DESPACHOS BK
ETL GLOBAL
Tax · Legal · Audit

Seguimos sumando juntos

1er CONGRESO NACIONAL DESPACHOS BK ETL GLOBAL

RIOJA FORUM
9 Y 10 DE SEPTIEMBRE

Periciales actuales en materias de ciberseguridad y estafas.

DESPACHOS BK
ETL GLOBAL
Tax · Legal · Audit

CIBERSEGURIDAD
Que es y cual es su importancia:

CIBERSEGURIDAD – Conceptos.

- **La ciberseguridad es la práctica de proteger los sistemas más importantes y la información** confidencial ante ataques digitales. También es conocida como seguridad de la tecnología de la información (TI). Las medidas de ciberseguridad están diseñadas para combatir las amenazas a los sistemas en red y aplicaciones, que se originen **tanto desde dentro como desde fuera de una organización.**
- En 2020, el coste medio de una brecha de seguridad en los datos fue de 3,86 millones de dólares a nivel mundial. Estos costes incluyen los gastos de descubrimiento y respuesta a la brecha, **el coste del tiempo de inactividad y los ingresos perdidos, así como los daños a la reputación a largo plazo para un negocio y su marca.** (Fuente: IBM)
- Una buena estrategia de ciberseguridad debe presentar **múltiples capas de protección**, desde la formación del usuario final hasta la protección de los datos en la "nube" o dispositivos móviles, pasando por seguridad especifica para los sistemas y aplicaciones, además de una **política rigurosa de protección de datos.**
- **Las empresas están más conectadas que nunca**. Sus sistemas, usuarios y datos residen y operan en diferentes entornos. La seguridad basada en el perímetro ya no es adecuada. Una **estrategia de confianza cero (Zero Trust)** establece controles para validar la autenticidad y la finalidad de cada usuario, dispositivo y conexión en la empresa.

CIBERSEGURIDAD – Mitos peligrosos.

