masempresas.cea.es
#masempresas

Ciber Riesgo: La Amenaza Constante

Ponentes:
Álvaro Sepúlveda Priego
Enrique Hernández Rodríguez

Grupo PACC Correduría de Seguros

CEA Confederación de Empresarios de Andalucía

Junta de Andalucía
Consejería de Transformación Económica, Industria, Conocimiento y Universidades

Asempal
CONFEDERACIÓN EMPRESARIAL DE LA PROVINCIA DE ALMERÍA

Contenidos

01

Ciber Riesgo:

El seguro de incendio del siglo XXI

02

El seguro como consultoría:

La importancia del cuestionario

03

¿Protección o Servicios?

04

Resumen de Coberturas :

Vinculación de la póliza con gestiones técnicas

05

Casos prácticos:

Medidas Preventivas, Medidas Correctivas y transferencia al seguro

06

Preguntas frecuentes

1. Ciber Riesgo: El seguro de incendio del siglo XXI

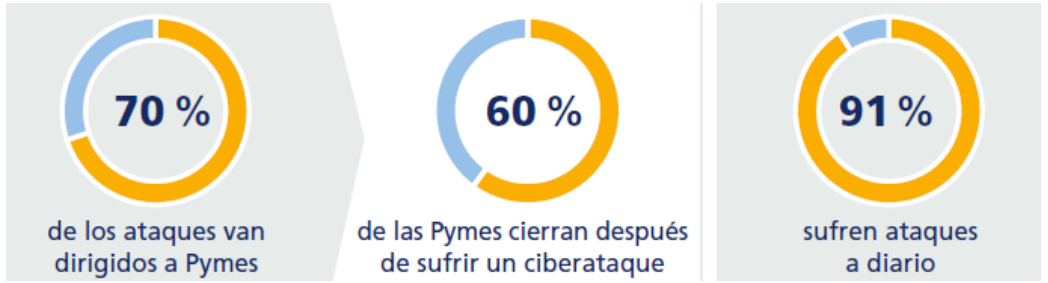
El seguro de incendio se crea en 1.676 como respuesta al gran incendio de Londres, un pequeño incendio en una panadería se propagó por toda la ciudad arrasando con 13.200 casas y negocios así como con 87 iglesias incluida la catedral de San Pablo.

La predominante construcción con madera, las medidas de seguridad de la época y los procesos productivos a base de carbón desencadenaron el desastre, el fuego "aprovechó" las debilidades en los edificios para provocar un colapso sin precedentes en la capital del imperio.

Si extrapolamos este suceso a nuestros días, el desarrollo de internet y la dependencia de las empresas a todo lo digital es caldo de cultivo para que el fuego, en forma de ataque cibernético, aproveche la falta de protección de los usuarios, ya sean particulares o empresas, para devorar información y paralizar nuestro día a día.

1. Ciber Riesgo: El seguro de incendio del siglo XXI

- Cualquier empresa, pequeña o grande es susceptible *de sufrir un ataque cibernético* que tenga consecuencias no solo en sus equipos, sino en la información y los datos que maneja.
- Solo en España, se producen *cada día 400 ciberataques a empresas* que suponen un *coste medio* para las empresas de *50.000 €*.
- *España es el país con más ataques cibernéticos* después de EE.UU. y de Reino Unido, y la previsión es que esta tendencia se mantenga.
- *El 70% de estos ataques los reciben las pymes y más de la mitad de éstas se ven obligadas a cerrar 6 meses después de haberlo sufrido*.



2. El seguro como consultoría: La importancia del cuestionario

Al igual que en los seguros de Daños o Responsabilidad Civil es vital dar la información correcta sobre medidas de seguridad o agravaciones de riesgo, en los seguros de CYBER hay que dar a la compañía información concreta sobre el negocio, uso de dispositivos, uso de software, uso de equipos y medidas de seguridad.

Estos datos no sólo sirven para configurar una oferta acorde a la situación de la empresa sino como consultoría en protección informática:

- Con el cuestionario identificamos debilidades
- Como empresarios conocemos la situación real de nuestra empresa frente a ciberataques
- La compañía hará una oferta conforme al riesgo y medidas de protección existentes
- La aseguradora propondrá mejoras y nos explicará el por qué son necesarias
- De contratar ponen a nuestra disposición servicios y contacto directo con consultoras de alto nivel : KPMG, Mckenzie, Deloitte, Lazarus…

3. ¿Protección o Servicios?

Las compañías pondrán a su disposición los siguientes servicios incluidos en póliza:

- *Recomendaciones legales sobre protección de datos.* Si tiene dudas sobre la nueva ley de protección de datos, le haremos recomendaciones generales para ayudarle a cumplir con la normativa.
- *Análisis de reputación en las redes*. Si quiere saber lo que dicen de su empresa en las redes, llevamos a cabo un análisis detallado para facilitarle la información y ayudarle a mejorarlo.
- *Recomendaciones de protección cibernética*. Si no sabe cómo protegerse o cómo reaccionar ante un incidente cibernético, le ofrecemos información tanto a usted como a sus empleados.
- *Asistencia cibernética 24 h*. Si las pantallas de su empresa se bloquean o tiene dudas sobre si una copia de seguridad está bien hecha, un especialista le ayudará a resolver el problema.
- *Software de protección*. Si necesita proteger sus equipos, comprobamos que su antivirus esté al día y le instalamos una aplicación para evitar el secuestro de información.
- *Copias de seguridad*. Si tiene información que no quiere perder, le ofrecemos un sistema de copias de seguridad diarias para que los datos de su empresa estén siempre a salvo.
- *Análisis de vulnerabilidad web, y red IP interna y externa*. Si quiere conocer el grado de vulnerabilidad de su web o de su red de dispositivos, analizamos qué peligros le pueden venir de internet, realizamos recomendaciones e implementamos soluciones.

