COMPROMISO DE CORREO (BEC) · FRAUDE EMPRESARIAL

EL FRAUDE SE MONTÓ DENTRO DE SU PROPIO CORREO. Y NADIE REVISA LAS REGLAS DE BUZÓN.

EL ATACANTE NO ROBA LA CONTRASEÑA PARA LEER: LA USA PARA CONFIGURAR EL TEATRO

> **UNA REGLA DE BUZÓN CREADA DESDE UNA DIRECCIÓN EXTRANJERA ES, EN LA PRÁCTICA, LA FIRMA DEL ATACANTE DEJADA EN LA ESCENA.**

Auditoría completa de la plataforma de correo: eventos, alias, delegados y reglas.

EL PROBLEMA

Una empresa detectó a tiempo una de esas pérdidas que solo se notan cuando el proveedor llama para cobrar lo que ya se pagó: alguien había pedido por correo el cambio de la cuenta bancaria para el pago de una factura, haciéndose pasar por la propia empresa.

La duda era dónde había estado el agujero, y la respuesta no estaba en el antivirus: estaba en los registros de la plataforma de correo.

LA INTERVENCIÓN

El peritaje pidió algo que casi ninguna empresa sabe que puede pedir: una cuenta con permisos de auditoría dentro de la plataforma de correo. Con ese acceso se exportó la totalidad de los eventos de la cuenta comprometida —la plataforma guarda el historial, aunque solo por tiempo limitado— y primero se verificó que no hubiera alias ni permisos delegados para enviar en su nombre.

Después vino la geografía de los accesos: casi todas las conexiones venían de la dirección habitual de la empresa, pero en medio de la rutina aparecía una serie de accesos desde otro continente. Y desde una de esas direcciones se habían creado reglas de buzón con filtros específicos: reglas que se activaban cuando un correo incluía ciertos nombres y el dominio de la operación.

Esa es la mecánica completa del fraude: el atacante desvía o esconde los correos que hablan de pagos, y la víctima ve una conversación recortada sin saberlo. El proveedor cobra, la empresa paga, y nadie nota que las instrucciones nunca salieron del proveedor real.

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

AUDITAR TARDE ES NO AUDITAR.

LOS EVENTOS DE LA PLATAFORMA SE CONSERVAN POR TIEMPO LIMITADO

QUÉ SE LOGRÓ

Gracias a la auditoría de la plataforma, la empresa documentó en su investigación interna el vector exacto del fraude: accesos desde el extranjero y reglas de buzón creadas por el atacante para recortar la conversación — con la respuesta técnica precisa a la pregunta «¿quién creó esas reglas?».

> **La enseñanza es de rutina barata: una vez al mes, revise las reglas de buzón de las cuentas que pagan y las que cobran. Nadie las revisa porque nadie las ve; el atacante lo sabe, y por eso empieza exactamente ahí.**

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 empresa paga por correo, revise hoy las reglas de buzón: el atacante ya sabe que usted no las mira. Somos su aliado digital.

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