Autenticación Multifactor (MFA)

MFA ayuda a contener los ataques de ciberdelincuentes

Muchos ciberataques requieren que un ciberdelincuente tenga acceso a la red corporativa o al correo electrónico. Con un acceso tradicional de usuario y contraseña, conocido como Autenticación de Factor Único (SFA), puede ser fácil para los ciberdelincuentes obtener acceso al sistema informático de una empresa.

Una vez que un atacante tiene acceso a su correo electrónico, puede hacerse pasar por usted, y enviar correos electrónicos falsos o, en caso de acceder a su red, explorar su entorno, aumentar sus privilegios, eliminar copias de seguridad y/o desplegar un ataque de ransomware.

Este tipo de ataques pueden ocurrir de diversas maneras:

Fuerza bruta o uso de una herramienta de descifrado de contraseñas para probar automáticamente muchas contraseñas comunes.

Recolección de credenciales o explotar el hecho de que muchas personas usan las mismas combinaciones de identificación y contraseña en varias cuentas.

Phishing o envío de un email falso para restablecer la contraseña, recopilando así la información del correo electrónico comercial de ese empleado.

Uno de los métodos más efectivos para contener a los ciberdelincuentes es la Autenticación Multifactor (MFA), que esencialmente ofrece una segunda capa de autenticación/defensa.

¿ Qué es el MFA?

MFA requiere dos o más factores de autenticación, o pruebas de identidad, para garantizar que aquellos que buscan acceso al correo electrónico de la empresa y otros activos criticos de la empresa sean realmente quienes dicen ser.
Por ejemplo, tres capas de autenticación podrían ser:

1. 

Algo que sabes
(normalmente es una contraseña o un código de verificación)

2. 

Algo que tienes
(un dispositivo de confianza que no es fácil de duplicar, como un móvil o una llave de seguridad

3. 

Algo que eres
(biometría)

> ***Teniendo dos o más factores de autenticación supone un reto importante para los atacantes, reduciendo sustancialmente el riesgo de intrusión.***

¿Por qué es importante el MFA?

La idea del MFA es que, aunque los ciberdelincuentes puedan robar lo que los usuarios legítimos saben, es mucho menos probable que también tengan lo que esos usuarios poseen. Por ejemplo, en el caso de una cuenta de correo electrónico, lo que los usuarios poseen es el token o dispositivo que genera o recibe un código único, y de corta duración que los ciberdelincuentes no tendrán.

Implementación del MFA

La activación del MFA puede ser una de las formas más rápidas e importantes de proteger las identidades de los usuarios. Muchos, si no la mayoría, de los servicios web habituales ofrecen MFA, aunque a menudo está desactivado por defecto.

Obtén asesoramiento de expertos para implementar el MFA que mejor se adapte a su empresa.

Chubb. Insured.℠

SP0279-MD 09/22