueron los medios de comunicación más utilizados y leídos, con más de 7 millones de visitas mensuales en ese entonces, calificándose como el 6° sitio web más consultado a nivel mundial. Actualmente es capital de la empresa Verizon, ya que fue adquirido en año 2016. En el año 2017 Verizon adquirió la mayor parte del negocio de internet de Yahoo por U$S 4.48 mil millones de dólares excluyendo sus participaciones en Alibaba Group y Yahoo Japan que fueron transferidos a la compañía sucesora de Yahoo, Altaba. (Wikipedia, s.f.).

Análisis del hecho

En el año 2013 la firma Yahoo sufrió una fuga de información que afectó a 500 millones de cuentas de correos y durante en el año 2014 reconoció haber tenido otro incidente de seguridad similar.

Cuando la firma fue adquirida por la empresa Verizon en el año 2016,

se dio a conocer que el total de cuentas comprometidas habría sido un poco más de 3.000 millones, por el cual se realizó una investigación de manera conjunta con FBI, a través de la cual se pudo determinar que los intrusos tuvieron acceso al código de propiedad, lo que permitió en acceso a la totalidad de cuentas de usuarios sin la necesidad de ingresar una sola contraseña.

Mayormente estos incidentes de seguridad ocurren vulnerando el eslabón más débil, los empleados, siendo esta una puerta de acceso a las infraestructuras tecnológicas de las empresas, donde las organizaciones cibercriminales logran su cometido.

De acuerdo a la investigación efectuada, se logró determinar que el acceso fue obtenido a través de una técnica de ingeniería social del tipo phishing, es decir, a través de la recepción de un correo malicioso en la bandeja de entrada del correo de un empleado, que por desconocimiento o falta de formación hizo clic en un enlace que lo redireccionó a un sitio web falso donde los atacantes lograron obtener credenciales de acceso a la base de datos de usuarios y la herramienta de gestión de cuentas.

Además, y con el avance de la investigación se logró establecer que los atacantes lograron instalar una puerta trasera para mantener el acceso a los servidores, robando las bases de datos y transfiriéndolos a servidores fuera de la organización. Por la metodología del ataque y código malicioso empleado pudieron determinar que la organización cibercriminal era de origen ruso.

El cuestionamiento que se le formula a la compañía Yahoo, es que existía un documento que en el mes de abril del año 2017 se le había enviado al ente regulador, a través del cual se admitió el incidente sufrido, es decir que el equipo de seguridad supo de su existencia desde un principio, por

haber informado a su servicio jurídico y a los altos cargos de la compañía de que “un acto patrocinado por un Estado” había accedido a datos de ciertas cuentas.

En ese documento, el comité de investigación indicaba que el equipo jurídico de la compañía disponía de información suficiente para justificar una investigación sustancial durante el año 2014, y concluyó que no se examinó suficientemente el “*hackeo*”, como así tampoco fue aconsejada debidamente sobre los riesgos comerciales y legales que podía provocar el incidente de seguridad.

Impacto

Como resultado de la fuga de información se vieron comprometidos datos sensibles como ser las direcciones de correo electrónico y las cuentas de recuperación, números de teléfonos, fechas de nacimiento y en algunos casos las preguntas de seguridad de ciertas personas.

Para la empresa el impacto desde mi punto de vista fue de alta importancia, ya que más allá de la cantidad de cuentas o información filtrada, la compañía tuvo que salir a comunicar a todos sus usuarios que realicen de manera urgente el cambio de contraseña e invaliden las preguntas de seguridad, tanto para las cuentas bajo el dominio “@yahoo.com” como para cualquier otro servicio que posean vinculado o empleen la misma contraseña, recomendando además de la habilitación de un doble factor de autenticación.

El impacto que sufrió la compañía por esta fuga de información fue negativo, afectando su reputación, su economía y parte de sus acciones, ya que por esta situación la empresa fue vendida por 350 millones de dólares en lugar de los 4.480 millones de dólares que cotizaba antes del incidente

de seguridad.

La sanción impuesta por el Organismo responsable de la protección de datos personales fue alrededor de 35 millones de dólares. (LAINFORMACION.COM, s.f.)

3.4 Caso Hotel Marriot

Descripción

La empresa Marriot Internacional es una cadena hotelera que fue fundada en el año 1993. En el año 1995 pasó a formar parte del capital Ritz-Carlton con un 49% del mismo, adquiriendo casi su totalidad en el año 1998.

Durante el año 2002 al 2003 la compañía sufrió una importante restructuración, y en el año 2015 efectuó la compra de la cadena Starwood por un monto total de más de 12.000 millones de dólares.

En la actualidad la cadena cuenta con 5.700 hoteles alrededor del mundo, con 1.1 millones de habitaciones, por lo que se convierte en la cadena hotelera más grande con presencia en más de 110 países.

Análisis del Hecho

En el mes de febrero del año 2020 la cadena hotelera dio a conocer públicamente que había sufrido un segundo hackeo y que ha dejado expuesta información de 5.2 millones de clientes.

Durante la investigación, si bien la compañía no dio a conocer más en detalle la técnica que fuera empleada, se pudo determinar que los atacantes habrían utilizado credenciales válidas de acceso al sistema de gestión hotelera de dos empleados de una de sus franquicias que emplean para

acceder a los sistemas de aplicación de la compañía. De esta forma una vez logrado el acceso obtuvieron la información de las bases de datos de los clientes, las cueles contenían nombres, correos electrónicos, programas de fidelización, empresas en las que trabajan y las preferencias de la habitación.

Por el hecho analizado, se presume que, para lograr el objetivo, los ciberdelincuentes emplearon técnicas de ingeniería social del tipo phishing para que los empleados del hotel accedan a esos correos o enlaces maliciosos y a partir de ahí hacerse de las credenciales de acceso. Otro dato no menor es que se cree que de acuerdo con la maniobra del ataque pudo haber sido realizado por una organización criminal de origen chino.

Por otra parte, la empresa hotelera aclaró que, de acuerdo con su investigación, no existió evidencia alguna de que se vieran comprometidos los datos bancarios, las contraseñas de acceso a la plataforma por parte de los clientes o la información del pasaporte.

No obstante, las contraseñas de la totalidad de cuentas Marriot Bonvoy fueron desactivadas preventivamente con el fin de que los usuarios que han sido afectados logren restablecer de manera obligatoria su contraseña cuando inicie sesión nuevamente, pero en esta oportunidad y para evitar este tipo de incidentes de seguridad, procedieron con la habilitación de un segundo factor de autenticación para garantizar un acceso seguro.

A raíz de lo sucedido la compañía habilitó oportunamente un portal web para que los clientes de la cadena hotelera puedan verificar si su cuenta había sido comprometida, instando al usuario que realizar el cambio de las credenciales de acceso. (RIVERA, s.f.)

Impacto

Como consecuencia de la filtración de los datos, se estima que se comprometió información personal de más de 5 millones de clientes, pero esta, no incluía datos bancarios, sino datos como nombres, contraseñas, lugar de trabajo y preferencias de la habitación.

No es la primera vez que le sucede a la compañía ya que en el año 2018 sufrió un ataque de similares características, pero con un impacto mayor ya que en ese entonces se filtró información más sensible como ser los datos de las tarjetas de crédito. El atenuante para ese incidente fue que los datos almacenados se encontraban cifrados con el algoritmo de *Advance Encryption Stardard* (AES-128).

El impacto fue significativo para la empresa ya que tuvo que pagar una multa por 110 millones de euros por incumplir con el Reglamento General de Protección de Datos Personales europeo (GDPR) por sus siglas en inglés, respecto a la filtración de datos del año 2020 y 26.4 millones de euros por la brecha de seguridad que sufriera en el año 2018.

Gran parte del gasto por las multas impuestas, fueron absorbidas por las compañías de seguro ya que este tipo empresas transfieren los riesgos para que sean las aseguradoras quienes afronten ese impacto económico.

Por este hecho, además haber afectado económicamente a la compañía y a la confidencialidad de la información, resultó comprometida su reputación por la desconfianza generada en sus clientes al ver que sus datos personales se encontraban circulando por la internet profunda a la compra del mejor postor.

