CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

CIBERINCIDENTES EN NIVELES DIRECTIVOS Y DE GESTIÓN CRÍTICA

ANTECEDENTES

El funcionamiento de los negocios y servicios dependen, en gran medidad, de tomadores de decisiones, pero también de quienes ejecutan esas decisiones en la organización, y los cibercriminales son conscientes de eso.

Los **niveles directivos y de gestión crítica** de empresas, industrias, bancos, entidades financieras y organizaciones gubernamentales son algunos de los **blancos predilectos** para los ciberatacantes.

Los **ataques dirigidos a estos blancos involucran a quien toma la decisión y quien gestiona la decisión**, y explota la relación de confizan o la costumbre para comenter un fraude.

Este tipo de incidentes explota una **vulnerabilidad que yace en la relación cotidiana de directivos y administradores de los negocios** para inducir a errores que pueden traer serias consecuencias.

BEC | COMPROMISO DE CORREO EMPRESARIAL

Se trata de un ciberataque en el que el estafador utiliza un correo electrónico haciéndose pasar por alguien de autoridad o de confianza en un organización para engañar a otros, especialmente en mandos medios, para que realicen envíos de dinero o divulguen información sensible de la entidad.

Los atacantes suelen concentrarse en objetivos financieros de las organizaciones y diseñan estrategias para recolectar información de sus víctimas, como quienes son los responsables de las transferencias de dineros (pagos) y los canales que utilizan para ese propósito, ello con el fin de encontrar y explotar vulnerabilidades.

CSIRT

CIBERINCIDENTES EN NIVELES DIRECTIVOS Y DE GESTIÓN CRÍTICA

BLANCOS DE ATAQUE

- Ejecutivos y líderes, porque los detalles sobre ellos a menudo están disponibles públicamente en el sitio web de la empresa, por lo que los atacantes pueden pretender conocerlos.
- Empleados de finanzas y personal de cuentas que tienen detalles bancarios, métodos de pago y números de cuenta.
- Gerentes de Recursos Humanos con registros de empleados, declaraciones de impuestos, información de contacto y horarios.
- Empleados nuevos o de nivel de entrada que no podrán verificar la legitimidad de un correo electrónico con el remitente.

TIPOS DE ATAQUES BEC

Los atacantes se basan principalmente en tácticas de ingeniería social para engañar a empleados y ejecutivos desprevenidos. A menudo, se hacen pasar por el director ejecutivo o cualquier ejecutivo autorizado para ordenar o realizar transferencias electrónicas. Además, los estafadores también investigan cuidadosamente y monitorean de cerca a sus posibles víctimas y sus organizaciones.

1. Esquema de factura falsa
2. Fraude del CEO
3. Compromiso de cuenta
4. Suplantación de identidad del abogado
5. Robo de datos

ESQUEMA DE FACTURA FALSA

Los atacantes se hacen pasar por un proveedor legítimo que presta servicios a la organización y envían un correo electrónico que se asemeja a uno real.

El correo se trata de una factura falsa que parece legítima y se solicita el pago de servicios a una cuenta que pertenece o es controlada por los estafadores.

FRAUDE DEL CEO

Este ataque se aprovecha de la relación de poder o las costumbres dentro de una empresa.

El atacante falsificará la cuenta del CEO o una persona del nivel directivo y enviará un correo electrónico instruyendo al destinatario -por lo general, del área de finanzas o un mando medio,e incluiso a otro empleado- para que ejecute una compra o envie dinero mediante una transferencia bancaria.

COMPROMISO DE CUENTA

Los atacantes toman control de una cuenta de correo electrónico de un ejecutivo o empleado y la utilizan para solicitar pagos de facturas a los proveedores que figuran en sus contactos de correo electrónico.

Luego, los pagos se envían a cuentas bancarias fraudulentas.

SUPLANTACIÓN DE INDENTIDAD DEL ABOGADO

Este tipo de ataque se aprovecha del hecho de que es probable que los empleados dentro de una organización cumplan con las solicitudes de un abogado o representante legal porque no saben cómo validar la solicitud.

ROBO DE DATOS

Este tipo de ataque se dirige al personal de Recursos Humanos y Finanzas que administra datos de los miembros de la organización.

El objetivo es robar información confidencial sobre las personas que pertenecen a la entidad para luego venderla en la Dark Web o para se utilizada en un futuro ataque.

