WHITE PAPER CIPHRAVERSE

Fraude del CEO: cómo funciona y cómo se corta

El fraude del CEO es un fraude por correo electrónico conocido como BEC: alguien se hace pasar por un directivo o un proveedor y pide una transferencia urgente o un cambio de cuenta bancaria. No hace falta malware: el ataque se dirige a las personas y al proceso de pago, y por eso el antivirus y el cortafuegos no lo detienen.

Cómo se monta el engaño

El atacante investiga la empresa en LinkedIn y en la web corporativa: quién firma los pagos, cuándo viaja el gerente. Elige ese momento para escribir, a menudo desde una dirección muy parecida a la real o desde una cuenta ya comprometida. El mensaje pide algo urgente y confidencial: una transferencia a un proveedor nuevo, un pago anticipado, o el cambio de cuenta bancaria de un proveedor habitual. A veces sigue una llamada para reforzar la presión.

Por qué elude los controles técnicos

No hay archivo adjunto malicioso ni enlace que analizar. Si la cuenta del directivo fue comprometida antes por phishing, el correo es auténtico y pasa cualquier filtro. El ataque explota la jerarquía y la urgencia, no una vulnerabilidad técnica, así que ninguna herramienta de seguridad perimetral lo va a frenar por sí sola.

Los controles que funcionan

- Verificación fuera de banda: confirmar todo pago o cambio de cuenta bancaria por un canal distinto al del mensaje, llamando a un número ya conocido, nunca al que aparece en el correo.
- Doble autorización: ningún pago por encima de un umbral definido sale sin la aprobación de una segunda persona.
- Cultura donde decir que no al jefe está bien: quien duda de un pago o lo retrasa para verificarlo no debe temer consecuencias.
- Procedimiento fijo para cambios de cuenta bancaria de proveedores: toda modificación se confirma por teléfono con un contacto conocido antes de tocar los datos de pago.

Ninguno de estos controles requiere presupuesto de tecnología. Define hoy quién autoriza los pagos por encima de un umbral y cómo se verifica un cambio de cuenta bancaria antes de mover un euro.