3.5 Caso Facebook

Descripción

Facebook es un servicio de redes sociales y medios de comunicación online estadounidense con sede en la ciudad de Menlo Mark California. El sitio web fue creado y lanzado en el mes de febrero del año 2004 por Mark Zuckerberg junto a otros estudiantes de la universidad de Harvard y compañeros de habitación. En principio la red social fue pensada solamente para los estudiantes de Harvard, pero luego se extendió su uso para todo el sector educativo.

Desde el año 2006 a cualquiera persona que diga tener más de 13 años se le ha permitido convertirse en un usuario registrado en la plataforma.

En el mes de febrero del año 2012 la empresa Facebook comienza a cotizar en bolsa alcanzando una valoración de 104 mil millones de dólares, considerándose como una de las más altas. Comenzó a vender sus acciones al público tres meses después, pero la mayoría de sus ingresos los obtiene a través de los anuncios que aparecen en pantalla.

Ese mismo año, Facebook compra a la red social Instagram por 1.000 millones de dólares, una plataforma que solo estaba enfocada en la fotografía y que de la mano de Zuckerberg la hizo crecer exponencialmente.

Finalmente, en el año 2014 la firma californiana adquirió a WhatsApp por 22.000 millones de dólares y hoy Facebook es una red social que cuenta con más 3000 millones de usuarios en todo el mundo. (DOULIERY, s.f.).

Análisis del Hecho

La compañía Facebook sufrió el robo de una base de datos que

contenía más de 267 millones de identificaciones de usuario, número de teléfono y nombre de Facebook, quedando expuesto los datos para que cualquier persona pudiera acceder a ellos sin contraseña ni ningún otro tipo de autenticación.

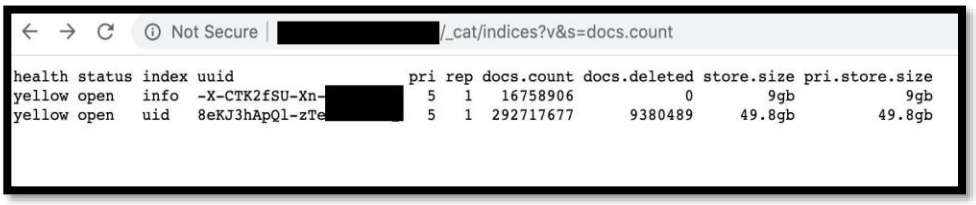
Según la investigación se cree que los datos obtenidos se debieron a una vulnerabilidad en la API de Facebook que fuera explotada por una organización criminal desde Vietnam según la evidencia y que con los datos obtenidos podrían utilizarse para realizar futuras campañas de phishing y spam SMS a gran escala, entre otras amenazas que pueden llegar a sufrir los usuarios afectados.

La base de datos estuvo expuesta durante casi 2 semanas, luego de ese tiempo se eliminó su acceso. Cronológicamente se supo que:

- El 4 de diciembre de 2019, los motores de búsqueda indexaron la base de datos por primera vez.
- El 12 de diciembre del 2019, los datos se publicaron para descarga en un foro de hackers.
- El 14 de diciembre de 2019, se descubrió la base de datos e inmediatamente se envió un informe de abuso al ISP que administraba la IP del servidor.
- El 19 de diciembre, se eliminó el acceso a la base de datos.
- El 2 de marzo del 2020, el motor de búsqueda BinaryEdge indexó un segundo servidor que contenía registros idénticos más 42 millones adicionales.
- El 4 de marzo del 2020, se descubrió un segundo servidor y se alertó al proveedor del servicio de alojamiento.
- El 4 de marzo de 2020, el servidor fue atacado y eliminado por autores desconocidos.

A continuación, se puede apreciar el sitio donde se encontraba publicada la base de datos filtrada:

Registro de la base de datos expuesta en el servidor



Fuente obtenida desde el sitio web https://cdn.comparitech.com/wp-content/uploads/2019/12/facebook-uid-exposure-1-1.jpg

En la siguiente imagen se logra identificar los tipos de datos que fueron expuestos:

Tipo de datos expuestos

Fuente obtenida desde el sitio web https://www.comparitech.com/blog/information-security/267-million-phone-numbers-exposed-online/

Con el avance de la investigación se pudo determinar que la mayoría de los usuarios afectados eran de los Estados Unidos, y que los datos filtrados contenían:

- Identificación única de Facebook
- Número de teléfono
- Nombre completo
- Marca de tiempo

El servidor que alojaba los archivos para descargarlos incluía una página de inicio con un panel de inicio de sesión y una nota de bienvenida.

El segundo servidor expuesto en marzo del año 2020 contenía los mismos datos 267 millones de registros más 42 millones de registros adicionales. Este era un servidor de Elasticksearch de EE. UU y 25 millones de registros contenían información similar, ID de Facebook, números de teléfono y los nombres de los usuarios.

Por otro lado 16.8 millones de los nuevos registros contenían más información, como ser:

- Identificador de Facebook
- Número de teléfono
- Detalles del perfil
- Correos electrónicos
- Algunos datos personales

Si bien la compañía no preciso más datos, y no quedó del todo claro como obtuvieron los atacantes esa información. Unas de las posibilidades era que la información de las bases de datos fue robada de la API del desarrollador de Facebook antes que la empresa restringiera el acceso a los números de teléfono en el 2018, ya que los desarrolladores utilizan API para agregar contexto social a sus aplicaciones al acceder a los perfiles de los usuarios, la lista de amigos, los grupos, las fotos y otro dato como los eventos. En ese entonces los números de teléfonos estaban disponibles para los desarrolladores externos de API. Luego del 2018 ese fallo de configuración fue corregido.

Otra posibilidad es que la API de Facebook podría tener agujeros de

seguridad que facilitara a los atacantes acceder a los identificadores de usuarios y números de teléfono, incluso después de haber restringido en acceso a este tipo de información. Y como última opción se comenta que los datos hayan sido robados sin usar la API y extraídos de las páginas de perfiles visibles públicamente, a través del empleo de la técnica de "*Scraping*" por el cual *bots* automatizados filtran rápidamente una gran cantidad de páginas web copiando la información de cada una de las bases de datos. Para estos casos en muy difícil que Facebook o cualquier red social pueda diferenciar un bots de un usuario legítimo cuando realiza la consulta.

Impacto

La compañía conducida por Mark Zuckemberg ha admitido los errores por la filtración de sus datos, he insistía después del incidente de seguridad que continuaba siendo la persona adecuada para dirigirla porque, el insiste "en que en la vida hay que aprender de los errores".

No obstante, no alcanzó para admitir los errores y ha generado un fuerte deterioro de su imagen, al tal punto de que usuarios de la red social borraran sus cuentas, migren hacia otras alternativas del mercado.

Por la parte económica su impacto fue más notorio ya que tuvo una fuerte caída en el valor bursátil de una de las principales compañías tecnológicas.

Dentro de los descargos que efectuó Zuckemberg es haber reconocido que no se adoptó una visión amplia sobre cuales eras las responsabilidades de la compañía ante un hecho de este tipo.

A raíz de lo sucedido la compañía Facebook anunció un cambio en sus políticas de confidencialidad y uso de la información, una de las primeras

en tres años.

En dicho documento se aclara como la red social comparte la información pública con herramientas vinculadas a esa firma, como Instagram, WhatsApp y Messenger, y determina un lenguaje más claro sobre el uso de los datos.

Posteriormente, y como consecuencia de lo sucedido fue citado por el Congreso de los E.E. U.U para responder a las preguntas de los legisladores sobre la filtración de los datos.

Por último, la Comisión Federal de Comercio (FTC) de los Estados Unidos ha impuesto una multa de 5.000 millones de dólares a Facebook por la filtración de sus datos de millones de usuarios de todo el mundo. Se trata de la sanción más elevada jamás impuesta a una compañía tecnológica en los E.E.U.U.

3.6 Caso Disney Plus

Descripción

Disney Plus en un servicio de *streaming* propiedad de la empresa *The Walt Disney Company*. El servicio ofrece contenido de películas, documentales, cortos, programas y series de televisión producidas por The Walt Disney y Walt Disney Televisión. Su interfaz presenta diferentes secciones temáticas con los contenidos de Disney, Pixar, Marvel, Star Wars, National Geofraphic y Star.