CSIRT

CIBERINCIDENTES EN NIVELES DIRECTIVOS Y DE GESTIÓN CRÍTICA

DATOS Y CIFRAS DEL BEC

DATOS Y CIFRAS DEL BEC

CSIRT | CIBERINCIDENTES EN NIVELES DIRECTIVOS Y DE GESTIÓN CRÍTICA

28 % El promedio de miembros de una organización que abren un correo BEC

63 % Probabilidad de que una empresa grande experimente un ataque BEC

2 % El total de los ataques BEC que son reportados

81 % Aumentaron los ataques BEC durantes el segundo semestre de 2022

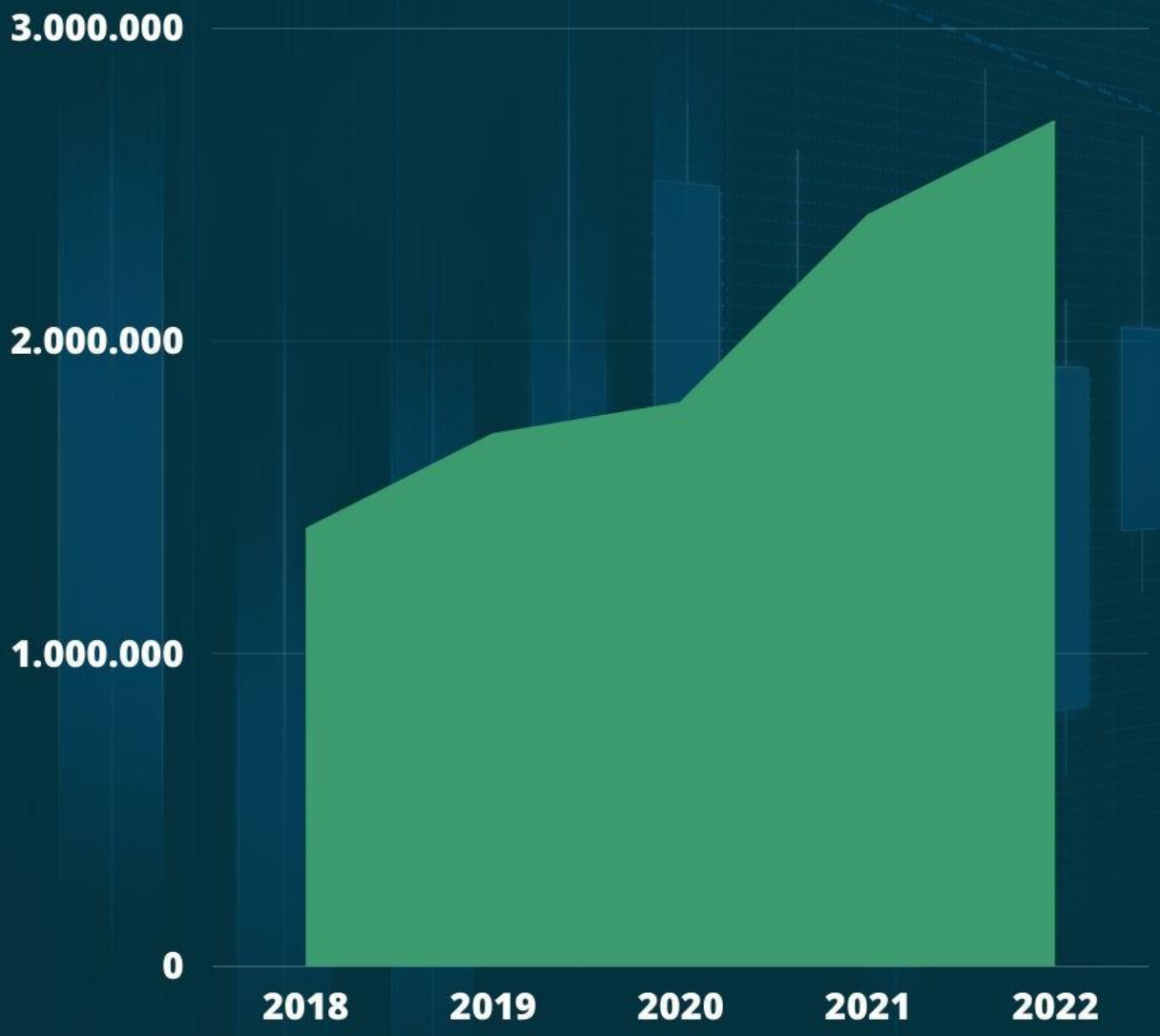
65 % Aumentaron las pérdidas globales por ataques BEC

36 % De personas que respondieron un ataque BEC habían sido comprometidos en un ataque anterior

10 % El número de víctimas de los ataques BEC crece año tras año, casi un 10%.

90 % Empresas españolas experimentaron BEC en 2022, 13% más que 2021. Aumenta so del español en estos ataques.