Formación a Empleados. Formación continua a la plantilla incluyendo simulacros de ataque y creando un protocolo de actuación

4. Resumen de Coberturas : Vinculación de la póliza con gestiones técnicas

¿CÓMO LE PROTEGEN LAS PÓLIZAS CIBERRIESGO?

- Cuando entramos en lenguaje profesional sobre informática y tecnología, es muy fácil que nos perdamos en lo tecnicismos y la terminología anglosajona, por lo que pasamos a exponerle las coberturas de nuestro producto de la manera más clara posible.
- Actuaciones inmediatas y de contingencia: Si un pirata informático entra en su sistema y le impide acceder a sus archivos, lo restauramos para que pueda seguir trabajando.
- Gestión de incidentes: Si le roban información sensible o confidencial de sus clientes, investigamos el origen y alcance del incidente y gestionamos las reclamaciones que se deriven.
- Recuperación de datos electrónicos: Si un virus cifra los archivos de sus ordenadores y no puede leer ni acceder a nada, los recuperamos para que pueda continuar con su actividad.
- Reparación o reemplazo del hardware: Si por un ataque cibernético, estropean un disco duro o la impresora, reparamos o reemplazamos la parte de la maquinaria afectada.
- Responsabilidad civil frente a terceros: Si le roban datos bancarios o médicos y le denuncian, investigamos el robo y cubrimos posibles reclamaciones de terceros.

4. Resumen de Coberturas : Vinculación de la póliza con gestiones técnicas

¿CÓMO LE PROTEGEN LAS PÓLIZAS CIBERRIESGO?

- Sanciones por incumplimiento de normativa: Costes económicos por incumplimiento del Reglamento General de Protección de Datos, los mismos pueden alcanzar los 20 M € o el 4% de la facturación y poner en peligro la viabilidad de la empresa.
- Responsabilidad por publicaciones en internet: Si hackean sus cuentas y publican información falsa de su negocio o producto, neutralizamos esa información eliminándola de la red.
- Pérdida de beneficios: Si por un ataque cibernético, se ve obligado a suspender la actividad, le pagamos las pérdidas económicas que sufra mientras no pueda continuar con su actividad.
- Incidentes de ciber extorsión: Si roban datos sensibles de sus clientes y le amenazan con publicarlos, abonamos los gastos para salvaguardar la información.
- Fraude por robo de identidad: Si suplantan su identidad y se hacen pasar por usted para cerrar un acuerdo con un proveedor, nos hacemos cargo de los honorarios y costes de esa suplantación.
- Fraude por ingeniería social: Si engañan a un empleado para que haga una transferencia bancaria, le pagamos el importe de la transferencia.
- Fraude informático: Si hackean los datos de las cuentas bancarias para robarle dinero, le devolveremos la cantidad que le hayan robado.

5. Casos Prácticos (Ransomware-Phising-suplantación-fraude al ceo) : Medidas Preventivas, Medidas Correctivas y transferencia al seguro

- RANSOMWARE

El ransomware es un tipo de programa malicioso, cuyo principal objetivo es infiltrarse en los sistemas informáticos de las empresas para dañarlos, bloquearlos o cifrarlos.

Se caracteriza porque inutiliza y bloquea determinados archivos del sistema pidiendo un rescate (normalmente en moneda virtual) para recuperar la información. Su nombre le viene de esta peculiaridad, "ransom", rescate en inglés y "software", de programa.

Normalmente este tipo de programas se camuflan dentro de otros programas o aplicaciones de uso habitual (por ejemplo, archivos adjuntos en correos electrónicos, links de anuncios, videos, actualizaciones de programas fiables etc.) que invitan a la víctima hacer clic para combinar con otras técnicas de ataques que consiguen instalarse en los quipos informáticos pasando desapercibidos para el usuario.

Existen muchos tipos de ransomware, entre los que destacan el que provoca el secuestro del ordenador (imposibilidad de usarlo), y el cifrado de sus archivos (criptoware), sea cual sea el soporte en que esté (equipos individuales, en red, en nube, etc.)

Cabe reseñar la proliferación de ransomware diseñados específicamente para atacar dispositivos conectados a internet, siendo denominados RoT(Ransomware of Things).

Durante los últimos años numerosos estudios, consultoras expertas y organismos estatales a nivel mundial coinciden en afirmar que ha sido la gran amenaza que se ha materializado en las empresas, y se prevé que siga siéndolo adoptando formas más sofisticadas y complejas, dificultando su detección y subsanación.

5. Casos Prácticos (Ransomware-Phising-suplantación-fraude al ceo) : Medidas Preventivas, Medidas Correctivas y transferencia al seguro

Ransomware

Ejemplos de este tipo de ciber-riesgo son los famosos Wannacry, cuyos costes se estimaron entorno a los 200 millones euros, NotPetya, especialmente sangrante para algunas compañías como la farmacéutica americana MSD con 310 millones de dólares, la logística FedEx con 300 millones de dólares.