El servicio se lanzó por primera vez en noviembre del año 2019, solo en los EE. UU y Canadá. Hoy se encuentra disponible en la mayoría de los continentes con un alto grado de competitividad con el resto de las plataformas que ofrecen el mismo servicio.

En el mes de agosto del año 2016 Disney se volvió accionista minoritario en la empresa BAMTech por unos U$S 1000 millones de dólares, aumentando sus acciones para fines del año 2018 a un 75% del total, alcanzando los U$S 1580 millones de dólares.

La plataforma de Disney con la integración recientemente de Star posee aproximadamente 95 millones de suscriptores, casi el 50 % respecto a su competidor “Netflix”, que posee 200 millones de usuarios.

Análisis del hecho

Por el mes de noviembre del año 2019, piratas informáticos comenzaron a secuestrar las cuentas de los usuarios de Disney Plus horas después de su lanzamiento.

Las cuentas afectadas se encontraban a la venta en foros de piratería o en la *Dark Web* a precios que variaban desde los 3 a 11 dólares de acuerdo con una investigación realizada por ZDNet.

La compañía para ese entonces comenzó a recibir las quejas de sus clientes que no podían transmitir sus películas y programas favoritos y algunos incluso no podían acceder directamente a sus cuentas, les desconectaban de todos los dispositivos asociados y les cambiaban el correo electrónico y la contraseña de la cuenta robada.

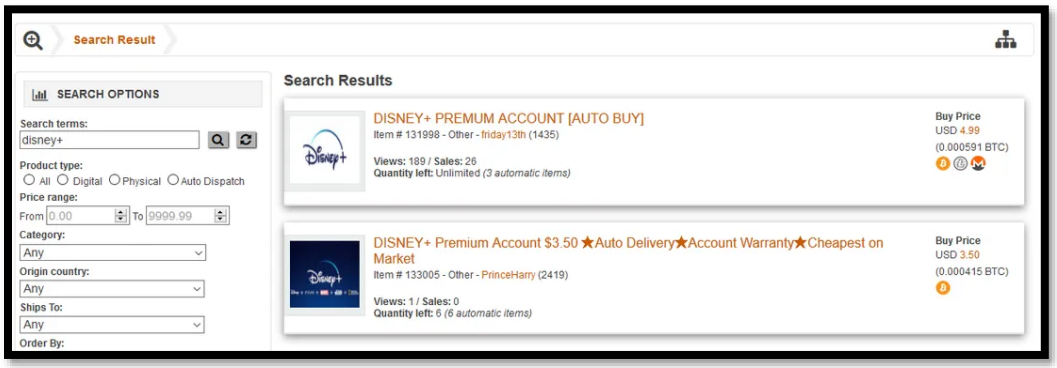
Pasada las horas, el malestar de los usuarios comenzó a tener mayor protagonismo en las redes sociales como Twitter y Reddit.

Por la forma en que se realizaba la maniobra se presume que los atacantes obtuvieron acceso a las cuentas mediante el uso de

combinaciones del correo electrónico y contraseña que habrían sido filtradas en otros sitios y en algún caso podría haberse obtenido con la infección del algún tipo de *malware* como puede ser el *Keylogger* para capturar el registro del teclado cuando el usuario escribe los datos de las credenciales de acceso.

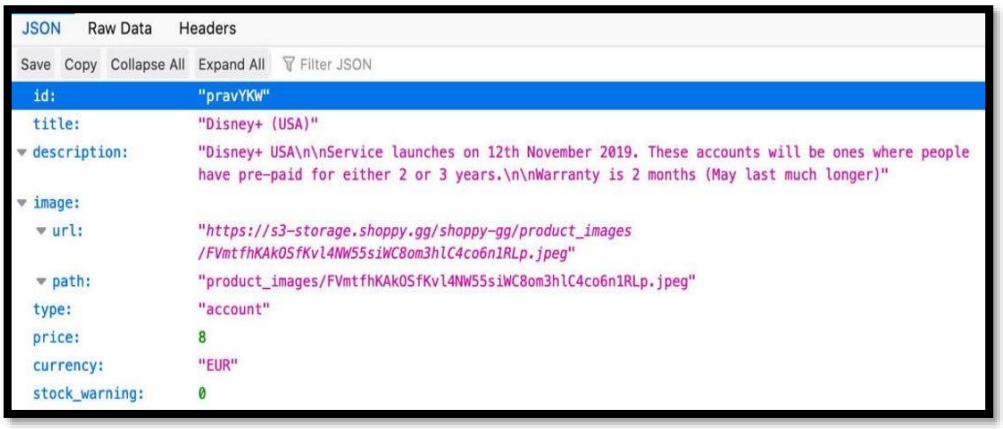
A continuación, se describe una captura de pantalla donde se muestra la publicación y venta de cuentas con acceso a la plataforma de Disney:

Otro ejemplo de la venta ilegal del servicio de streaming en un foro ruso



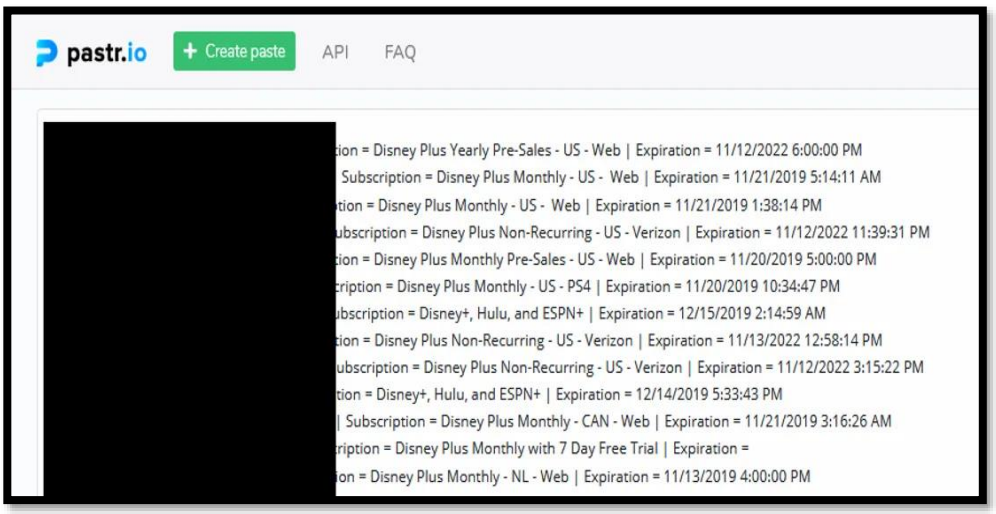
Fuentes obtenidas desde el sitio web https://www.zdnet.com/article/thousands-of-hacked-disney-accounts-are-already-for-sale-on-hacking-forums/

Captura de pantalla de una fuente de inteligencia de amenazas para las cuentas de Disney+ que se venden en un mercado ruso



Fuentes obtenidas desde el sitio web https://www.zdnet.com/article/thousands-of-hacked-disney-accounts-are-already-for-sale-on-hacking-forums/

En algunos foros incluso se podía visualizar los datos filtrados en texto plano, donde los atacantes ofrecían de manera gratuita acceso a los servicios de Disney para la comunidad de los piratas informáticos a través de sus foros. Los investigadores pudieron verificar que las cuentas ofrecidas se encontraban activas al momento de la prueba:



Fuentes obtenidas desde el sitio web https://www.zdnet.com/article/thousands-of-hacked-disney-accounts-are-already-for-sale-on-hacking-forums/

Los investigadores de ZDNet se intentaron contactar con los responsables de la empresa Disney para advertirles de lo sucedido y verificar que sistemas de seguridad poseen para proteger a los usuarios del robo o secuestro de sus cuentas, pero no obtuvieron ningún tipo de respuesta antes de que se publicara el artículo.

La consultora ZDNet en su publicación recomienda de manera preventiva que estos servicios online deben contar con soluciones de autenticación de múltiples factores como una solución simple tendiente a evitar los ataques de fuerza bruta o ingeniería social. Por otro lado, sugiere no utilizar las mismas cuentas de correo y contraseña en todos los servicios que emplean en internet. (CATALIN, s.f.)

Impacto

Del caso analizado se desprende que la filtración de esos datos no se debió a una falla o debilidad de seguridad de la infraestructura de la empresa Disney, según lo afirma la misma compañía, por lo tanto, no existió una brecha de seguridad. La hipótesis que se manejaba era que esas cuentas de usuarios podrían haber sido hackeadas en otra plataforma y utilizado el mismo correo y contraseña para registro en Disney Plus.

Si bien no afecta con un impacto económico a la compañía, indirectamente le afecta a la reputación e imagen de la compañía, por dos razones, una por no brindar un adecuado procedimiento de seguridad en el acceso a la plataforma y la otra por la falta de credibilidad de sus clientes, ya que los clientes registrados o aquellos nuevos que se quieran suscribir, evaluarán este aspecto cuando observan que sus datos se encuentran circulando por el ciberespacio.

3.7 Caso Cencosud

Descripción

La empresa Cencosud (Centros Comerciales Sudamericanos S.A) es un consorcio empresarial multinacional de procedencia chilena que opera en numerosos países de América, fundamentalmente en el rubro minorista. El mismo fue fundado y es controlado por el empresario alemán nacionalizado en Chile Hosrt Paulmann.

La empresa originalmente comenzó con un autoservicio denominado las “Brisas” en el sur de chile fundado junto a su hermano en la ciudad de Temuco. En el año 1976 se separan las operaciones y Horst inaugura la empresa Jumbo, este fue el primer hipermercado del país. Años más tarde se despliega en la ciudad de Buenos Aires. Pasado los años continuó el crecimiento en varios países y ya en el año 2011 Cencosud registraba ingresos por venta equivalente a los 15.600 millones de dólares anuales, discriminados de la siguiente manera: 41% provenían de Chile su país de origen, mientas que el 29% lo hacía desde Argentina, 21% de Brasil, 8% de Perú y el 1% de Colombia.

Cuenta con más de 130.000 empleados como parte del capital humano distribuidos entre todas las sucursales de América del Sur.

Análisis del hecho

Durante el mes de noviembre del año 2020 y en plena pandemia producto del Covid-19, la empresa Cencosud sufrió un importante ciberataque y fuga de información mediante la infección de un *malware* del tipo “*Ransomware*” que le ocasionó el bloqueo de los sistemas a cambio de poder liberarlos si se pagaba un rescate inicialmente de U$S 70 millones de

dólares, el cual con el pasar de los días, los atacantes llegaron a reducirlo a U$S 4 millones de dólares.

Si bien los directivos de la compañía decidieron no pagar el rescate, se sabe que los ciberdelincuentes lograron obtener el control del Sistema Operativo Central y desde ahí acceder a las bases de datos. Las empresas afectadas incluían a Jumbo, Easy, París y Santa Isabel las que fueron afectadas por el *Ransomware* Egregor.

Las notas de rescate que se utilizó cuando se lanzó el ataque, se comenzaron a imprimir en varios supermercados en las terminales de venta al público, con el siguiente mensaje:

"¿Qué pasó? Tu red fue atacada, tus computadoras y servidores fueron bloqueados, tus datos privados fueron descargados.

¿Qué significa eso? Significa que pronto los medios de comunicación, sus socios y clientes se conocerán.

¿Cómo se puede evitar? Para evitar este problema debe ponerse en contacto con nosotros DENTRO DE TRES DÍAS.

¿Y sino lo contactamos en tres días? Comenzaremos la publicación de datos.

Eso puedo manejarlo solo. Es su derecho, pero en este caso todos los datos serán publicados.

¡No tema a esta amenaza! Esta no es la amenaza, sino el algoritmo de nuestras acciones. Si tienes cientos de millones de dólares no deseados no hay nada por qué preocuparse, esa misma es la cantidad exacta de dinero que gastará para la recuperación y los pagos.

Me convenciste. Entonces necesitas contactarnos, hay algunas formas de hacerlo...

Recomendada el método más seguro:

a) Descargar un navegador especial

b) Instalar el navegador

c) Abre nuestro sitio web con chat en vivo en el navegador tor y siga las instrucciones de esta página.

Si el primer método no es adecuado para vos

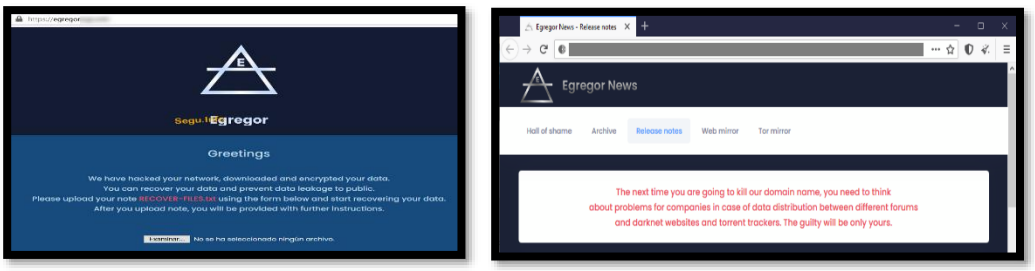
Abre nuestro sitio web con nuestro chat en vivo en el tor...

¿Qué obtendré en caso de un acuerdo? Obtendrás el descifrado completo de sus máquinas en la red, la confirmación del listado completo de la pila de la eliminación de datos (SIC) descargados de nuestros servidores, la recomendación y la confidencialidad completa sobre el incidente...".

Según el análisis realizado por la consultora AppGate, Egregor ha estado activo desde mediados de septiembre del año 2020 y se cree que ha estado vinculado a presuntos ataques contra organizaciones como GEFCO, Banners & Noble y las empresas de videojuegos Crytek y Ubisoft. (IPROUP, s.f.)

Este tipo de *ransomware* se lo ha asociado con el modelo del tipo *Ransomware As-a-Service* (RaaS) en el que los usuarios pueden suscribirse para acceder al *malware.* Una vez comprometidos los sistemas los atacantes dejan una nota a la víctima informando que su sistema fue infectado y sus archivos cifrados exigiendo que establezcan contacto a través de la red "*THE ONION ROUTER*" (TOR) por sus siglas en inglés para organizar el pago.

Egregor mantiene al menos un dominio .onion y dos dominios web tradicionales, el primero de ellos se registró el 6 de septiembre del 2020 y el segundo el 19 de octubre de 2020.



Fuentes obtenidas desde el sitio web https://blog.segu-info.com.ar/2020/11/nuevo-ransomware-egregor-cencosud-jumbo.html

Esta variante de *ransomware* utiliza una variedad de técnicas anti-ofuscación y empaquetamiento del *Layload* para evitar su análisis. En una de las etapas de ejecución la carga útil de Egregor se puede descifrar si se proporciona la clave correcta a través de una línea de comando, por lo tanto, el archivo no se puede analizar ni de manera manual ni mediante el empleo de una *sandbox* (Entorno seguro).

Se lo considera dentro de la familia de los más agresivos en términos de negociación con las víctimas. Solo da 72 hs para contactar al atacante ya que de lo contrario los datos de la víctima se procesan para su publicación. El pago del rescate se negocia a través de un chat especial asignado a cada víctima y se emplean criptoactivos.

Cuando el *malware* se ejecuta termina con los siguientes procesos:

agntsvc.exe; dbeng50.exe; dbsnmp.exe; dumpcap.exe; encsvc.exe; excel.exe; firefoxconfig.exe; infopath.exe; isgqlplussvc.exe; jmysqld-opt.exe; msaccess.exe; mspub.exe; mydesktopqos.exe; mydesktopservice.exe; mysqld.exe; mysqld-nt.exe; ocautoupds.exe; ocomm.exe; ocssd.exe; onenote.exe; oracle.exe; outlook.exe; powerpnt.exe; procexp*.exe; procexp.exe; procmon*.exe; python.exe; sqbcoreservice.exe; sqlagent.exe; sqlbrowser.exe; sqlservr.exe; sqlservr.exe; sqlwriter.exe; steam.exe; synctime.exe; thebat*.exe; thunderbird.exec; visio.exe; winword.exe; wordpad.exe; wpython.exe;

Este tipo de *ransomware* emplea un esquema de cifrado de archivos híbrido basado en cifrado de flujo Chacha y el cifrado asimétrico RSA. La clave pública maestra RSA-2048 del atacante esta insertada en el cuerpo del troyano. Cuando se ejecuta en la máquina de la víctima Egregor genera un par único de claves RSA de sesión. A partir de ahí, la clave privada RSA de la sesión es exportada y cifrada por ChaCha con una clave generada de forma única más un *nonce*, luego la clave y el *nonce* son cifrados por la clave RSA pública maestra.

