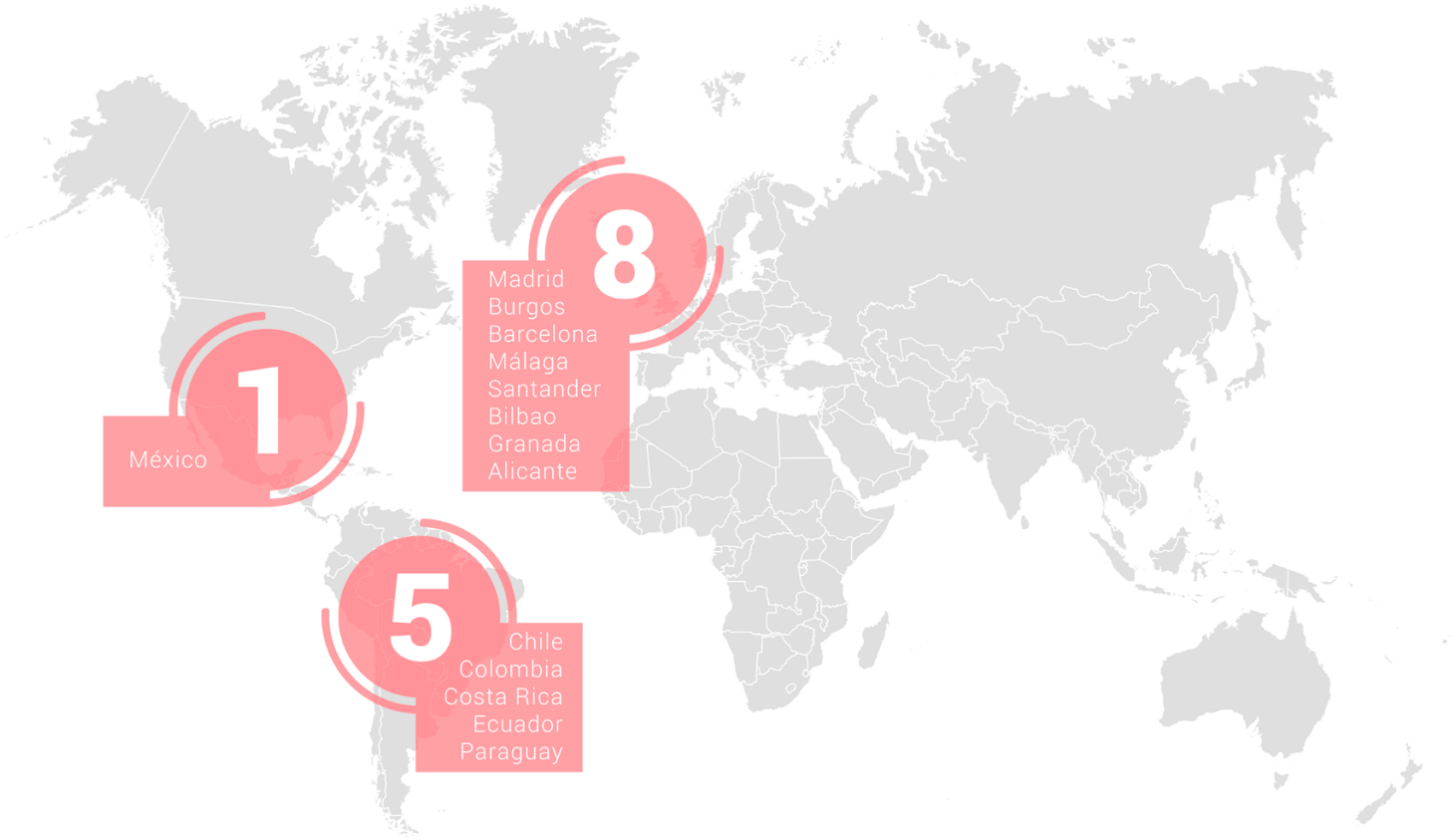
GrupoACMS
CONSULTORES

GRUPO ACMS Consultores

Qué es Spoofing y Phishing: Ciberseguridad en la Empresa



AENOR
ER
Empresa Registrada
ISO 9001

(ER-0772/2013)

Alcance ISO 9001

Diseño, desarrollo, implantación, formación y mantenimiento de sistemas de gestión de la calidad, medioambiental, de la prevención de riesgos laborales, protección de datos, seguridad alimentaria y de la calidad y competencia técnica en laboratorios clínicos.

Alcance ISO 27001

Los sistemas de información que dan soporte a las actividades de diseño, desarrollo, implantación, formación y mantenimiento de sistemas de gestión y el diseño, desarrollo y comercialización de software de sistemas de gestión de acuerdo con la declaración de aplicabilidad vigente.

AENOR
ER
Seguridad Información
ISO/IEC 27001

(SI-0021/2020)

Publicado el 18/02/2021

Recomendaciones para evitar problemas de Ciberseguridad en la Empresa

A través de un claro ejemplo vamos a explicar cuál es la mejor manera de evitar tanto el spoofing y como el phishing en la empresa y aportaremos las recomendaciones necesarias para que no vuelva a ser víctima de una estafa y engaño a través de internet.