Un ejemplo de ataque y sus consecuencias sería por ejemplo un correo con una factura que llega al departamento de contabilidad de una gran empresa. El usuario abre la factura e infecta a su equipo y todos los equipos que están conectados en la misma red. El atacante toma todos los activos digitales empresariales como rehenes, cifrando la información.

Pide un pago a la empresa a cambio de la clave de cifrado, además usa técnicas de presión para que la víctima pague amenazando con dejar datos irrecuperables pasado un tiempo, publicar información, eliminar todos los datos, incrementar cantidad a pagar pasado un tiempo, etc.

5. Casos Prácticos (Ransomware-Phising-suplantación-fraude al ceo) : Medidas Preventivas, Medidas Correctivas y transferencia al seguro

Ransomware

- **Móvil:** Económico.
- **Causa Del Incidente:** Descuido o negligencia de un usuario al aceptar un correo, actualizar una aplicación o cualquier otra tarea cotidiana.
- **Métodos De Ataque:** Ransomware. Ingeniería social, suplantación de identidad, uso de Botnets.
- **Tipo De Riesgo Afectado:** Daños Patrimoniales, Responsabilidad Civil, Daño Reputacional (en caso de falta de servicio), Responsabilidad de Administradores y Directivos, etc.
- **Impacto Económico Del Incidente:** El impacto total de este tipo de ataque resulta difícil de calcular, no sólo por los costes directos e inmediatos (sin contar el pago del rescate, hecho que no garantizaría la recuperación de la información) como remediación de sistemas y restablecimientos de los servicios afectados, sino por el conjunto de daños provocados, como el reputacional, ventas no realizadas, pérdida de confianza de los clientes e inversores, sanciones, penalizaciones de contratos, etc., incluso pérdidas de vidas. Debido a las características del ataque, puede asegurarse que este tipo de ciber-riesgo es de los más costosos para las empresas, incluyendo el supuesto pago por rescate.

- **SECTORES MÁS AFECTADOS POR ESTE TIPO DE INCIDENTES**

Los ataques por este tipo de ciber-riesgo han crecido exponencialmente a todo tipo de usuarios, destacando en los últimos años los sectores de energía (persiguiendo la interrupción del suministro), gubernamentales, sanitario, telecomunicaciones, domésticos, negocios, gobiernos e incluso servicios críticos como hospitales o centrales energéticas.

5. Casos Prácticos (Ransomware-Phising-suplantación-fraude al ceo) : Medidas Preventivas, Medidas Correctivas y transferencia al seguro

Ransomware

- **LECCIONES APRENDIDAS**

MEDIDAS PREVENTIVAS	Establecimiento de un Modelo de Gobierno Corporativo de Ciberriesgos. Copias de seguridad y procedimientos que permitan restaurar los datos y archivos en un periodo de tiempo específico. Políticas de contratación con fabricantes de HW y SW más estrictas (Security by default). Instalación de software anti-ransomware. Aplicación del principio de mínimos privilegios: adecuar los accesos a la información susceptible de ser cifrada a los usuarios realmente necesarios. Formación en seguridad de información y mejorar los controles de política interna y de seguridad de la información. Campañas de concienciación en seguridad de información.	**MEDIDAS CORRECTIVAS**	**GESTIÓN**	Análisis forense para determinar la veracidad del incidente y su tamaño. Recuperar las bases de datos de las copias de seguridad en el tiempo adecuado. Comunicación del hecho delictivo a los Cuerpos y Fuerzas de Seguridad. Campaña de relaciones públicas (cuando se produzca pérdida de reputación).
		MEDIDAS CORRECTIVAS	**TRANSFERENCIA (Cobertura de seguros)**	Gastos de mitigación y análisis forense. Pérdida de beneficios. Ciber extorsión. Gastos de reputación. Gastos legales. Multas y sanciones. Responsabilidad Civil (aunque en general es difícil encontrar pólizas que cubran las reclamaciones por este tipo de incidente). Consejeros y Directivos.

5. Casos Prácticos (Ransomware-Phising-suplantación-fraude al ceo) : Medidas Preventivas, Medidas Correctivas y transferencia al seguro

PHISHING

El término phishing se refiere a las técnicas utilizadas por cibercriminales para suplantar la identidad de un sitio web con objeto de sacar algún tipo de beneficio engañando a las víctimas. El modus operandi más sencillo del phishing se divide en tres fases:

1. **Relación de una imagen de la página web.** Consiste en crear un sitio web falso similar al que se quiere imitar. Hoy en día existen herramientas automatizadas que directamente simulan la navegación que haría un usuario para descargar el contenido completo de la página web. A partir de los datos descargados, estas herramientas crean un código web y las imágenes necesarias, para poder publicar dicha página.
2. **Colocación de la página web.** Para que una página web pueda ser accedida debe estar publicada en un servidor web. Existen dos principales métodos que utilizan los delincuentes bien hackear un servidor web legítimo de alguna empresa y añadirle la página web falsa, de forma silenciosa dentro de los contenidos de la página web. Esta primera opción no tiene coste directo, pero la disponibilidad de la página web falsa tendrá un tiempo de publicación limitada que va desde que se coloque la página web hasta que la empresa propietaria de la página web se percate de este uso indebido.