Los resultados se guardan en un archivo binario como, por ejemplo: *C:/ProgramData/dtb.dat*, así como una cadena codificada en Base64 en las notas de rescate.

Para cada archivo de datos que procesa Egregor, genera una clave Chacha de 256 bits y un *nonce* de 64 bits, cifra el contenido del archivo por chacha, luego cifra usando la clave pública RSA de sesión y los guarda junto con alguna información auxiliar al final del archivo cifrado.

Como medida preventiva la gente de seguridad informática de la empresa afectada comunicó el bloqueo de las siguientes IP´s y dominios maliciosos, de acuerdo con el siguiente detalle:

En ese entonces luego de lo sucedido se informó para que se bloqueen las siguientes IP relacionadas al ataque a Cencosud. (INFOSEC, s.f.)

C&C

185.82.126[.]8

IPs

185.238.0[.]233

45.153.242[.]129

217.8.117[.]147

91.199. 212[.]52 (FALSO POSITIVO, corresponde a un certificado de crt.sectigo.com)

Dominios principales

*www.egregor[eliminado].**

egregor[eliminado].onion*

**egregor.top*

sekhmet.**

Impacto

Teniendo en cuenta la magnitud del ataque que afectó a la continuidad de un cierto sector del negocio, la empresa Cencosud interrumpió sus operaciones de cobro por al menos 48 hs. en las sus líneas de cajas hasta que los sistemas fueran restablecidos.

Por el momento se desconoce si por la fuga de información la compañía tuvo que afrontar la erogación de algún tipo de multa que fuera impuesta por los organismos de contralor de la protección de los datos personales.

Si bien desde un principio la compañía tomó la decisión de no negociar con los atacantes que la extorsionaban con el pago de 70 millones de dólares que luego se redujeron a 4 millones de dólares, su impacto económico fue relativamente importante ya que no pudo facturar por sus ventas en la totalidad de sucursales que componen la compañía.

El problema radica en que los datos de los clientes obtenidos por los ciberdelincuentes puedan luego ser usados contra los titulares. Especialmente en casos que contengan datos de tarjetas de crédito y/o fotografías de los documentos de identidad de sus clientes. Cuando ocurre un incidente que involucra el robo de datos de los clientes, las compañías

deberían notificarlos de lo sucedido para que tomen los recaudos necesarios.

Otro de los factores para tener en cuenta y no menor, es la afectación de la reputación de la empresa Cencosud en cuanto al compromiso para el cuidado o resguardo de los datos sensibles de sus clientes.

A raíz del incidente la Dirección Nacional de protección de datos personales (DNPDP) de nuestro país de acuerdo con el artículo 31 de la Ley 25.326 y sus normas reglamentarias sancionó a la empresa Cencosud Argentina por la suma de $ 290.000.

3.8 Caso Mercado pago

Descripción

La empresa Mercado Libre/Mercado Pago es una multinacional de origen argentino con sede en la Ciudad de Buenos Aires, dedicada fundamentalmente al comercio electrónico en Latinoamérica.

La compañía fue fundada en el año 1999 y en la actualidad cuenta con operaciones a través de la web además de Argentina, en Brasil, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, República Dominicana, Uruguay y Venezuela.

El comercio electrónico se destaca por la publicación de productos para la compra o venta, sean estos nuevos o usados, servicios ofrecidos en distintos rubros, entre otros.

Cuenta con una propia plataforma de cobro llamada “Mercadopago” para los compradores y de pago y abonos para los vendedores.

Se estima que para el 2016 la empresa ya tenía más de 174 millones de usuarios en todo el continente y había vendido más de 181 millones de productos.

La compañía cotiza en bolsa y se encuentra valuada en unos 12.700 millones de dólares y sus acciones subieron un 20 % en el 2022.

Durante el año 2019 se presume que ha facturado unos 80 millones de dólares, teniendo un alto crecimiento a partir del año 2020 producto de la pandemia del Covid-19.

Análisis del hecho

En el mes de marzo del año 2022 la compañía reconoció haber sufrido un incidente de seguridad por el cual los ciberdelincuentes accedieron a sus sistemas y obtuvieron código fuente.

De acuerdo con lo informado por los analistas de seguridad de la compañía accedieron a los datos de aproximadamente 300.000 usuarios de casi 140 millones de usuarios de toda la plataforma. Aseguran que no han encontrado evidencia de que los sistemas de infraestructura hayan sido vulnerados o que se hayan obtenido contraseñas de usuarios, balances de cuentas, inversiones, información financiera o tarjetas de pago.

Este hackeo fue atribuido a un grupo cibercriminal conocido como Lapsus$, quien publicó entre sus seguidores una encuesta donde invitaba a elegir el próximo objetivo de ataque, argumentando ***"¿Cuál debiera ser nuestra próxima filtración?". Las opciones eran el acceso al código fuente de Vodafone, de Impresa, ¿o de Mercado Libre?"***, e informando que tenía en su poder más de 24.000 repositorios.

Fuente obtenida desde el sitio web
https://www.infobae.com/economia/2022/03/07/filtracion-masiva-en-mercado-libre-

Por otro lado, se confirmó que el grupo hacker Lapsus$ también se encuentra detrás de la filtración de datos de empresas gigantes como Samsung y Nvidia. (INFOBAE, s.f.)

Si bien no se sabe la metodología empleada para lanzar los ataques, la policía de Londres (Reino Unido) procedió con la detención de siete adolescentes que tendrían presuntas conexiones con el grupo cibercriminal que se hace llamar Lapsus$.

Con el avance de las investigaciones, y a finales del mes de marzo del año 2022, se le atribuyó el ataque a un joven de 16 años residente de Oxford, Inglaterra quien sería el autor intelectual de los ataques perpetuados, conocido por los alias “White” o “Breachbase”, quien tendría acumulada una suma de más de 10.6 millones de libras, unos 15 millones de dólares.

Existen especulaciones en el entorno que el grupo Lapsus$ habría empleado credenciales robadas para acceder a la información e incluso de haber contado con participación interna de las compañías. (iProUP, s.f.)

En conclusión, la DNPDP resolvió dejar sin efecto el acta labrada y determinó no sancionar a Mercado Libre, instando a la compañía a implementar diversas medidas técnicas y organizativas que resulten necesarias para prevenir futuros incidentes similares al ocurrido.

Impacto

Si bien la compañía no sufrió una sanción económica, ni ningún tipo de apercibimiento por parte de la AAIP, creería que en este caso puntual se trataría de un impacto reputacional, ya que este tipo de incidente tomó estado público a través de diferentes medios, tantos en redes sociales como televisivos. El problema fundamentalmente radica en que con los datos obtenidos de los clientes, los atacantes pueden lanzar nuevos ataques, como por ejemplo los de ingeniería social.