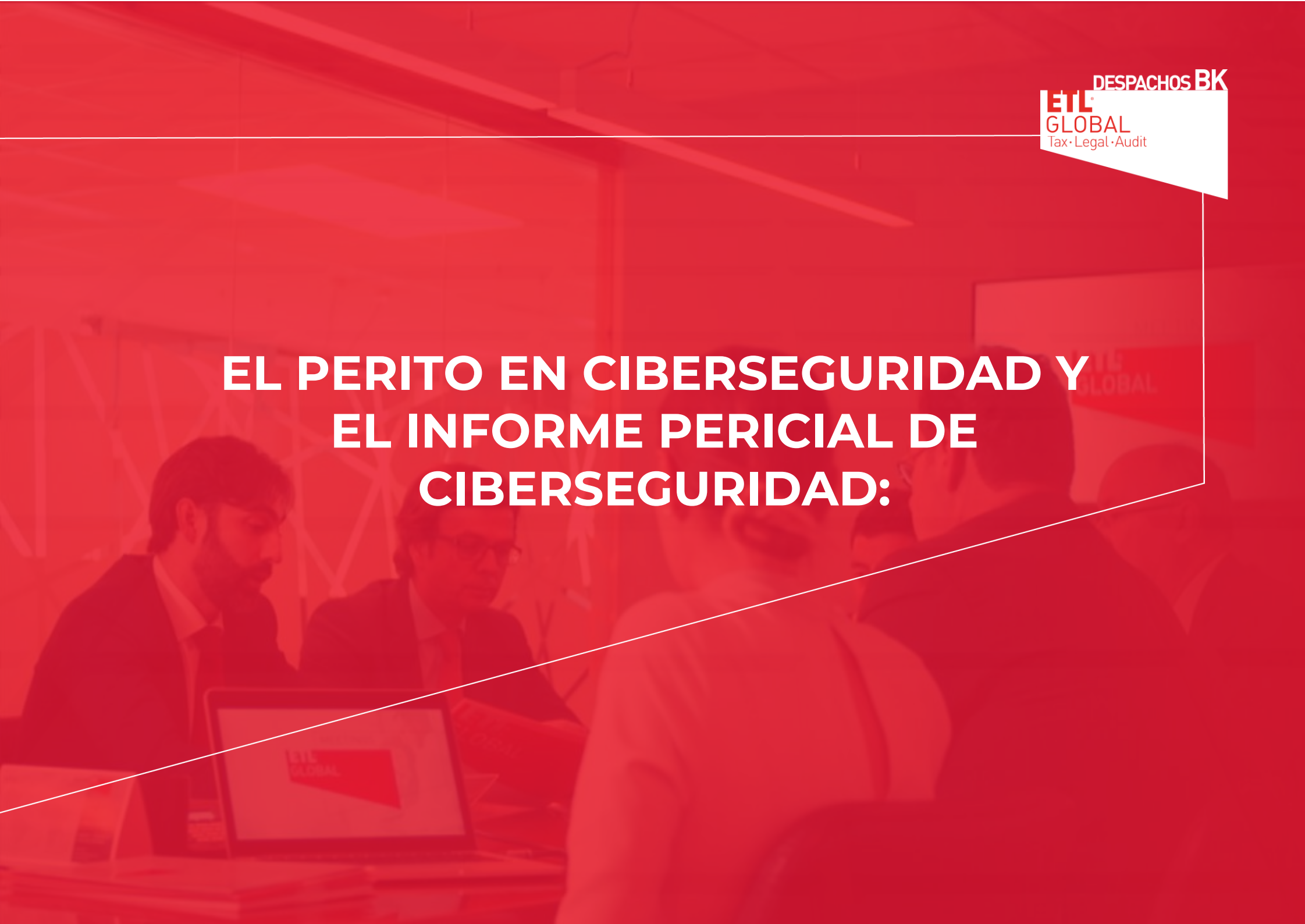
- **Los ciberdelincuentes son externos.** En realidad, las brechas de ciberseguridad mas comunes suelen ser el resultado de ataques internos que pueden trabajar en conjunto atacantes externos. Estos atacantes internos pueden formar parte de grupos organizados, e incluso contar con el apoyo de estados o naciones.
- **Los riesgos son conocidos.** Los casos de riesgo crecen continuamente, con la notificación de miles de nuevas vulnerabilidades en aplicaciones y dispositivos antiguos, pero también en los nuevos. El error humano, en concreto por parte de empleados o usuarios negligentes, sigue en aumento y es la causa de la mayoría de las brechas de seguridad en los datos, .
- **Mi sector es seguro.** Todos los sectores tiene su parte de riesgo, ya que los ciberdelincuentes explotan las necesidades de las redes de comunicación que existen en todas las organizaciones tanto públicas como privadas. Por ejemplo, los ataques de ransomware (secuestro de información) están dirigidos a más sectores que nunca, incluida la administracion publica, las organizaciones sin ánimo de lucro, cadenas de suministro, etc.

CIBERSEGURIDAD – Amenazas mas comunes.

- **Ransomware. E**s un tipo de programa malicioso que bloquea archivos, datos o sistemas y amenaza con borrar o destruir los datos, o con publicar los datos privados o confidenciales, a menos que se pague un rescate a los ciberdelincuentes.
- **Amenazas internas.** Empleados actuales o pasados, clientes, proveedores, o cualquier persona que haya tenido acceso a nuestros sistemas o redes anteriormente puede ser considerado una amenaza si abusa de sus permisos de acceso. Las amenazas internas pueden ser invisibles para las soluciones de seguridad tradicionales, como los cortafuegos y los sistemas de detección de intrusiones, que se centran en las amenazas externas.
- **Phishing. E**s una forma de ingeniería social que engaña a los usuarios para que proporcionen información confidencial. Se ha producido una avalancha de phishing con la pandemia, ligada al crecimiento del teletrabajo.
- **Man-in-the-middle.** Es un ataque de escuchas no autorizadas, donde un ciberdelincuente intercepta y retransmite mensajes entre dos partes para robar datos.
- **Ataques de denegación de servicio distribuido (DDoS).** Un ataque DDoS intenta hacer caer un servidor, un sitio web o una red sobrecargándola con tráfico, generalmente desde varios sistemas coordinados.

