Publicado en Madrid el 16/08/2023

'Man in the middle', una amenaza cibernética en auge según Eduardo León de Mi Perito Informático

La ciberestafa conocida como 'man in the middle' es un ejemplo más de, hasta qué punto, los delincuentes cibernéticos están sofisticando sus técnicas de actuación. Un engaño que ha afectado ya a miles de empresas en todo el mundo, y que pone de relieve la necesidad de estar alerta y de adoptar medidas preventivas en un entorno que está cada vez más digitalizado

La también conocida como estafa del CEO implica desde la creación de cuentas a nombre de personas cuya identidad el delincuente está suplantando, hasta la intervención de las comunicaciones entre empresas.

Un delito en dos fases

El ciberestafador primero engaña a una persona para hacerse con sus datos personales. Para ello, suele publicar anuncios en los que ofrece trabajo o vende algún tipo de producto.

Con la excusa de formalizar el contrato, obtiene una foto del DNI de su víctima, y con este documento abre una cuenta bancaria online a nombre de la persona engañada sin que esta lo llegue a saber.

Por otro lado, el hacker infecta los equipos de una empresa e interviene sus comunicaciones. Cuando considera que ha llegado el momento adecuado, altera el correo electrónico enviado por la empresa proveedora a la empresa cliente. En ese correo electrónico manipulado se ha cambiado el número de cuenta en la que la entidad cliente debe hacer el ingreso para pagar a su proveedor por ese número de cuenta que el delincuente ha creado a nombre de la persona a la que ha engañado previamente.

De esta forma, la empresa paga su factura, pero el abono no lo recibe su acreedor, sino el delincuente que aprovecha el tiempo del que dispone hasta que los implicados se den cuenta de lo sucedido para trasladar el dinero a un exchange de criptomonedas y hacerlo desaparecer.

La importancia de actuar lo antes posible

Man in the middle es una estafa muy sofisticada en la que los afectados pueden tardar semanas en percibir que hay un problema.

Lo que aconsejan los expertos en seguridad informática es prevenir todo lo posible adoptando todas aquellas medidas que se sabe que pueden evitar. Por ejemplo, usar en la empresa una contraseña para el WiFi que sea difícil de detectar, no conectar los equipos de trabajo a redes públicas o no descargar ficheros de correos electrónicos que procedan de remitentes no verificados.

Si la prevención no es suficiente y la estafa se produce, hay que denunciar el hecho a la Policía o la

Guardia Civil. Pero, como bien aconseja Eduardo León Pavón de Mi Perito Informático, antes de tomar medidas hay que ponerse en manos de expertos en evidencia digital en Internet.

Porque la existencia de negligencia por parte de la empresa cliente, no verificando los datos de pago, puede hacer que sobre ella recaiga todavía la responsabilidad de pagar a su acreedor.

La labor del perito es demostrar si se ha actuado con la diligencia debida, y si para la empresa que ha pagado erróneamente al estafador era posible o no saber si estaba siendo víctima de un engaño.

Frente a una estafa de alta complejidad como esta, la experiencia de los expertos en informática y el asesoramiento legal especializado son esenciales para esclarecer las responsabilidades y buscar una solución equitativa que cause el menor daño posible a las dos empresas que se han visto involucradas.

Datos de contacto:
Eduardo León - Mi Perito Informático
+34652992001

Nota de prensa publicada en: Madrid

Categorías: Nacional E-Commerce Ciberseguridad