4. Criterio de ordenamiento de acuerdo con la criticidad del hecho

Para poder determinar el grado de ordenamiento de acuerdo con la criticidad del hecho analizado, se ha tenido en cuenta los siguientes factores:

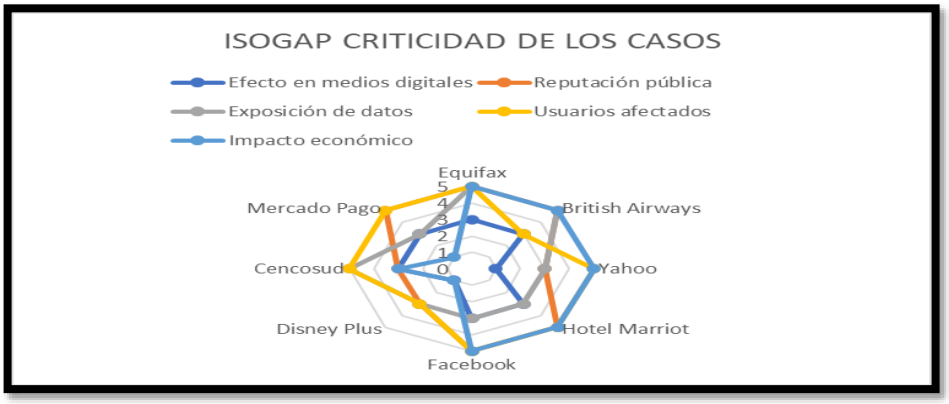
- Efecto en medios digitales
- Reputación Pública
- Tipo de exposición de datos
- Usuarios afectados
- Impacto económico

Para ello se efectuará una valoración cualitativa de acuerdo con la importancia de los factores que se han seleccionado, siendo estos ALTO, MEDIO y BAJO según consta en el siguiente detalle:

ALTO = 5 **MEDIO= 3** **BAJO= 1**

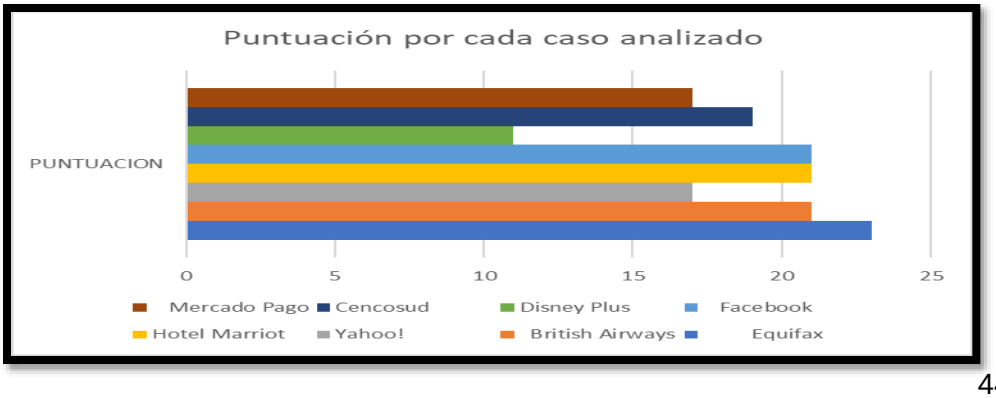
Casos	Efecto en medios digitales	Reputación pública	Exposición de datos	Usuarios afectados	Impacto económico
Equifax	MEDIO	ALTO	ALTO	ALTO	ALTO
British Airways	MEDIO	ALTO	ALTO	MEDIO	ALTO
Yahoo	BAJO	MEDIO	MEDIO	ALTO	ALTO

Hotel Marriot	MEDIO	ALTO	MEDIO	ALTO	ALTO
Facebook	MEDIO	ALTO	MEDIO	ALTO	ALTO
Disney Plus	BAJA	MEDIA	MEDIA	MEDIA	BAJO
Cencosud	MEDIO	MEDIO	ALTO	ALTO	MEDIO
Mercado Pago	MEDIO	ALTO	MEDIO	ALTO	BAJO



En la siguiente tabla se describe el cálculo cuantitativo sumando los factores de exposición de cada caso analizado y se demuestra en un Gráfico ISOGAP:

CASO	PUNTUACION
Equifax	23
British Airways	21
Yahoo!	17
Hotel Marriot	21
Facebook	21
Disney Plus	11
Cencosud	19
Mercado Pago	17



Teniendo en cuenta el resultado de los análisis efectuados anteriormente, a continuación, se procede a ordenar los 8 casos de estudio de acuerdo con los que tuvieron un mayor impacto reputacional y económico, considerando el 1ro. como el más crítico y así sucesivamente hasta llegar el 8vo. como el de menor criticidad:

N° ORDEN	CASO
1	Equifax
2	British Airways
3	Hotel Marriot
4	Yahoo!
5	Facebook
6	Cencosud
7	Mercado Pago
8	Disney Plus

5. Tipos de amenazas Cibernéticas

Vivimos en un mundo donde internet conecta todo, desde dispositivos móviles, artefactos hogareños, equipos informáticos, infraestructuras críticas, y el tan conocido mundo del internet de las cosas (IOT), es por eso por lo que la ciberseguridad nunca ha sido tan importante como lo es en estos últimos 5 años.

Si bien es importante contar con servicios de IT, Software y hardware actualizados, es elemental entender los tipos de ataques más frecuentes que sufren las empresas por la acción de ciberdelincuentes que buscan lograr su cometido. En este apartado se procederá a describir 6 casos de tipos de amenazas, de las cuales los más frecuentes son las que realizan atacando el comportamiento humano a través de técnicas de ingeniería social.

Amenaza 1: Phishing

El phishing es un correo electrónico malicioso que intenta suplantar la identidad de una entidad u organización, con el fin de que el usuario

(víctima) ingrese al supuesto sitio oficial e ingrese sus credenciales de acceso, es decir, el usuario y la contraseña. (COMPUTER, s.f.)

Amenaza 2: Phishing basado en SMS (*Smishing*)

El *Smishing* es similar al *phishing* pero con la particularidad que se recibe a través de mensajes de texto pudiendo ser por ejemplo, a través de SMS, *Whatsaap*, Telegram entre otras. Las plataformas de correo electrónico como Google o Microsoft Outlook cuentas con herramientas de inteligencia de amenazas con la capacidad para detectar correos de phishing como de spam, en cambio a través de un mensaje de texto cualquiera por desconocimiento puede abrir un enlace malicioso. (COMPUTER, s.f.)

Los tipos de ataques más comunes tanto del phishing como del smishing son los que intentan suplantar la identidad de un banco, un servicio de correspondencia postal, o empresas promocionando productos en oferta. (COMPUTER, s.f.)

Amenaza 3: Estafas de PDF

Este tipo de amenaza se recibe generalmente a través de un correo electrónico, y es una de las técnicas que más emplean los atacantes ya que saben que es muy probable que el usuario desconfíe de un enlace adjunto y no haga clic, a que abra el archivo sin dudarlo. (COMPUTER, s.f.)

Amenaza 4: *Malware* y *Ransomware*

Los ciberdelincuentes saben que muchas de las empresas mantienen sus datos en servidores que se conectan a Internet, y no todos cuentas con las herramientas de seguridad, prevención de intrusión o políticas de actualización de parches de seguridad.

La infección por *malware* se ha incrementado notablemente y cada vez existe una complejidad en su desarrollo que las soluciones de antivirus

que no actúan por comportamiento no los logran detectar. (COMPUTER, s.f.)

El *ransomware* es una variante de *malware* que una vez que el equipo es infectado comienza a cifrar la información que el equipo posee almacenado, y se propaga hacia los recursos compartidos que se encuentran en la red cifrándolos también. En la mayoría de los casos los atacantes dejan un mensaje para que el usuario efectúe un pago en criptomonedas si desea recuperar la información. Esta última acción no garantiza que aun pagando se recuperen los datos. La problemática que se viene presentando en los últimos ataques que se han visto, es que no solo exigen el pago para recuperar la información, sino que amenazan a la víctima que harán pública la información si no abonan la demanda. (COMPUTER, s.f.)

Amenaza 5: Exposición de la Base de Datos

La exposición de la base de datos es una brecha de seguridad crítica que expone la información de las empresas a los ciberdelincuentes generalmente por un error de configuración del servicio web que las exponen. (COMPUTER, s.f.)

Amenaza 6: Denegación de Servicio (DoS)

La denegación de servicio se refiere a un ataque externo que intenta hacer que un recurso informático no esté disponible para los usuarios que desean acceder a la información. Esto lo realizan inundando una red o servidor con excesivas solicitudes y datos. Generalmente ese ataque lo realizan sobre servicios web o de correo electrónico. No significa que siempre sea por la maniobra de los ciberdelincuentes, sino que puede darse por unas excesivas peticiones legítimas ante una determinada demanda. (COMPUTER, s.f.)

6. Como mitigar una fuga de información

Independientemente a desarrollar y actualizar políticas de acceso a la información de manera continua, es fundamental que toda organización siga el principio del mínimo privilegio, esto quiere decir que un usuario solo debe tener acceso a aquella información estrictamente necesaria para desarrollar sus actividades diarias, siempre y cuando la información que maneje sea confidencial.

Por otro lado, la ciberseguridad ofrece varios productos y servicios para mitigar la fuga de información, como ser los destinados a la gestión del ciclo de vida de la información, productos para el control de dispositivos externos, y los destinados a evitar fugas de información, conocidos como soluciones DLP (*Data Loss Prevention*).

El factor humano juega un papel muy importante ante este tipo de amenazas, por eso es muy importante llevar a cabo campañas de concientización en materia de ciberseguridad dentro de las Organizaciones para evitar que por una mala acción del usuario se vea comprometido su activo más valioso, la información. (INCIBE, 2016)

¿Ahora bien, la pregunta que nos debemos hacer es que pasa si ocurre una fuga de información? La respuesta desgraciadamente con aplicar solo la prevención no es suficiente, ya que de ocurrir este tipo de incidente puede generar un impacto muy negativo, no solo económico sino reputacional, pudiendo llegar a afectar a otras Organizaciones incluso a varios usuarios.

Cuando se habla de fuga de información, se refiere a la pérdida de la confidencialidad, de tal forma que información sensible sea accedida por personal no autorizado o personas ajenas a la empresa. Existen un conjunto

de normativas y leyes que ponen especial énfasis en el uso y tratamiento de datos de carácter personal que prevén sanciones del generalmente del tipo económico para este tipo de delito.

En nuestro país, la autoridad responsable que vela por el cumplimiento de la Ley de protección de datos personales (Ley 25.326) es la Agencia de Acceso a la Información Pública (AAIP), y sus disposiciones complementarias como la Resolución 47/2018 Respecto a las “Medidas de seguridad recomendadas para el tratamiento y conservación de los Datos personales en medios informatizados y no informatizados”.

Si una empresa oculta un incidente de fuga de información, y la AAIP no detectase, la sanción podría ser aún mayor. Esto es uno de los factores más importantes en la gestión de la fuga de información y, por ende, una las responsabilidades de la organización, de cara a decidir si se hace público, a quién se debe informar y en qué orden, así como otros aspectos relativos a la comunicación del suceso.

Teniendo en cuenta que existen muchos aspectos y distintas situaciones dentro de este tipo de incidentes de seguridad, una mala gestión podría ocasionar un efecto distinto al esperado, es decir, se puede potenciar el efecto negativo del incidente. A continuación, se mencionan las recomendaciones efectuadas por el Instituto Nacional de Ciberseguridad de España INCIBE:

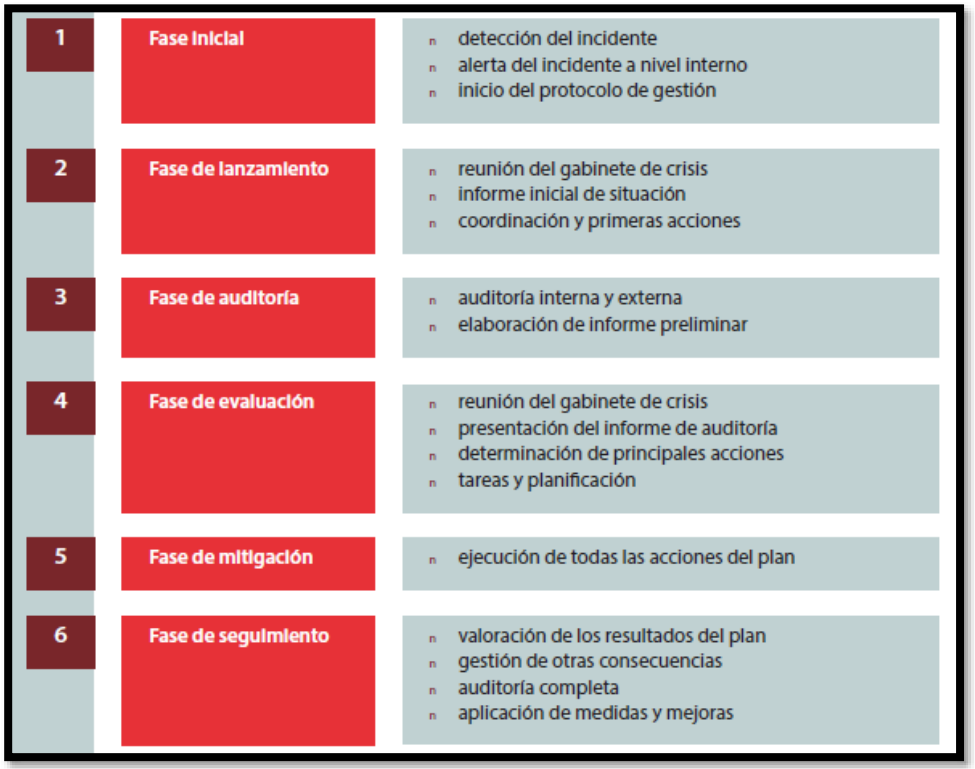
“Uno de los mayores retos a los que se enfrentan las organizaciones es conseguir la detección temprana del incidente”.

“Mantener la calma y actuar con organización es fundamental para evitar decisiones incorrectas o que pueden provocar consecuencias negativas adicionales”.

"Además de la interna, también es necesario realizar una auditoría externa. El objetivo de ésta será conocer el tamaño, gravedad y nivel de difusión de la filtración en el exterior de la organización".

"Se debe considerar que al tratarse de una evaluación inicial las tareas se diseñan en función de la información disponible, que puede ser incompleta".

A continuación, se describen las principales fases para la gestión de una fuga de información: Fase inicial, Fase de Lanzamiento, Fase de Auditoría, Fase de Evaluación, Fase de Mitigación y por último Fase de Seguimiento.



Fuente INCIBE – Fases de una Gestión de Fuga de Información

7. Conclusión General

Luego de haber realizado en análisis de los 8 casos de empresas privadas que en los últimos 5 años han sufrido una brecha de seguridad que ocasionara la fuga de su información, y teniendo en cuenta la metodología que han empleado las organizaciones criminales para lograr su objetivo, puedo concluir que un incidente de seguridad de este tipo le puede suceder a cualquier empresa u organismo, principalmente aquellas que poseen servicios expuestos a internet.

Claramente se observa en los diferentes casos analizados la gran dificultad que tienen las empresas para proteger y garantizar la confidencialidad, integridad y disponibilidad de sus datos, todas buscan proteger su activo más valioso, pero lamentablemente no pueden evitar ser víctimas de los ciberatacantes.

Las metodologías empleadas tienen algo en común, el factor humano. Los criminales han encontrado una puerta de acceso a las infraestructuras tecnológicas de las empresas a través de sus empleados. Los vectores de ataques se centraron en 2 grandes categorías: Explotación de vulnerabilidades conocidas y ataques de ingeniería social del tipo phishing, enviando un correo malicioso a cuentas de correo específicas de la organización.

Estos incidentes de seguridad ocasionan mayormente un impacto negativo para las empresas, tanto en su imagen y reputación, como en su economía y ciertamente podría llegar a afectar la continuidad del negocio, sumado a la desconfianza y exposición de datos sensibles de los clientes, que terminan perjudicándolos por no contar con un adecuado o deficiente plan de seguridad.

Durante la pandemia producto del COVID-19, el crecimiento del cibercrimen se estima que se ha incrementado más de un 300%, esto se debió principalmente a la gran dificultad que tuvieron las empresas para continuar sus operaciones con el empleo bajo la modalidad de teletrabajo, ya que tuvieron que adaptar y efectuar cambios radicales en sus infraestructuras tecnológicas para que sus empleados puedan acceder a los sistemas y bases de datos de manera remota, y que la transformación digital ha crecido notablemente con el avance de la tecnología. El comercio electrónico es un claro ejemplo de cómo nos alcanzó ese cambio de cultura ya que desde un dispositivo móvil efectuamos distintas transacciones, desde una transferencia bancaria, pago de servicios, compras de electrodomésticos o productos en tiendas, compras de criptomonedas entre otras.