Ataque al departamento financiero por Ciberdelincuentes

Vamos a contar la historia de Jose Antonio, responsable de pago de una empresa del sector de la construcción.

Jose Antonio tiene entre otras responsabilidades el pago de proveedores, nóminas y demás gastos de la organización. Normalmente tiene planificado los ingresos y gastos, pero siempre se presenta algún pago que tiene que realizar con urgencia, al margen de la planificación.

Una mañana de lunes, cuando estaba intentando conectarse a la triste realidad de la semana que tenía por delante, recibió un email del director de la empresa indicando que tenía que pagar con urgencia 70.000 euros a un nuevo proveedor. En el email se indicaba que era realmente urgente y de vital importancia para la empresa. Además, figuraba un número de cuenta.

Dado que el director de la empresa no era la primera vez que exigía pagos con cierta urgencia, Jose Antonio ni lo dudo, se metió por internet en las cuentas del banco y procedió a realizar la transferencia.

De ese lunes José Antonio se acordaría toda su vida. Al final de la mañana, cuando el CEO le llamó para otro asunto, le comentó que ya había realizado el pago de los 70.000 euros que le había pedido por email.

El director no sabía de qué estaba hablando. El no había enviado ningún email.

¿Qué ocurrió ese fatídico lunes?

Tanto José Antonio como el director de la compañía fueron víctimas de una técnica de los ciberdelincuentes denominada spoofing. Consiste en la Falsificación de la dirección de correo electrónico o la URL de una organización para hacerse pasar por ella, de modo que el usuario crea que la comunicación que le envían es legítima y caiga en el engaño, proporcionando sus credenciales de acceso y datos personales.

Mediante información que sin darnos cuenta vamos publicando en internet los ciberdelincuentes investigan quienes son los directivos de las empresas, los responsables del departamento financiero, etc.

En este caso lo ciberdelincuentes se hicieron pasar por el director de la compañía y pidieron un pago de urgencia a un número de cuenta. La empresa perdió 70.000 euros en un momento.

José Antonio y el director se pusieron en contacto con el Banco para confirmar el fraude y acto seguido denunciaron el hecho a las Fuerzas y Cuerpos de Seguridad del Estado.

¿Cómo se pueden evitar este tipo de problemas de Ciberseguridad?

Cada vez es más común este tipo de ciberataques a las empresas. Las organizaciones se tendrían que tomar más en serio este tipo de riesgos y luchar por evitarlos.

Se pueden tomar muchas soluciones puntuales pero consideramos que sería bueno implantar un sistema de seguridad de la información bajo la Norma ISO 27001 para ver los riesgos y posibles soluciones en su conjunto.

En este caso en particular se habría evitado el problema si el personal de la organización hubiese recibido cursos de concienciación sobre seguridad de la información. De esta manera habría conocido de la existencia de técnicas como el spoofing o el phishing y José Antonio habría podido dudar del email del director que con urgencia exigía el pago de una fuerte suma de dinero.

Por otra parte, la organización podría haber documentado, como parte del sistema de seguridad ISO 27001 un protocolo de pagos. En este protocolo, porejemplo, se podría indicar que para importes superiores a 3.000 euros, los pagos requieren una segunda confirmación del solicitante del pago mediante teléfono.

Las empresas pueden gastar grandes cantidades de dinero en antivirus y otras soluciones tecnológicas, pero deben tener en cuenta que la parte más vulnerable es el usuario. Es necesario contar con su participación y concienciarle de los riesgos de seguridad de la información a los que se enfrenta la organización en su día a día.

Consultoría de Ciberseguridad

Si necesita asesoramiento personalizado no dude en contactar con nuestros expertos en Seguridad de la Información. En Grupo ACMS Consultores nos avalan más de 20 años de experiencia y podemos brindarle toda la ayuda que necesite.

Formación relacionada con Seguridad de la Información

Nos definimos como una compañía consultora independiente cuyo objetivo fundamental es suministrar servicios de consultoría en las áreas de Gestión empresarial, que representen para el cliente una solución excelente, que satisfaga sus necesidades explícitas o implícitas, tenga en cuenta las regulaciones y normas aplicables, y cumpla los objetivos de plazo y coste establecidos.

Madrid

C/ Campezo 3, nave 5 28022 Madrid

Tfno.: (+34) 91 375 06 80

Burgos

Centro de Empresas, 73 09007 Burgos

Tfno.: (+34) 947 041 645

Barcelona

C/ Plaça Universitat 3 08007 Barcelona

Tfno.: (+34) 93 013 19 49

Málaga

C/ Alejandro Dumas 17 29004 Málaga

Tfno.: (+34) 95 113 69 04

México

José González Varela 15 14700 Tlalpan

Tfno.: (+52) 5513 39 96 22

www.grupoacms.com
informacion@grupoacms.com