La segunda opción pasa por la compra de un dominio similar al que se quiere copiar (por ejemplo, supongamos el nombre de una empresa Karla que tiene una página web www.karla.com, posibles dominios de suplantación serían www.kaarla.com, www.karlaa.com, www.karlaweb.com, etc.) y la compra de los servicios de publicación en la nube, para colocar la página web falsa. Los delincuentes suelen aprovecharse de la escasa colaboración internacional existente seleccionando países con una escasa legislación al respecto. El inconveniente de esta técnica es que conlleva unos pequeños costes asociados al registro del dominio y la contratación de la página web.

3. **Distribución de la dirección web falsa.** Esta es la última fase de este tipo de ata-ques y consisten en hacer llegar la página web falsa al mayor número de usuarios posible, de forma que se incremente al máximo las probabilidades de éxito. A tal fin los delincuentes suelen comprar bases de datos con direcciones de emails que sue-len ir clasificadas por nacionalidades del usuario de cara a acotar el tipo de engaño lo máximo posible.

5. Casos Prácticos (Ransomware-Phising-suplantación-fraude al ceo) : Medidas Preventivas, Medidas Correctivas y transferencia al seguro

PHISHING: Caso

A mediados de 2010 el propietario de una pequeña empresa de Estados Unidos recibió una llamada de alerta del director de la sucursal del pequeño banco con el que trabajan. El director le comentaba que en la cuenta bancaria no había dinero suficiente para hacer frente al pago de las nóminas. El propietario de la pequeña empresa se sorprendió, aunque no había sido de lejos el mejor año las ventas se estaban comportando bien y la situación financiera de la empresa era buena. Lo más probables es que se tratará de un error del banco por lo que acordó con el director de la sucursal acercarse para analizar la situación y buscar soluciones.

Una vez en la sucursal el director le mostraba al propietario de la empresa el listado de movimientos de la cuenta sobre la que se realizaban los pagos de las nóminas. Durante toda la semana se habían registrado pequeñas transferencias de dinero a distintas cuentas que habían disminuido los casi 20.000$ que se disponían a poco más de 3.000$. El director del banco le aseguraba que habían chequeado las transferencias y que todas se habían realizado con el usuario del que disponen.

Una vez en la empresa el propietario habló con las pocas personas que tenían acceso a los usuarios que manejan las cuentas bancarias, todos confirmaron que no habían realizado dichas transferencias. En ese momento el propietario de la empresa decidió poner en conocimiento de las autoridades los hechos para denunciarlo. Desde la Policía le recomendaron adquirir los servicios de una empresa especializada de seguridad.

La empresa especialidad de seguridad inició una investigación enfocando el caso hacia los ordenadores de aquellas personas que manejan las cuentas. Tras la investigación se identificó que uno de los trabajadores de la compañía había recibido un mensaje con un enlace web.

Cuando los especialistas hablaron con el trabajador les comentó que había abierto el correo, siguiendo los pasos que le habían indicado (cambio de contraseña), pero que esta no se llegó a realizar porque la página le mostró un error. Los especialistas de seguridad no consiguieron acceder a la página web del mensaje porque ésta ya no estaba disponible.

El propietario de la empresa tuvo que hacer frente en primera instancia a la pérdida económica de las transacciones realizadas, aunque con la colaboración del banco se pudieron retroceder algunas de las últimas transacciones realizadas.

Asimismo, el propietario de la empresa acordó con el banco reforzar el acceso a las cuentas de la empresa mediante el uso del modo de acceso seguro que implica el utilizar un código de verificación en el acceso.

5. Casos Prácticos (Ransomware-Phising-suplantación-fraude al ceo) : Medidas Preventivas, Medidas Correctivas y transferencia al seguro

PHISHING: Caso

Móvil Del Incidente

- Económico.
- Robo de Información confidencial.
- Daño Reputacional.

Causa Del Incidente

Engaño a un empleado mediante el empleo de técnicas de ingeniería social por los delincuentes con la finalidad de acceder a los datos confidenciales de la víctima (claves y contraseñas) para realizar pagos y transferencias de dinero a través de Internet

Métodos De Ataque

- Phishing y sus diversas tipologías y evoluciones: Pharming, Wi-Phishing, Spear Phishing, Smishing y Vishing.
- Ingeniería Social.
- Suplantación de identidad.

Tipo De Riesgo Afectado

- Daño patrimonial
- Información.
- Daño reputacional.

Impacto Económico Del Incidente

De cientos de euros a millones de euros.

Sectores Más Afectados Por Este Tipo De Incidentes

Existe una tendencia a la baja en la aplicación de este método para grandes empresas, pero se mantiene para particulares y Pymes.

5. Casos Prácticos (Ransomware-Phising-suplantación-fraude al ceo) : Medidas Preventivas, Medidas Correctivas y transferencia al seguro

PHISHING

- **LECCIONES APRENDIDAS**

MEDIDAS PREVENTIVAS	Establecimiento de un Modelo de Gobierno Corporativo de Ciberriesgos. Sistemas de seguridad de filtrado de web y de email. Procedimientos: nunca responder a ninguna solicitud de información personal a través de correo electrónico, llamada telefónica o mensaje corto (SMS). Autentificación por doble o triple factor. Formación en seguridad de información y mejorar los controles de política interna y de seguridad de la información. Campañas de concienciación en seguridad de información.	**MEDIDAS CORRECTIVAS**	**GESTIÓN**	Tratar con la entidad bancaria informándola de lo sucedido. Análisis forense para determinar el alcance y causa del incidente. Denunciar ante las autoridades. Restablecer contraseñas.
			TRANSFERENCIA (Cobertura de seguros)	Gastos de mitigación y análisis forense. Robo de identidad (si bien no repone el dinero robado). Gastos Reputacionales. Gastos legales. Crime. Consejeros y Directivos.

5. Casos Prácticos (Ransomware-Phising-suplantación-fraude al ceo) : Medidas Preventivas, Medidas Correctivas y transferencia al seguro

SUPLANTACION DE IDENTIDAD

Pese a las múltiples variantes que presenta, con carácter general podemos decir que la suplantación de identidad es un tipo de ataque mediante el cual una persona consigue hacerse pasar por otra, típicamente engañando al elemento (persona o sistema) encargado de verificar la identidad de la misma en el proceso de registro o acceso.

Lo anterior se logra, generalmente, demostrando que se conoce información o se poseen determinadas características de la persona suplantada, que pueden ir desde datos personales (fecha de nacimiento, DNI, nombre de los hijos, etc.) hasta, en el caso extremo, sus credenciales de acceso.

También puede utilizarse ingeniería social (o ausencias de control) para lograr engañar al elemento encargado del registro o acceso y conseguir la suplantación sin necesidad de conocer la información que normalmente se requiere.

5. Casos Prácticos (Ransomware-Phising-suplantación-fraude al ceo) : Medidas Preventivas, Medidas Correctivas y transferencia al seguro

SUPLANTACION DE IDENTIDAD: Caso

Imaginemos que en la compañía ACME se despide a un trabajador, con buenos conocimientos tecnológicos, por conductas no acordes con el código ético y que este trabajador busca venganza. Para llevarla a cabo, se le ocurre suplantar la identidad del CEO de ACME en una red social de amplia difusión y comenzar a difundir información falsa de la compañía.

Inicialmente, utiliza herramientas automáticas que permiten obtener la lista de todos los contactos que tiene el CEO en su cuenta, y descarga su foto de perfil y la información que aparece publicada. Después crea un perfil falso, idéntico al perfil original y posteriormente, utilizando también librerías automáticas, va agregando uno a uno a todos los contactos del CEO de ACME, personalizando la solicitud de tal modo que diga "Por favor, ten en cuenta que a partir de este momento esta es mi nueva cuenta en la red social".

Una vez que va recibiendo las aceptaciones de los contactos, comienza a difundir información aparentemente normal y, en un momento dado, publica que deja ACME porque éticamente no puede soportar por más tiempo las directrices del dueño encaminadas a publicar noticias falsas de una determinada tendencia.

Otro ejemplo de suplantación de identidad sería el que podría sufrir una persona normal que, pese a ser un usuario habitual de Internet y realizar habitualmente transacciones de comercio electrónico (con un poder adquisitivo medio), tiene poca conciencia de seguridad.

Esta persona está registrada en un foro web de aficionados al motor. Esta web, muy popular y con un elevado número de usuarios, llama la atención de un grupo de hackers, que comienzan a analizar las vulnerabilidades del sitio, encontrando una que les permite acceder a los servidores. Una vez dentro, son capaces de acceder a las bases de datos y obtienen las cuentas de los usuarios registrados, que incluyen la dirección de correo y sus contraseñas de acceso al foro, y cuelgan esta información en un sitio específico utilizado habitualmente por hackers de diversa índole.

Como el usuario reutilizaba en el foro la misma contraseña que en su cuenta de correo electrónico personal, las herramientas automáticas utilizadas habitualmente por otros hackers detectan las cuentas comprometidas y prueban a acceder a la cuenta de correo electrónico de la víctima, lo que consiguen dado que el usuario utilizaba, por comodidad, la misma contraseña. Posteriormente, los hackers, dentro de la cuenta de correo de la víctima, listan los e-mails existentes con el objetivo de identificar servicios habituales de compra a través de Internet. Tras esto, resetean la contraseña de acceso a estos sitios (generalmente el proceso consiste en enviar un enlace al correo del usuario para poder llevar a cabo la operación de reseteo), acceden a estas webs de compras y, reseteando las contraseñas, se dedican a comprar con las tarjetas de crédito allí almacenadas, enviando la mercancía a puntos de recogida públicos con destinatarios ficticios.

5. Casos Prácticos (Ransomware-Phising-suplantación-fraude al ceo) : Medidas Preventivas, Medidas Correctivas y transferencia al seguro

SUPLANTACION DE IDENTIDAD: Caso

- **Móvil**

Una vez realizada la suplantación, y dependiendo de la entidad o medio en el que se haya logrado llevar a cabo la misma, el atacante puede comenzar a actuar en nombre de la persona suplantada, buscando en la mayoría de las ocasiones obtener algún tipo de beneficio económico o comprometer la reputación de la víctima o de terceros relacionados con él.

En este sentido, algunas de acciones habituales suelen ser solicitar un crédito o préstamo hipotecario, extorsionar a la víctima, solicitar transferencias, contratar servicios en nombre de un tercero beneficiándose de los mismos, difundir información u opiniones falsas buscando un determinado efecto o enmascarar acciones delictivas.