PÉRDIDAS ECONÓMICAS



Los ataques BEC suponen unas pérdidas casi 80 veces mayores que las del ransomware.

2,7 billones de dólares en péridas el 2022

INCIDENTES DESTACADOS

#1

2013-2015
Facebook y Google: estafa BEC de $ 121 millones

2014
Scouler Co. (USA): estafa de adquisición de $ 17,2 millones

#2

2015
Ubiquiti: fraude de proveedores de $46,7 millones

2016
Violación de información de nómina de Snapchat. Robo de datos

2018
Save the Children (organización benéfica): $1 millón

2019
Parroquia St. Ambrose en Ohio (USA): $1.75 millones

#3

2019
Toyota: ataque BEC de $ 37 millones

2020
Gobierno de Puerto Rico: transferencia de $2.6 millones

2021
Empresario Obinwanne Okeke: $11 millones en pérdidas

2021
Treasure Island (Organización benéfica para personas sin hogar): pérdida de $ 625,000

2022
Banco Central de Chile
$ 205 mil dólares en pérdidas

CSIRT

CIBERINCIDENTES EN NIVELES DIRECTIVOS Y DE GESTIÓN CRÍTICA

CSIRT

CIBERINCIDENTES EN NIVELES DIRECTIVOS Y DE GESTIÓN CRÍTICA

LA AMENAZA DE BEC EN EL SECTOR PÚBLICO

AMENAZA DEL BEC EN EL SECTOR PÚBLICO

- Los registros de incidentes acumulados no son muchos, pero son severos. El caso público más conocido afectó al Banco Central en 2022 y dejó $ 205.000 dólares en pérdidas.
- En la mayoría de los eventos reportados, los miembros de la organización advirtieron un error en forma oportuna.
- Las organizaciones que cuentan con sistemas de control interno tienen mejores chances de advertir un ataque BEC.
- La entidades que concentran el rol de gestión financiero en una sola persona, son más propensos a ser víctimas de un BEC.
- CSIRT puede asegurar que esta amenaza está en aumento en los últimos meses y sus consecuencias económicas son altas.

CSIRT

CIBERINCIDENTES EN NIVELES DIRECTIVOS Y DE GESTIÓN CRÍTICA

¿CÓMO NOS PROTEGEMOS DEL BEC?

CAPACITACIÓN Y ENTRENAMIENTO

Los ataques BEC se dirigen a los miembros de una organización, lo que hace que la capacitación en concientización sea fundamental para la ciberseguridad de la empresa o servicio.

Capacitar a los miembros de la organización, desde los líderes hasta los empleados, sobre cómo identificar y responder a un ataque BEC es esencial para minimizar la amenaza de esta forma de phishing. Asegúrese de que todos sepan cómo detectar enlaces de phishing, un dominio y una dirección de correo electrónico que no coinciden, y otras señales de alerta.

Realice simulaciones de ataques BEC para que las personas reconozcan una cuando suceda.

SEPARACIÓN DE FUNCIONES

Los ataques BEC intentan engañar a los miembros de una organización para que realicen una acción específica (como enviar dinero o información confidencial) sin verificar el origen de la solicitud. La implementación de políticas para estas acciones que requieren la verificación de la orden puede ayudar a disminuir la probabilidad de un ataque exitoso.

AUTENTICACIÓN DE DOS FACTORES

Configure la autenticación de dos factores (o de múltiples factores) en cualquier cuenta que lo permita y nunca la desactive.

CSIRT

CIBERINCIDENTES EN NIVELES DIRECTIVOS Y DE GESTIÓN CRÍTICA

FORTALEZCA POLÍTICAS DE CONTRASEÑA

Revise y fortalezca la Política de Contraseñas de su organización y la suya propia, considerando, por ejemplo, elevar el largo de las contraseñas míni- mas.

CSIRT

CIBERINCIDENTES EN NIVELES DIRECTIVOS Y DE GESTIÓN CRÍTICA

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CORREO: SOC@INTERIOR.GOB.CL
FORMULARIO: WWW.CSIRT.GOB.CL
TELÉFONO: 1510

¿Y SI MI ORGANIZACIÓN FUE VÍCTIMA DE BEC?

Ante la hipótesis probable de que el vector de entrada por medio del cual fueron capturadas las credenciales de los usuarios fue algún tipo de spear phishing , se sugirie reforzar con una campaña interna de concientización sobre este tipo de incidentes. Se sugiere utilizar material que ya ha generado con este fin el CSIRT de Gobierno, y que este tipo de campañas internas se mantenga en el tiempo.

CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática