BEC (*Business Email Compromise*) y los ataques de Phishing se están volviendo complejos

Los ataques BEC y Phishing se han convertido en el método más común que utilizan los delincuentes cibernéticos para atacar a las personas en el trabajo y en el hogar. Los ataques BEC y Phishing eran tradicionalmente correos electrónicos enviados por los atacantes para engañarlo y hacer algo indebido, como abrir un archivo adjunto de correo electrónico infectado, hacer clic en un enlace malicioso o compartir su contraseña. Si bien los ataques tradicionales continúan hoy en día, muchos ciberdelincuentes están creando BEC avanzados y correos electrónicos de phishing que son más personalizados y más difíciles de detectar. También están utilizando tecnologías como herramientas de inteligencia artificial, mensajes de texto, redes sociales o incluso llamadas telefónicas para engañarlo. Aquí las últimas técnicas y cómo puedes detectarlos.

Los ciberdelincuentes están haciendo su investigación

Los correos electrónicos BEC y Phishing solían ser más fáciles de detectar porque eran mensajes genéricos enviados a millones de personas al azar. Los ciberdelincuentes no tenían idea de quién sería la víctima; simplemente sabían que cuantos más correos electrónicos enviaban más personas podían engañar. A menudo podíamos detectar estos ataques más simples al buscar correos electrónicos extraños con frases como "Estimado cliente", faltas de ortografía o mensajes que eran demasiado buenos para ser verdad, como príncipes nigerianos que ofrecían millones de dólares.

Los ciberdelincuentes de hoy son mucho más sofisticados. Ahora investigan a sus posibles víctimas para crear un ataque más personalizado. En lugar de enviar un correo electrónico de phishing a cinco millones de personas o que parezcan correos electrónicos genéricos enviados por empresas, lo envían solo a cinco personas y adaptan el ataque para que parezca enviado por alguien que conocemos. Los ciberatacantes logran esto al hacer lo siguiente:

- Investigan nuestros perfiles de LinkedIn, lo que publicamos en las redes sociales o utilizando información que está disponible públicamente o que se encuentra en la *Dark Web*.
- Elaboran mensajes que parecen provenir de compañeros de trabajo o proveedores que conoce y con los que trabaja.
- Aprenden cuáles son sus pasatiempos y envían un mensaje haciéndose pasar por alguien que comparte un interés común.
- Investigan si acaba de regresar de un viaje y luego redactan un correo electrónico que haga referencia al viaje.

Los ciberdelincuentes están utilizando otros métodos para enviar los mismos mensajes como mensajes de texto o incluso llamadas por teléfono.

Cómo Detectar Los Ataques BEC (*Business Email Compromise*) Avanzados

Debido a que los atacantes cibernéticos se toman su tiempo e investigan a sus posibles víctimas, puede ser más difícil detectar. La buena noticia es que aún puede detectarlos si sabe lo que está buscando. Hágase las siguientes preguntas antes de tomar medidas sobre un mensaje sospechoso:

1. ¿El mensaje crea un sentido de urgencia? ¿Estás siendo presionado para eludir las políticas de seguridad de su organización? ¿Te están apresurando a cometer un error? Cuanto mayor sea la presión o el sentido de urgencia, más probable es que se trate de un ataque.

2. ¿Tiene sentido el correo electrónico o mensaje? ¿El director ejecutivo de su empresa le enviaría un mensaje de texto urgente pidiéndole ayuda? ¿Su supervisor realmente necesita que se apresure a comprar tarjetas de regalo? ¿Por qué su banco o compañía de tarjeta de crédito le pediría información personal que ya debería tener? Si el mensaje parece extraño o fuera de lugar, puede ser un ataque.

3. ¿Está recibiendo un correo electrónico relacionado con el trabajo de un compañero de trabajo de confianza o quizás de su supervisor, pero el correo electrónico está utilizando una dirección de correo electrónico personal como @gmail.com?

4. ¿Recibió un correo electrónico o mensaje de alguien que conoce, pero la redacción, el tono de voz o la firma del mensaje son incorrectos e inusuales?

Si un mensaje parece extraño o sospechoso, puede ser un ataque. Si desea confirmar si un correo electrónico o mensaje es legítimo, una opción es llamar a la persona u organización que le envió el mensaje con un número de teléfono confiable.

Recuerda que eres por mucho la mejor defensa. Usa el sentido común.