Dentro de las acciones de suplantación que buscan conseguir un beneficio económico o dañar la reputación de la víctima, se podría destacar el caso en el que empresas competido-ras utilicen estos medios para suplantando la identidad de algún directivo o empleado con acceso a información confidencial y sensible ya sea de carácter económico o de otro tipo, y utilizarla en su provecho.

- **Causa Del Incidente**

Para lograr la suplantación de identidad, se puede contar con la obtención de las claves y los datos personales a través del Phishing o la suplantación web y otras formas de ciber ataque que conlleven la revelación o el robo de datos personales, para su posterior explotación.

También se podría producir cuando se rompe la cadena de confidencialidad, identificación y verificación de la identidad personal.

Por otro lado, en muchas organizaciones esto se puede producir ante una mala educación organizativa en lo referente a la seguridad cibernética.

- **Métodos De Ataque**

Los modos más habituales mediante los que los atacantes consiguen obtener los datos de las víctimas suelen ser los de explotar la información publicada en redes sociales (LinkedIN, Twitter, Facebook, etc.) , realizar "hackeos" directamente a la víctima, bien comprar en el mercado negro registros robados a compañías hackeadas o llevar a cabo ataques de ingeniería social en los que el atacante se hace pasar (por ejemplo) por un empleado de fuerzas del orden o de una compañía de suministros básicos para solicitar información privada a la víctima.

Con estos "hackeos" se consigue acceder a claves y accesos personales y confidenciales remitidos o almacenados por el propio usuario en sus bases de datos y/o correo electrónico, y a través de esas claves de usuario cometer la suplantación de identidad.

También se pueden conseguir a través del Phishing y de la suplantación del correo/web.

- **Tipo De Riesgo Afectado**

Daño reputacional, daño patrimonial, responsabilidad civil (en el caso de revelación de información crítica).

5. Casos Prácticos (Ransomware-Phising-suplantación-fraude al ceo) : Medidas Preventivas, Medidas Correctivas y transferencia al seguro

SUPLANTACION DE IDENTIDAD: Caso

- **Impacto Económico Del Incidente**

Muy variado, el impacto directo e indirecto puede llegar a alcanzar elevadas cantidades.

- **Sector Más Afectado Por Este Tipo De Incidentes**

Cada vez son más usuarios los afectados por este tipo de ciber ataque. De hecho, según el Eurostat, España es uno de los países de la Unión Europea donde más suplantaciones/robos de identidad se teníanregistrados, con un 7% de los cibernautas en los últimos 12 meses analizados.

Los sectores más afectados varían desde instituciones bancarias, hasta instituciones estatales, pasando por el sector sanitario.

Además, con la influencia de las Redes Sociales, cada vez está más extendido este tipo de amenaza.

5. Casos Prácticos (Ransomware-Phising-suplantación-fraude al ceo) : Medidas Preventivas, Medidas Correctivas y transferencia al seguro

SUPLANTACION DE IDENTIDAD: Lecciones aprendidas

MEDIDAS PREVENTIVAS

Establecimiento de un Modelo de Gobierno Corporativo de Ciberriesgos.

Herramientas de tecnología de la información que reduzcan los posibles efectos de este tipo de ataques.

Campañas de concienciación en seguridad de información (no establecer la misma contraseña para todo, crear contraseñas seguras, cambiarlas regularmente, no enviar información personal susceptible vía correo electrónico u otro tipo de vías sensibles, navegación solo por lugares oficiales, realización de transacciones seguras...).

MEDIDAS CORRECTIVAS

GESTIÓN

Análisis forense para determinar el alcance y causa del incidente.

Denunciar ante las autoridades.

Comunicación a las partes afectadas (bancos, instituciones estatales, etc.).

Campaña de relaciones públicas (cuando se produzca pérdida de reputación).

MEDIDAS CORRECTIVAS

TRANSFERENCIA (Cobertura de seguros)

Gastos de mitigación y análisis forense.
Suplantación de identidad.
Crime.
Pérdida de Beneficios.
Gastos reputacionales.
Ciber extorsión.
Responsabilidad Civil.
Consejeros y Directivos.

5. Casos Prácticos (Ransomware-Phising-suplantación-fraude al ceo) : Medidas Preventivas, Medidas Correctivas y transferencia al seguro

FRAUDE AL CEO

También conocido en ingles como "Whaling Attack" ("Caza de ballenas" o "Caza del pez gordo") o "BEC Attack" (Business Email Compromise), es una de las formas de ciberdelincuencia más recientes y con un mayor crecimiento.

Se trata de un tipo de fraude en el que los cibercriminales aprovechan la facilidad de suplantación de identidad inherente a los medios de comunicación electrónicos (en particular el correo electrónico) que combinan con técnicas de engaño (ingeniería social) para incitar a un empleado, previamente elegido como víctima, a realizar algún tipo de transacción sensible (financiera o de información), hacia un destino controlado por los atacantes, pasando a su poder. Los controles y procedimientos internos de las compañías, en ocasiones demasiado laxos, no logran detectar el fraude hasta que se ha llevado a efecto.

En el caso más simple, los estafadores envían un correo electrónico a un empleado incauto elegido como víctima, perteneciente al área Financiera o Contable de la compañía. El correo, que viene de una dirección supuestamente legítima de alguna persona de la alta dirección, como el Director General (o CEO, de ahí el nombre del fraude), apremia al empleado para que envíe dinero o realice el pago de una factura a una determinada cuenta bancaria. Esta cuenta, bajo el control de los ciberdelincuentes, estará ubicada en algún país donde resulte prácticamente imposible seguir su rastro de forma que, si la operación se lleva finalmente a efecto, no se podrá recuperar el dinero.

Bajo este mismo esquema han aparecido otras variantes; en unos casos, los ciberdelincuentes solicitan al empleado el envío de información sensible de la compañía (que será luego empleada con otros fines maliciosos), o también se hacen pasar por un proveedor de la compañía que solicita un cambio en la cuenta bancaria en la que se abonan los servicios o suministros prestados por otra nueva (que por supuesto estará bajo su control).

Si bien el vector de ataque principal es el correo electrónico, también se utiliza el teléfono, mensajes de texto, servicios de mensajería electrónica como Telegram o Whatsapp, e incluso una combinación de varios de esto medios (por ejemplo, iniciar el contacto con la víctima con una primera llamada telefónica, para continuar posteriormente con el correo electrónico).

Es un tipo de un fraude muy dirigido y bien preparado para el que los ciberdelincuentes se toman tiempo estudiando a la víctima (a partir de informaciones disponibles en internet, publicaciones en redes sociales, investigación de los empleados, etc.) hasta tener la información suficiente para hacer que el ataque sea lo más realista y exitoso posible.

FRAUDE AL CEO: Casos

El pasado 12 de agosto de 2016, Leoni, el mayor fabricante de cables eléctricos de Europa con más de 81.000 empleados repartidos por 31 países, anunció públicamente que había sido víctima del "fraude del CEO" por un importe cercano a los 40 millones €. La Directora Financiera (CFO) de una fábrica de la compañía ubicada en Bistrita (Rumanía) recibió un correo electrónico que parecía provenir de uno de los altos ejecutivos de la compañía en Alemania.

La Dirección General para la Investigación de la Delincuencia Organizada y el Terrorismo de Rumanía (DIICOT) informó que los estafadores tenían un amplio conocimiento sobre los procedimientos internos para aprobar y procesar transferencias ya que, de las cuatro que Leoni tiene en Rumanía, esta fábrica es la única autorizada para transferir dinero.

En enero de 2016 el fabricante francés de maquinaria industrial Etna Industrie, con unos 50 empleados, fue víctima del fraude del CEO por importe de unos 100.000 €. Una empleada de la compañía recibió una llamada telefónica indicándole que en breve recibiría un correo de la Directora General de la Compañía, Carole Gratzmuller, dándole instrucciones; se trataba de una operación confidencial de adquisición de una compañía en Chipre; tenía que seguir las indicaciones que le darían desde un despacho de abogados. En breve recibió varios correos y llamadas telefónicas desde el supuesto despacho. Finalmente se llegaron a realizar transacciones de unos 500.000 € si bien gracias a la intervención de los bancos, "sólo" 100.000€ llegaron a su destino final.

5. Casos Prácticos (Ransomware-Phising-suplantación-fraude al ceo) : Medidas Preventivas, Medidas Correctivas y transferencia al seguro

FRAUDE AL CEO: Casos

- **Móvil Del Incidente:** Económico.
- **Causa Del Incidente:**
  - Engaño a un empleado.
  - Controles inadecuados dentro de la organización.
- **Métodos De Ataque:** Ingeniería social.
- **Tipo De Riesgo Afectado:** Daño patrimonial.
- **Sectores Más Afectados Por Este Tipo De Incidentes**

Según publicó en febrero de 2017 el Centro de Denuncias de Delitos en Internet (IC3) del FBI, "el fraude del CEO continúa creciendo, evolucionando y apuntando a negocios de todos los tamaños. Desde enero de 2015, ha habido un aumento del 1.300 % en las pérdidas identificadas, que ahora suman más de 3 mil millones de dólares".

El dinero sólo se ha podido recuperar en un 4% de casos. El fraude afecta desde pequeñas empresas hasta grandes corporaciones y en cualquier ámbito de actividad (compañías priva-das, administraciones públicas, universidades, hospitales, escuelas...).

En la mayoría de los casos, el dinero se ha traspaso a cuentas en China y Hong Kong.

En los últimos tres años se han reportado fraudes en más de 100 países. Es una de las formas de delincuencia de mayor crecimiento.

5. Casos Prácticos (Ransomware-Phising-suplantación-fraude al ceo) : Medidas Preventivas, Medidas Correctivas y transferencia al seguro

FRAUDE AL CEO: Lecciones aprendidas

MEDIDAS PREVENTIVAS		Establecimiento de un Modelo de Gobierno Corporativo de Ciberriesgos. Procedimientos internos de autorización de operaciones. Formación en seguridad de información y mejorar los controles de política interna y de seguridad de la información. Campañas de concienciación en seguridad de información.
MEDIDAS CORRECTIVAS	**GESTIÓN**	Tratar con la entidad bancaria. Denunciar ante las autoridades.
	TRANSFERENCIA	Crime.

6. Preguntas frecuentes FAQ

1. No veo la necesidad de contratar una póliza de ciberseguridad.

En 2021, los ataques cibernéticos supondrán la primera causa de delito en el mundo y las consecuencias de sufrirlo pueden, incluso, comprometer la continuidad de la empresa.

