Vuelta a la actividad: cómo proteger a tu empresa frente a estafas por correo (BEC)

Con el inicio del año y la vuelta a la actividad a pleno rendimiento, las empresas retoman proyectos, pagos a proveedores, cierres contables y nuevas operaciones. Este contexto de mayor volumen de trabajo y urgencias es, precisamente, uno de los momentos preferidos por los ciberdelincuentes para lanzar ataques dirigidos a las organizaciones.

Uno de los fraudes más habituales y con mayor impacto económico en el entorno empresarial es el **Business Email Compromise (BEC)** o **Correo Corporativo Comprometido**.

¿Qué es un ataque BEC?

Se trata de un tipo de estafa en la que los atacantes **suplantan la identidad de directivos, empleados o proveedores de confianza**, o bien acceden de forma ilegítima a cuentas reales de correo corporativo, con el objetivo de engañar a la empresa y provocar transferencias económicas, cambios de cuentas bancarias o la cesión de información sensible.

A diferencia de otros ataques más masivos, los BEC son **fraudes muy personalizados**, basados en el conocimiento previo de la organización y en la confianza entre las personas que forman parte de ella.

¿Cómo operan los estafadores?

Los atacantes suelen emplear técnicas de ingeniería social combinadas con accesos no autorizados a correos electrónicos. Algunas de las estrategias más comunes son:

- Solicitudes urgentes de transferencias bancarias aparentando ser un directivo de la empresa.
- Envío de facturas falsas o modificaciones de datos bancarios de proveedores habituales.
- Correos enviados desde cuentas reales comprometidas, lo que dificulta su detección.
- Peticiones dirigidas a departamentos financieros o de recursos humanos para obtener información sensible.

Señales de alerta a tener en cuenta

Existen ciertos indicios que pueden ayudar a detectar este tipo de estafas:

- Cambios inesperados en las instrucciones de pago o en los datos bancarios.
- Mensajes que transmiten urgencia o presión para actuar rápidamente.
- Solicitudes que se salen de los procedimientos habituales de la empresa.
- Pequeñas variaciones en la dirección de correo del remitente o en el dominio.

¿Cómo puede protegerse tu empresa?

Algunas medidas clave para reducir el riesgo de sufrir un ataque BEC son:

- Verificar por un canal alternativo cualquier solicitud de pago o cambio de cuenta bancaria.
- Implantar autenticación multifactor (MFA) en el acceso al correo corporativo.
- Formar y concienciar a los equipos sobre este tipo de fraudes.
- Definir protocolos claros para autorizaciones y validaciones internas.

¿Necesitas ayuda?

Desde **Binaura – Grupo Monlex**, ayudan a las empresas a **reforzar su seguridad digital**, evaluar riesgos y definir medidas técnicas y organizativas para prevenir este tipo de estafas.

Si deseas más información o asesoramiento, puedes contactar con su equipo escribiendo a: info@binaura.es

La prevención y la concienciación son clave para empezar el año con una empresa más segura.