DESPACHOS BK
ETL GLOBAL
Tax · Legal · Audit

EL PERITO EN CIBERSEGURIDAD Y EL INFORME PERICIAL DE CIBERSEGURIDAD:



CARACTERISTICAS DEL PROFESIONAL

El perito en ciberseguridad es un profesional (perito informático colegiado) con experiencia contrastada en análisis de casos de ciberseguridad de todo tipo para aportar **una opinión experta de carácter legal** para ser utilizada en un juicio.

Debe ser minucioso y con una elevada capacidad analítica para identificar todos los factores que influyen en el análisis y valoración de las reclamaciones relacionadas con la ciberseguridad. En su análisis, deberá acceder a la información de los sistemas y a continuación identificar los elementos clave sobre los que sustentar su caso ante el juez. El perito deberá hacer un diagnostico, dar argumentos y redactar un informe pericial con su dictamen.

El informe pericial tiene que tener un **lenguaje comprensible para las personas sin conocimientos informáticos, con especial atención a los jueces.** Es muy importante que conste de una **parte de antecedentes** que sirva de contexto, una **parte de análisis** donde se detalle la metodología y criterios empleados, y por último cuáles son las **conclusiones** que extrae con todo lo anterior.

En los procesos judiciales pueden intervenir dos tipos de perito informático:

El perito judicial informático: Estudia las cuestiones que se le plantean y aporta sus conclusiones para asesorar al órgano judicial a definir su opinión sobre un aspecto técnico en el que éste no tiene conocimientos.
El perito informático de parte: Actúa a instancia de una de las partes en el proceso. Normalmente antes de formular ninguna demanda, y para evaluar las probabilidades de que prospere. Trabaja junto al abogado de la parte y le aporta razonamientos técnicos que le sean de ayuda en su cometido. Es el mas habitual.

ISO/IEC 27037 DIRECTRICES PARA LA IDENTIFICACIÓN, RECOPILACIÓN, ADQUISICIÓN Y PRESERVACIÓN DE EVIDENCIA DIGITAL. (Ratificada por AENOR en diciembre de 2016.)

Se busca que la estandarización se adopte de manera generalizada, haciendo más sencillo comparar, combinar y contrastar los resultados de investigaciones que se hayan realizado por diferentes personas u organizaciones y probablemente en diferentes jurisdicciones.

La evidencia digital: La evidencia digital se define como información y datos de valor para una investigación que se almacena, recibe o transmite por un dispositivo electrónico. Se dice que la información que se almacena electrónicamente es «digital» porque se desglosa en dígitos; unos y ceros, que se guardan y recuperan mediante un conjunto de instrucciones llamadas software o código.

La evidencia digital puede provenir de cualquier tipo de almacenamiento electrónico o medios de comunicación, como teléfonos, ordenadores, consolas de videojuegos, pendrives, y los nuevos dispositivos IoT. Por su naturaleza, la evidencia forense digital es muy frágil, y puede ser dañada fácilmente o alterada debido a un manejo inadecuado. Las pruebas viciadas que puedan haber sido adquiridas o protegidas sin el nivel requerido de seguridad pueden ser legalmente inadmisibles.

ISO/IEC 27037 DIRECTRICES PARA LA IDENTIFICACIÓN, RECOPILACIÓN, ADQUISICIÓN Y PRESERVACIÓN DE EVIDENCIA DIGITAL. (Ratificada por AENOR en diciembre de 2016.)

El propósito fundamental de los estándares de forense digital ISO/IEC 27037, 27041, 27042 y 27043 es promocionar **métodos de buenas prácticas** y procesos para la investigación forense de evidencia digital.
Este estándar no reemplaza requerimientos legales específicos de cualquier jurisdicción, la evidencia digital se rige por tres principios fundamentales: **relevancia, confiabilidad y suficiencia.**

La relevancia es una condición técnicamente jurídica, a través de la cual debería ser posible demostrar que el material adquirido es relevante para la investigación, que contiene información de valor para ayudar a la investigación del hecho y que hay una buena razón para que se haya adquirido. Todo aquello que no cumpla con este requisito será irrelevante y excluido del material probatorio recabado para efectos del caso bajo estudio.

La confiabilidad es otra propiedad fundamental en la cual se establece que todos los procesos utilizados en el manejo de la potencial evidencia digital deben ser auditables y repetibles. Los resultados de la aplicación de tales procesos deben ser reproducibles. La evidencia que se extrae u obtiene es lo que deber ser y que, si un tercero sigue el mismo proceso, deberá obtener resultados similares verificables y comprobables.

La suficiencia es la propiedad que está relacionada con la complejidad de las pruebas informáticas, se debe haber reunido suficiente material para permitir una adecuada investigación, es decir que se tienen los elementos suficientes para sustentar los hallazgos y verificar las afirmaciones efectuadas sobre la situación investigada.

FASES HABITUALES DEL PROCESO

Planificación de la intervención. Junto al abogado se determinará fecha y hora de las actuaciones, personal técnico necesario y los recursos tecnológicos requeridos. Es importante definir si alguna tarea de recolección de evidencia digital se llevará a cabo en el lugar del hecho, o si se procederá en el laboratorio.

Realizar las intervenciones necesarias. Según el plan de acción elaborado anteriormente, y que nos genera como resultado un conjunto de información. Siempre teniendo en cuenta el principio: **“Mayor información es igual a Mejor investigación”.**

Asegurar la información. La finalidad es garantizar actuaciones seguras, **evitando procesos que podrían alterar la evidencia digital.** Se pueden realizar copias de la información verificando el hash de la imagen forense para autenticar y preservar la integridad de los datos. Teniendo como referencia los principios de confiabilidad y suficiencia, se debe asegurar que las evidencia y sus copias forenses cumplen las políticas establecidas por la autoridad competente.

Análisis y documentación. Identificar los elementos que se utilizan, con marcas y modelos, números de serie, o características que los distingan. Reflejar la cadena de custodia de las evidencias. Fundamentar todas las acciones, los métodos, técnicas y herramientas utilizadas. **Es muy importante que el lenguaje utilizado sea formal, pero no necesariamente técnico**, y que permita informar el resultado de la investigación de forma clara y concisa, ya que el lector no tiene porqué conocer la parte técnica. Elaborar un dictamen o informe detallado, y asegurar que las evidencias, y sus copias forenses cumplen las políticas establecidas por la autoridad competente.

INCIBE
INSTITUTO NACIONAL DE CIBERSEGURIDAD

WWW.INCIBE.ES

CONOCE INCIBE

- El Instituto Nacional de Ciberseguridad de España (INCIBE), anteriormente Instituto Nacional de Tecnologías de la Comunicación, es una sociedad dependiente del Ministerio de Asuntos Económicos y Transformación Digital a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial y consolidada como entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, red académica y de investigación, profesionales, empresas y especialmente para sectores estratégicos.
- Con una actividad basada en la investigación, INCIBE contribuye a construir ciberseguridad a nivel nacional e internacional. La actividad de INCIBE se proyecta en el plano internacional a través de foros especializados en gestión de incidentes y garantizando el alineamiento con las estrategias europeas en la materia.
- Formación especializada. INCIBE pone a tu disposición cursos gratuitos de formación online en materia de ciberseguridad. Desde múltiples ópticas: para empresas y autónomos, para profesional tecnológicos, para familias, y material general de información y concienciación.
- Cuenta con un departamento de cumplimiento legal, que asesora a profesionales y empresas sobre como aumentar la confianza del mercado cumpliendo la ley vigente. RGPD, LPI, LSSI - Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico.
- Cuenta con un observatorio que nos puede avisar de manera periódica de las amenazas mas importantes.

DESPACHOS BK
ETL GLOBAL
Tax · Legal · Audit

CASOS PRACTICOS MAS COMUNES:

1. PHISING, ESTAFA POR CORREO ELECTRONICO.
2. BEC, CORREO ELECTRONICO COMPROMETIDO

PHISING – Suplantación de identidad.

Es uno de los fraudes más conocidos y extendidos por la Red.

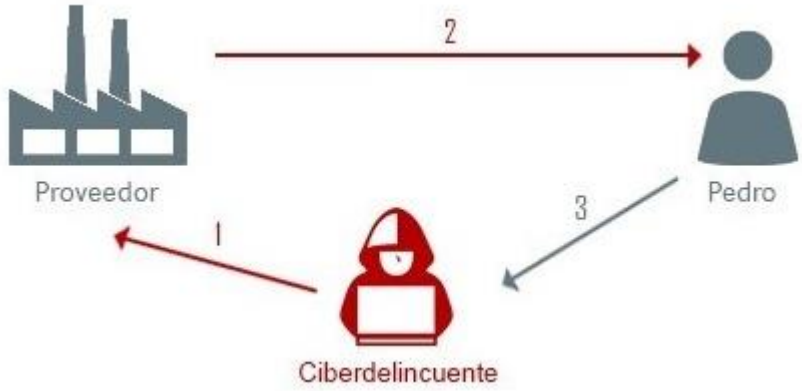
Con este nombre se conoce por una parte a la estafa que podemos sufrir, generalmente a través de un mensaje fraudulento de correo electrónico, con el que el ciberdelincuente pretende capturar de forma ilícita nuestros datos personales: como contraseñas de acceso a nuestros sistemas o datos de nuestras cuentas bancarias.
Y también se denomina así al ataque que sufrimos en nuestra web por el que cambian su aspecto para suplantar a una entidad a la que redirigen a los que pican en los mensajes fraudulentos que envían masivamente y que podrían ser enviados desde la página falsa de la entidad suplantada.

- Los ciberdelincuentes para engañar a las víctimas suelen suplantar la identidad de empresas y organizaciones reconocidas, comúnmente aquellas de las que pretenden robar la información, como por ejemplo, entidades bancarias o públicas, empresas del sector energético o de logística, etc.
- Los ciberataques de tipo phishing contienen en el cuerpo del mensaje un enlace que lleva a una página web fraudulenta, generalmente con la misma estética que la página web legítima a la que intenta suplantar.
- Para ofrecer más veracidad al fraude, la web fraudulenta suele utilizar un nombre de dominio similar al legítimo, siempre buscando como objetivo que las potenciales víctimas caigan en el engaño
- Una vez que la víctima del ataque ha facilitado toda la información que los ciberdelincuentes le solicitan, suele ser redirigida a la página web legítima de la empresa suplantada, con el fin de que el fraude pase el mayor tiempo desapercibido, hasta que la víctima se da cuenta.

1. PHISING – Cómo ocurre y cómo evitarlo

- Solemos recibir un email, una llamada telefónica o un mensaje SMS, que en realidad es un timo, con el que intentarán robarnos los datos personales, es decir, picaremos el anzuelo.
- Se debe concienciar a los usuarios para evitar que «piquen» en el anzuelo del email fraudulento y den por ese medio cualquier credencial que se les solicite.
- El responsable del correo debe mantener actualizados los filtros antispam y el software antivirus. Para detectar estas campañas lo antes posible y bloquearlas.
- Notificar al responsable del correo cualquier sospecha o correo extraño para su análisis.
- Ante cualquier duda, contactar con el remitente utilizando otro medio. Por ejemplo el teléfono.

2. BEC - BEC (del inglés Business e-Mail Compromise) o correo electrónico corporativo comprometido es un tipo de fraude contra empresas que realizan transferencias electrónicas de dinero.



El ciberdelincuente suplanta a uno de nuestros proveedores (Proveedor S.L.) e intercepta los correos de facturación que nos envía, cambiando la cuenta del banco donde realizar los pagos, de manera que hagamos una transferencia a una cuenta controlada por ellos.

Imaginaros que para el último pedido, una vez acordado el precio con el proveedor, hemos quedado en que nos van a enviar la factura por medio del correo electrónico para realizar la transferencia. Recibimos la factura y realizamos el pago al número de cuenta indicado en el correo recibido.

Pasados unos días, como no recibimos el pedido nos ponemos en contacto con Proveedor S.L. para reclamarlo. Una empleada de Proveedor S.L. nos indica que aún no han recibido el pago, requisito indispensable para realizar el envío.

Desde Pedro S.L. enviamos el justificante de la transferencia. Al comprobar el justificante, la empleada de Proveedor S.L. para reclamarlo. Una empleada de Proveedor S.L. nos advierte que ese no es su número de cuenta bancaria. ¿Qué ha sucedido? Puede ser que nuestra cuenta de correo o la de nuestro proveedor estén comprometidas, es decir, controladas por el ciberdelincuente.

ETL GLOBAL
Tax · Legal · Audit
DESPACHOS BK

BEC – ¿Que ha pasado?

CASO 1: Nuestra cuenta de correo está comprometida

El ciberdelincuente ha podido acceder a nuestra cuenta y ha creado una **regla de entrada en nuestro buzón de correo**. Esta regla, funciona reenviando todo el correo procedente de **facturacion @ proveedor . com**, a una cuenta de correo desconocida, **ciberdelincuente @ email . ru**, además, mueve el correo de la bandeja de entrada a una carpeta oculta, para que no lo detectemos.

Si revisamos las cabeceras del correo que hemos recibido con la cuenta bancaria modificada se detecta que la dirección desde la que se envió la factura es **facturacion @ proveedor . com**. El atacante ha creado un dominio muy parecido al de **Proveedor S.A.** para suplantar su identidad y cometer el fraude.

CASO 2: Cuenta de correo del proveedor comprometida

En este caso, **Proveedor S.A.** recibe llamadas de clientes que han recibido correos con facturas con el número de cuenta modificado, es decir, su correo está comprometido. Aparentemente los correos se envían desde la dirección legítima.

Se detecta una **regla de salida** en el buzón de correo de **Proveedor S.A.** que ellos no habían configurado. Esta regla, funciona interceptando todo el correo saliente con facturas hacia clientes, y los reenvía a una cuenta de correo desconocida, **ciberdelincuente @ email . ru**.

Es posible que su cuenta siga comprometida, ya que los correos a clientes están siendo enviados desde el correo legítimo. Es probable que el ciberdelincuente esté interceptando, toda la información que llega al buzón del proveedor para posteriormente acceder al **correo de facturación del proveedor** para cometer el fraude.

BEC – ¿Qué es la cabecera de un correo?

Un correo electrónico está formado por dos partes principalmente:
Las cabeceras: información de la transmisión del correo con la que podemos trazar el origen, destino, hora, asunto, filtrados de los servidores, etc.
El cuerpo: esta parte contiene el mensaje que queremos enviar al destinatario.

Desde nuestro gestor de correo (Por ejemplo Outlook), abrimos el correo en cuestión, y accedemos al menú ARCHIVO y hacemos click en PROPIEDADES. En la ventana que se abre podremos ver las cabeceras, seleccionarlas y copiarlas.