2. No entiendo de estos temas ni sé qué es esto de los ciberriesgos.

Precisamente una de las ventajas de Ciberseguridad es su sencillez. Lo contratas, activas el servicio siguiendo las instrucciones que te facilitaremos y ya puedes empezar a disfrutar de su protección. Y si tienes alguna duda durante el proceso de activación, nos llamas y te ayudamos. Estás confiando tu seguridad en manos de expertos, mientras te dedicas a lo que realmente te importa: hacer crecer a tu empresa.

3. Ya tengo un seguro para mi empresa.

Los seguros "tradicionales" de empresa y los de Responsabilidad civil no cubren los riesgos de ciberseguridad. Además, no contarás con las medidas de prevención activa que sí te ofrece el nuevo Ciberseguridad.

4. Mi empresa es pequeña. Nadie se fijará en ella.

Todas las empresas, incluso las de menor tamaño, están expuestas a ataques desde el momento en que gestionan algún tipo de dato, dependen de sistemas informáticos y contratan u ofrecen servicios a terceros. Además, las más pequeñas concentran gran parte de los ataques al estar más desprotegidas y ser por tanto más vulnerables.

6. Preguntas frecuentes FAQ

5. Mi empresa no es un objetivo.

Para sufrir sus consecuencias, ni siquiera tienes por qué ser objetivo de los delincuentes. El 80% de los incidentes tienen su origen en errores humanos, prioritariamente de los empleados. Basta con abrir un mensaje de correo electrónico malicioso para que un virus infecte todos tus ordenadores en línea.

6. Mis ordenadores están convenientemente protegidos.

No dudo que tus ordenadores están protegidos, pero Ciberseguridad va más allá de la protección de ordenadores. Dispones de otros servicios de prevención como el informe de vulnerabilidades de la web o materiales de concienciación en ciberseguridad para los empleados. Pero, sobre todo, en caso de un incidente de ciberseguridad, te facilitaremos inmediatamente soporte a través de un equipo de técnicos especializado en informática forense que le asistirá para aminorar el impacto del incidente y resolverlo con la mayor prontitud.

7. Nunca antes he sufrido un ataque.

Eso está muy bien, pero, ¿sabes que las empresas tardan una media de 210 días en percatarse de que han sufrido una intrusión en su sistema? Algunas ni siquiera lo saben hasta que no reciben un mensaje de extorsión o ven publicadas en las redes sus listas de clientes con todos los datos.

8. Se tratará de un seguro caro.

¿En cuánto valoras tu empresa? ¿Y los datos que tus clientes te han cedido para su custodia? ¿Sabes el importe de sanciones que deberías asumir en caso de fuga de datos de tus clientes? Seguro que las respuestas a estas cuestiones alcanzan importes infinitamente más importantes que la prima de este seguro que, dicho sea de paso, es muy competitiva.

9. Si sufro un ataque ya haré frente a sus consecuencias con mis propios recursos.

Hay que ser conscientes de los gastos y perjuicios indirectos que te puede suponer un ciberataque. A las posibles sanciones derivadas del incumplimiento de las medidas preventivas para evitar la sustracción de datos, pueden sumarse otros como la paralización del negocio mientras dura la investigación, la pérdida de confianza de tus clientes, la inversión económica para implementar un sistema de seguridad fiable que evite otro incidente, etc.

10. Mi actividad empresarial no es objetivo de ciberdelincuentes.

Los hackers no van a elegir a tu empresa por su actividad, sino por el valor de sus activos de información y por su nivel de vulnerabilidad. Si tienes una cartera de clientes, si manejas sus datos a través de sistemas informáticos, si tienes proveedores a los que estás interconectado, tu empresa es objetivo de los delincuentes aunque creas lo contrario.

Información y Consultas en
masempresas.cea.es

/CEA.es @CEA.es_ /CEA.es

+CEA Empresas

Gracias

GRUPO PACC
Correduría de **Seguros**

CEA
Confederación de Empresarios de Andalucía

Financiado por:

Junta de Andalucía
Consejería de Transformación Económica, Industria, Conocimiento y Universidades

Información y Consultas en
masempresas.cea.es

/CEA.es @CEA.es_ /CEA.es

+CEA mpresas

Coraboran:

Financiado por:

CEA
Confederación de Empresarios de Andalucía

Junta de Andalucía
Consejería de Transformación Económica, Industria, Conocimiento y Universidades

Asempal
CONFEDERACIÓN EMPRESARIAL DE LA PROVINCIA DE ALMERÍA

cec CONFEDERACIÓN EMPRESARIOS PROVINCIA DE CÁDIZ

ceco CENTRO DE FORMACIÓN, INICIATIVA Y APOYO A LA ACTIVIDAD EMPRESARIAL
CONFEDERACIÓN DE EMPRESARIOS DE CÓRDOBA

CGE CONFEDERACION GRANADINA DE EMPRESARIOS

FOE Federación Onubense de Empresarios

CEJ CONFEDERACION DE EMPRESARIOS DE JAEN

cem CONFEDERACIÓN DE EMPRESARIOS DE MÁLAGA

ces CONFEDERACIÓN DE EMPRESARIOS DE SEVILLA

Fomento de la Cultura Emprendedora