Caja de herramientas de ciberseguridad de la GCA: documento guía para las herramientas de «Proteja su correo electrónico y reputación»

Los delincuentes suelen utilizar habitualmente los correos electrónicos para iniciar un ciberataque. Resulta extremadamente rápido y barato enviar miles de correos electrónicos a destinatarios desprevenidos con la esperanza de que al menos algunos de ellos caigan en la trampa, piensen que son auténticos y hagan clic en el enlace de un sitio web maligno o descarguen un archivo adjunto dañino.

De este modo, el sistema informático podría verse infectado por algún tipo de malware o ransomware, lo que daría acceso al criminal para robar datos valiosos o transferir dinero a cuentas fraudulentas. También podría permitirle tomar el control de los sistemas y manipular los datos bancarios, de modo que los clientes hicieran los pagos en otras cuentas pensando que le están pagando a usted.

El uso de correos electrónicos de phishing es extremadamente eficaz para los delincuentes, ya que pueden llegar rápidamente a miles de víctimas potenciales. Sin embargo, para tener éxito, estos correos electrónicos deben parecer que provienen de una fuente legítima.

Existen diversos mecanismos a disposición de los ciberdelincuentes:

- **Modificar el nombre mostrado en el mensaje:**
    - Alterando el nombre que aparece en el campo del remitente (*De*:)
    - Alterando la dirección de correo electrónico
        - *Para evitar engaños, coloque el cursor sobre el nombre mostrado y compruebe la dirección real antes de hacer nada.*

- **Cambiar el dominio por otro muy parecido:**
    - Alterando el nombre que aparece en el campo del remitente (*De*:)
    - Usando una dirección de correo electrónico muy parecida a la que se quiere suplantar (por ejemplo: *persona@e**rn**presabuena.com* en vez de *persona@e**m**presabuena.com*
        - *Para evitar engaños, compruebe detenidamente cualquier dirección de correo electrónico antes de hacer nada.*

- **Suplantar el nombre de dominio:**

    - Alterando el nombre que aparece en el campo del remitente (*De*:)
    - Suplantando plenamente la dirección de correo electrónico, incluido su nombre de dominio
        - *Para evitar la suplantación de nombres de dominio, use DMARC.*

Incluso después de realizar una o varias comprobaciones, actúe siempre con precaución y utilice otros medios para verificar la legitimidad de los mensajes sospechosos (por ejemplo, llamar al remitente para asegurarse de que ha enviado realmente el correo electrónico).

La falta de medidas de defensa contra la suplantación de nombres de dominio podría llevar a situaciones como las siguientes:

- Que los atacantes se hagan pasar por usted o uno de sus clientes o proveedores para reclamar pagos o realizar pedidos.
- Que los atacantes puedan hacerse pasar por otras personas de su organización.

En esos casos, podrían llevar a cabo fácilmente alguno de los siguientes ataques:

- **Fraude del CEO:** envío de un correo electrónico que parece ser del CEO o un alto cargo. Normalmente, este mensaje se utilizará para pedirle a un empleado que realice un pago inmediatamente.

    - *Avise a los empleados de que siempre deben realizar varias comprobaciones. Las empresas familiares suelen fiarse o realizar comprobaciones muy superficiales, lo que podría beneficiar a los atacantes.*

- **Compromiso de cuentas empresariales (BEC, por sus siglas en inglés):** este ataque se produce cuando la cuenta de correo de una organización se ve comprometida y se envían mensajes desde ella o bien cuando un correo electrónico fraudulento utiliza un nombre de dominio legítimo (suplantación del nombre de dominio). Estos mensajes pueden ir dirigidos a proveedores o clientes para reclamar algún pago, pero con los datos bancarios alterados. Como el atacante está *dentro de la organización*, el mensaje parecerá genuino y algunas técnicas de autenticación ratificarán que los datos del remitente son legítimos, lo que dificultará aún más su detección. Es posible que el atacante lleve algún tiempo dentro del sistema monitorizando las comunicaciones, por lo que estará muy bien informado.

    - *Utilice DMARC para evitar el ataque desde el principio si se utiliza la suplantación de nombres de dominio.*
    - *Utilice contraseñas seguras y mecanismos de autenticación multifactor para reducir las posibilidades de que la cuenta se vea comprometida.*
    - *Compruebe habitualmente la configuración de la cuenta de correo electrónico para asegurarse de que no se reenvían mensajes a direcciones desconocidas.*

- *Establezca una norma interna para comprobar todos los datos de los nuevos proveedores y clientes empleando al menos dos métodos diferentes. Si se realiza algún cambio, utilice siempre un método alternativo conocido para comprobarlo (por ejemplo, llame a un número de teléfono o una centralita de confianza y no utilice el que aparece en la firma, ya que también podría haberse modificado).*

DMARC

Con las reglas de DMARC (siglas en inglés de «autenticación de mensajes basada en dominios, informes y conformidad de reglas»), los remitentes pueden indicar que sus mensajes están protegidos. Además, estas políticas le dicen al receptor qué debe hacer si uno de los métodos de autenticación se realiza correctamente o falla.

DMARC:

- Impide que un suplantador se haga pasar por usted en un correo electrónico.
- Evita la recepción de correos electrónicos de un impostor.
- Proporciona información sobre los intentos de spam, phishing o spear phishing que utilizan el dominio de correo electrónico de su organización.
- Fomenta la confianza entre los clientes y la cadena de suministro.

Sin embargo:

- Para que sea eficaz, tanto el remitente como el receptor deben tener una regla de DMARC válida y una verificación de DMARC.
- Si el cliente y el proveedor usan DMARC, ***ambos*** estarán PROTEGIDOS frente a una eventual suplantación del dominio de correo electrónico. Si uno de ellos no lo usa, ninguno de los dos lo estará.
- Lo que ocurre una vez que se recibe el mensaje depende de la configuración de la regla de DMARC de los remitentes.

Utilice las herramientas de «Proteja su correo electrónico y reputación» para obtener más información sobre DMARC y configurarlo en su dominio de correo electrónico.

https://gcatoolkit.org/es/pequenas-empresas/proteja-su-correo-electronico-y-reputacion/