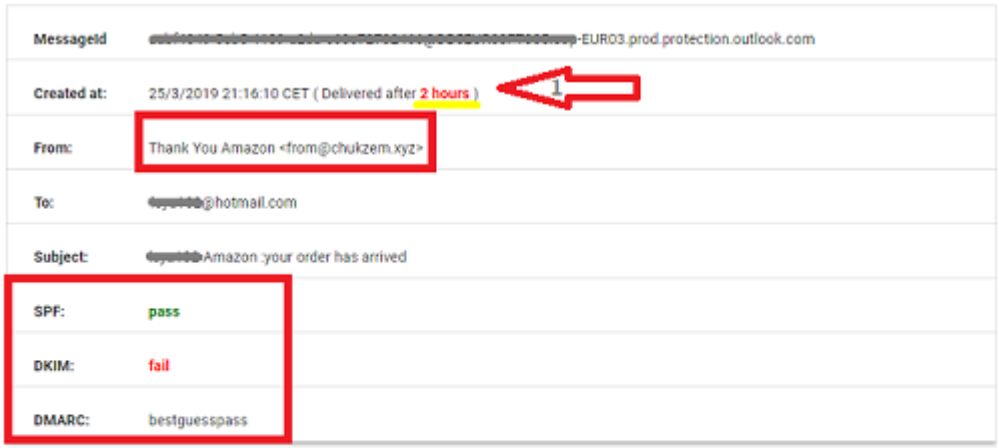
En la próxima diapositiva vemos detallada la cabecera de un correo fraudulento, comparada con uno veridico:

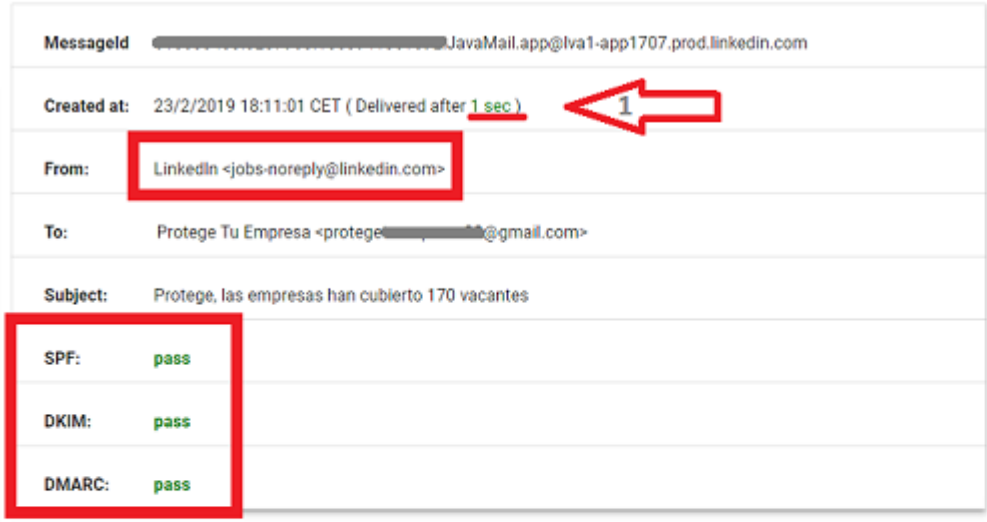
El correo fue entregado pasadas 2 horas, es decir, tardó 2 horas en llegar desde que se envió (en el último destacado pueden verse las direcciones de los servidores por las que pasa el correo hasta que es entregado).

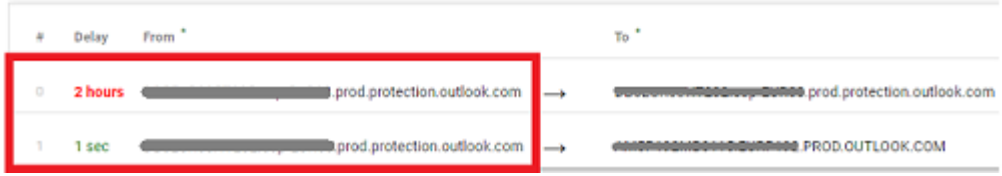
En el campo «From:» observamos que **el dominio chukzem.xyz no coincide con el supuesto emisor** del mensaje que en este caso dice ser una empresa de ventas online.

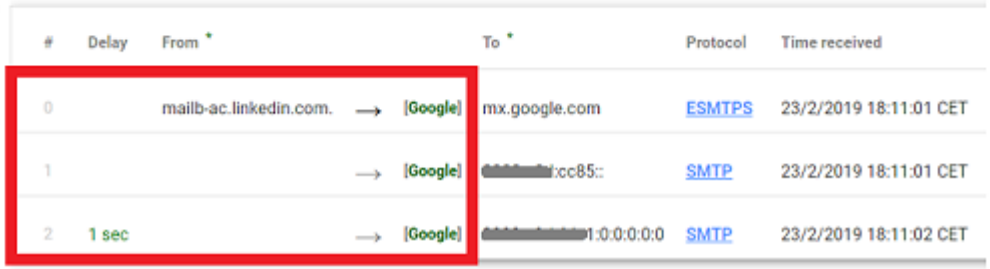
Los registros DKIM y DMARC no han pasado el control de verificación. Tanto el tiempo de entrega, como el remitente y los registros SPF, DKIM y DMARC nos están indicando que se trata de un claro ejemplo de email spoofing.

BEC – Comparación de cabeceras









BEC – Detalles de como ocurre y como evitarlo

- La víctima que está esperando un correo con la factura del proveedor, baja la guardia, presta menos atención y se confía, lo que hace que estos ataques sean muy efectivos. Además, es un fraude fácil para el ciberdelincuente pues puede obtener ingresos elevados y no precisa tener conocimientos avanzados,
- Los ciberdelincuentes recopilan datos sobre sus víctimas que luego usan para generar confianza. Entre otros, pueden utilizar nombres y cargos de los empleados, listas de correos de la web corporativa, redes sociales, filtraciones de terceros o mediante ingeniería social.
- En la mayoría de las ocasiones están varias semanas dentro del correo de la víctima, conociendo los pormenores de las operaciones antes de perpetrar el fraude, observan los correos y crean reglas específicas. Esperan a que llegue el momento oportuno para actuar, por ejemplo, cuando se espera una factura de un importe alto, hay un nuevo cliente o el responsable está de vacaciones
- Para evitarlo hay que “cuidar” el uso que hacemos del email corporativo. No utilizarlo para usos no profesionales (Redes sociales, concursos, compras, etc.) Evitar su uso en dispositivos no profesionales o no protegidos. Revisar periódicamente su configuración y cambiar las contraseñas. Estar alerta ante posibles fraudes masivos que suelen ser advertidos en medios de comunicación.
- Notificar al responsable del correo cualquier sospecha o correo extraño para su análisis.

DESPACHOS BK
ETL GLOBAL
Tax · Legal · Audit

PREGUNTAS A DEBATIR:

1. ¿Cuál es el objeto real del informe del perito de parte?, ¿Qué necesita el abogado?

2. ¿Está el usuario final (Cliente) preparado para afrontar esta pericial?

3. ¿Hacemos un uso responsable de las herramientas tecnológicas?

4. Correo electrónico. ¿Conocemos los riesgos?

5. Formación. ¿Están los profesionales implicados dispuestos a recibir la formación necesaria en este campo?

DESPACHOS BK
ETL GLOBAL
Tax · Legal · Audit

Seguimos sumando juntos

Bilbao – Burgos – Logroño – Miranda de Ebro
Oviedo – Salamanca - Vitoria-Gasteiz - Zamora

www.bketl.es