Otro de los aspectos que me llamó mucho la atención, es que independientemente el país donde se filtró la información, los entes responsables de la Protección de Datos Personales aplican severas sanciones económicas cuando ocurren brechas de seguridad de este tipo. Tal es el caso por ejemplo de los países europeos alcanzados por el Reglamento General de Protección de Datos Personales (RGPD), donde las sanciones superan los millones de dólares. En nuestro País, el órgano responsable es la Agencia de Acceso a la Información Pública y por el incidente de seguridad que sufriera la empresa Cencosud solamente fue sancionada con una multa de $ 290.000.

Un punto para destacar es que no solamente les ocurre a pequeñas o medianas empresas que recién se encuentran incursionando en temas de ciberseguridad, sino que les sucede a grandes compañías que poseen implementado Sistemas de Gestión de Seguridad de la Información (SGSI), recursos económicos, personal calificado en seguridad informática y seguridad de la información y las herramientas de seguridad adecuadas para

mitigar los incidentes.

Esto es un claro ejemplo que la revisión de los planes de seguridad debe efectuarse de manera periódica, es decir, lograr un proceso de mejora continua permanentemente, como lo es también contar con adecuados procedimientos y normativas para la gestión de riesgos que puedan minimizar el impacto al negocio cuando suceden estos hechos relevantes.

Es muy importante que se lleven a cabo de manera periódica procesos de revisión de los controles o salvaguardas de seguridad con el fin de detectar de manera temprana las vulnerabilidades o deficiencias de seguridad que puedan ser aprovechadas por los atacantes.

Muchas veces a las empresas tardan más de 3 meses en saber que son víctimas de un ataque cibernético, incluso algunas ni logran enterarse de que sus datos se encuentran a la venta en la internet profunda. Irónicamente podría decir que existes 2 tipos de empresas, las que fueron hackeadas y las que aún no lo saben.

Algunas de ellas cuando sufren este tipo de brechas de seguridad, ocultan la información pare evitar ser sancionadas, y deciden hacerlo público cuando algún especialista en Ciberseguridad comenta lo sucedido en sus redes sociales. Esto es claramente un error, ya que ni bien toman conocimiento de lo sucedido, no solo deben informar a las autoridades que velan por la protección de los datos personales, sino a sus clientes para que tomen los recaudos necesarios para efectuar el cambio de credenciales de acceso o dar de baja su tarjeta de crédito ó débito en caso de corresponder.

De acuerdo con los casos analizados concluyo que cuando hablamos de fugas de información solo pensamos que les puede suceder a las pequeñas compañías y no es así, les sucede incluso a las grandes

corporaciones.

Lo que se puede destacar es la importancia que tiene la capacitación o concientización de los empleados en materia de ciberseguridad. Haciendo una analogía con un conflicto bélico, en donde los soldados cuentan con drones, tanques, radares, armamento sofisticado, sino saben emplearlas van a perder la batalla. En el caso de las compañías, sucede algo similar, las empresas pueden contar una herramientas e infraestructura de seguridad de vanguardia, pero si los empleados no son formados todo va a ser en vano.

8. Bibliografía

ABC.ES. (21 de 09 de 2017). Obtenido de ABC.ES: https://www.abc.es/tecnologia/redes/abci-robados-datos-personales-mas-140-millones-clientes-equifax-grupo-crediticio-americano-201709081406_noticia.html

ACOSTA, D. (s.f.). *https://www.pcihispano.com/que-es-pci-dss/*.

BISCHOFF, P. (s.f.). *https://www.comparitech.com/blog/information-security/267-million-phone-numbers-exposed-online/*. Obtenido de https://www.comparitech.com/blog/information-security/267-million-phone-numbers-exposed-online/.

BISCHOFF, P. (s.f.). *https://www.comparitech.com/blog/information-security/267-million-phone-numbers-exposed-online/*.

CATALIN, C. (s.f.). *https://www.zdnet.com*. Obtenido de https://www.zdnet.com/article/thousands-of-hacked-disney-accounts-are-already-for-sale-on-hacking-forums/

COMPUTER, I. (s.f.). *IBIS COMPUTER*. Recuperado el 13 de 07 de 2022, de https://www.ibiscomputer.com/blog/130-las-6-principales-amenazas-de-ciberseguridad-para-las-empresas-en-2021-y-como-prevenirlas

DOULIERY, O. (s.f.). Obtenido de https://tn.com.ar/tecno/redes-sociales/2022/02/03/el-aniversario-de-facebook-la-evolucion-de-la-red-social-a-18-anos-de-su-creacion/?gclid=Cj0KCQjw1tGUBhDXARIsAIJx01lq0xHK40L4rmzvs5ooT_qmHPJQ4VXQbEtNDRKhUxdulxsqXqplEKsaAhk3EALw_wcB.

ECONOMISTA, E. (s.f.). *www.eleconomista.es*. Obtenido de https://www.eleconomista.es/tecnologia/noticias/9049619/04/18/Facebook-amplia-el-impacto-de-su-filtrado-de-datos-afecto-a-87-millones-de-usuarios.html

EQUIFAX. (15 de 05 de 2022). Obtenido de EQUIFAX: https://www.soluciones.equifax.com.ar/acerca-de-equifax/perfil-de-la-empresa

FBI.GOV. (28 de 01 de 2020). Obtenido de FBI.GOV: https://www.fbi.gov/wanted/cyber/chinese-pla-members-54th-research-institute/chinese-pla-members-wanted-8-5x11-web2b.pdf/view

https://www.riskiq.com/blog/labs/magecart-british-airways-breach. (s.f.).

INCIBE. (2016). *COMO GESTIONAR UNA FUGA DE INFORMACION.* INCIBE_PTE_AproxEmpresario_003_FugaInformacion-2016-v1, INSTITUTO NACIONAL DE CIBERSEGURIDAD, Madrid. Recuperado el 29 de Julio de 2022, de https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_fuga_informacion_0.pdf

INFOBAE. (10 de 02 de 2020). Obtenido de INFOBAE: https://www.infobae.com/america/eeuu/2020/02/10/estados-unidos-acuso-a-

cuatro-militares-chinos-por-el-hackeo-de-equifax-la-filtracion-de-datos-mas-grande-de-la-historia/
INFOBAE. (s.f.). *www.infobae.com*. Obtenido de https://www.infobae.com/economia/2022/03/07/filtracion-masiva-en-mercado-libre-acceden-sin-autorizacion-a-los-datos-de-300000-usuarios/

INFOSEC. (s.f.). *SEGU-INFO*. Obtenido de https://blog.segu-info.com.ar/2020/11/nuevo-ransomware-egregor-cencosud-jumbo.html

IPROUP. (s.f.). *IPROUP*. Obtenido de https://www.iproup.com: https://www.iproup.com/innovacion/18582-hackeo-a-cencosud-se-filtro-la-informacion

iProUP. (s.f.). *www.iproup.com*. Obtenido de https://www.iproup.com/innovacion/30376-hackeo-a-mercado-libre-y-samsung-detienen-a-7-adolescentes

KLIJNSMA, Y. (11 de 09 de 2018). *RISKIQ.COM*. Obtenido de RISKIQ.COM: https://www.riskiq.com/blog/labs/magecart-british-airways-breach/
LAINFORMACION.COM. (s.f.). *https://www.lainformacion.com/empresas/yahoo-pagara-28-millones-por-el-robo-de-datos-de-1-500-millones- de-usuarios/6346917/*.

Médico, F. d. (27 de 05 de 2020). *MAPLINK.GLOBAL*. Obtenido de MAPLINK.GLOBAL: https://maplink.global/blog/es/que-es-transformacion-digital/

RIVERA, N. (s.f.). *https://hipertextual.com/2020/04/marriott-hackeo-52-millones-clientes*.
Wikipedia. (s.f.). *https://es.wikipedia.org/wiki/Yahoo!*