COMPROMISO DE CORREO (BEC) · PAGOS INTERNACIONALES

FALTABA UNA LETRA EN EL DOMINIO. NADIE LA VIO.

AÑOS PAGANDO A SU PROVEEDOR DE SIEMPRE, HASTA QUE LOS CORREOS EMPEZARON A VENIR DE OTRO LADO

LOS EMPLEADOS NO HABÍAN SIDO HACKEADOS: HABÍAN SIDO LEÍDOS.

Copias forenses certificadas de los equipos: sin malware, sin infección — el ataque fue de lectura.

EL PROBLEMA

Una empresa llevaba años pagando facturas a su agente en el extranjero: la misma operación de rutina, con la misma persona al otro lado del correo. Un verano, los correos del pago empezaron a venir de esa misma persona pero con una diferencia casi invisible en el dominio: faltaba una letra.

Nadie la vio. Los pagos siguieron su curso hasta que el agente real avisó que no le había llegado nada.

LA INTERVENCIÓN

El análisis forense de los equipos de los dos empleados que manejaban los pagos se hizo en sitio, con copias certificadas y huella digital. Los equipos quedaron limpios: aplicaciones, programas, registros y la tabla maestra de archivos del disco —ese registro que documenta todo lo que ha existido en el equipo— sin rastro de malware ni de accesos no autorizados.

La cronología del engaño, reconstruida de los correos, era de manual: la cuenta apócrifa pedía pagos con datos exactos de las facturas —números, fechas, montos que solo conocía quien estaba dentro de la operación—, envió una tabla de pendientes idéntica a la del agente real, adjuntó los «nuevos» datos bancarios y hasta notificó «no haber recibido» un pago para presionar. Cuando la empresa pidió verificar, la cuenta real respondió que no existía cambio alguno; y solo entonces, días después de realizados los pagos, se reportó el detalle del dominio.

Y la falla estructural más grave: el nombre del agente no estaba registrado como marca en ningún país — cualquiera podía abrir una empresa, y una cuenta bancaria, con ese nombre. El atacante no falsificó una empresa: simplemente la creó.

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

EL FRAUDE VIVE EN UNA LETRA.

LEER EL DOMINIO COMPLETO, LETRA POR LETRA, DE LOS CORREOS QUE PIDEN CAMBIAR UNA CUENTA

QUÉ SE LOGRÓ

Gracias al análisis forense, la empresa documentó en su investigación la mecánica completa del fraude: equipos limpios, brecha de información en la cadena de proveedores, dominio apócrifo con identidad oculta y la lección registrada — el ataque fue de lectura, no de infección.

> **La enseñanza es triple: lea el dominio completo de los correos que piden cambiar una cuenta; registre la marca de su negocio, porque si el nombre no existe, cualquiera puede usarlo; y cuando un proveedor anuncie cambios bancarios, la confirmación se hace por otro canal — siempre, sin excepción.**

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 sus pagos salen por correo, una letra puede costarle el año: verifique por otro canal. Somos su aliado digital.

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