COMPROMISO DE CORREO (BEC) · PAGOS INTERNACIONALES

PAGÓ A UN PROVEEDOR QUE NO EXISTÍA. LA COMA DELATÓ AL COPISTA.

DOS CORREOS EL MISMO DÍA PIDIENDO EL PAGO: UNO VERDADERO, UNO IDÉNTICO — CON LA MISMA COMA MAL PUESTA

> **QUIEN FABRICÓ EL CORREO FALSO COPÓ EL TEXTO DEL VERDADERO CON SU ERROR Y TODO.**

Análisis de fuentes abiertas sobre el dominio apócrifo: la infraestructura del fraude al descubierto.

EL PROBLEMA

Una empresa compraba insumos a un gran fabricante extranjero, con el mismo contacto comercial de siempre. Un otoño, el contacto avisó por correo del cambio de las cuentas bancarias para los pagos. La empresa pagó varias veces, notificando cada pago, hasta que el fabricante real reportó —semanas después— que ellos jamás habían cambiado de cuenta.

Para entonces, los pagos habían salido a destino desconocido. El peritaje empezó por la prueba reina, y estaba a la vista de todos.

LA INTERVENCIÓN

El mismo día, con horas de diferencia, llegaron dos correos pidiendo el pago: uno de la cuenta verdadera y otro de una cuenta idéntica salvo por el dominio —uno de esos dominios baratos que se compran en minutos—. Ambos abrían con el mismo primer párrafo. No parecido: idéntico, incluido un error de redacción del original. Y el remitente llegaba maquillado: mostraba la dirección verdadera como nombre visible, pero la cuenta real de envío era la apócrifa.

El análisis del dominio con fuentes abiertas abrió la segunda escena: el dominio apócrifo vivía en un servidor compartido con decenas de dominios más, todos registrados por la misma mano — uno por empresa a suplantar, esperando su turno. Y el golpe que duele: el impostor adjuntó estados de cuenta con fechas, partidas y precios que solo conocían empleados de ambas empresas. Eso no se inventa: hubo una brecha previa de información.

La cronología de notificaciones cerró el caso: la empresa avisó del cambio de cuentas a sus contactos reales y nadie alertó nada; pagó y notificó cada pago a las cuentas apócrifas; y el fabricante negó el cambio semanas después del primer aviso.

Caso anonimizado para proteger la identidad de las partes. Los detalles técnicos se describen a nivel general.

TODO CAMBIO DE CUENTA SE CONFIRMA POR UN CANAL DISTINTO AL CORREO QUE LO ANUNCIÓ.

Y LA ALARMA NO SE APAGA PORQUE EL SUPUESTO PROVEEDOR RESPONDA CON CALMA

QUÉ SE LOGRÓ

Gracias al análisis forense, la empresa documentó en su investigación la anatomía completa del fraude: el correo gemelo con su error copiado, la infraestructura de dominios del mismo dueño, la brecha previa de información y el silencio semanas del fabricante — cada pieza con su evidencia verificable.

> **La regla que debería estar pegada en toda tesorería: semanas de silencio del proveedor real no son descuido — son el precio de no verificar por un segundo canal.**

POR QUÉ DURIVA ES LA MEJOR OPCIÓN

≡

EFICIENCIA

Metodología propia probada en miles de dictámenes, con equipos que trabajan en paralelo sobre la evidencia.

TIEMPO

Respuesta ágil en escenarios de urgencia procesal, con la misma calidad técnica y documentación completa.

18

TRAYECTORIA

Más de 18 años de cómputo forense en México y América Latina. Creador del primer sistema operativo forense latinoamericano, presidente del Consejo Americano de Ciberseguridad y Cómputo Forense, autor de seis libros especializados.

Si su proveedor cambia de cuentas por correo, confirme por otro canal antes de pagar. Somos su aliado digital.

Caso anonimizado para proteger la identidad de las partes. Los detalles técnicos se describen a nivel general.