Doble factor de autenticación

La autenticación es el acto o proceso de confirmar que algo (o alguien) es quien dice ser para posteriormente acceder a ciertos recursos definidos y **la autorización** es el proceso sobre el cual se establecen que tipos de recursos están permitidos o denegados para cierto usuario o grupo de usuarios concreto.

Para poder realizar los dos procesos o actos anteriores con éxito (sobre todo la autenticación), la mayoría de los sistemas están basados en tres fuentes de información:

- **Lo que sé**: existe una información, como por ejemplo una contraseña, que se supone que sólo conoce la persona que desea autenticarse y que, por tanto, si es correcta se considera acreditada la identidad del legítimo usuario.
- **Lo que tengo**: existe algún objeto que está en posesión de la persona que quiere autenticarse. Si se puede verificar que esa persona tiene ese objeto, se la considerará legítima, como una tarjeta magnética o un móvil.
- **Lo que soy**: este apartado se refiere a la biometría, cualquier parámetro biológico que pueda ser medido y nos diferencie de cualquier otra persona. Los más habituales son la huella dactilar, el iris de un ojo o nuestra cara.

De lo que se trata con el uso del doble factor de autenticación es de combinar dos o más fuentes de información de las mencionadas anteriormente para intentar tener una mayor seguridad en el proceso de autenticación.

Por ejemplo, un proceso de autenticación que requiere un código obtenido a partir de una aplicación o un mensaje SMS, además de una contraseña para acceder al servicio es un proceso que cumple estas condiciones.

El caso anterior es un método muy utilizado por ejemplo en procesos de autenticación y autorización en el sector bancario, debido a la criticidad de las operaciones que manejan estas compañías llevan utilizando métodos de doble factor desde hace mucho tiempo (por ejemplo un dispositivo físico junto con un PIN en el caso de las tarjetas financieras).

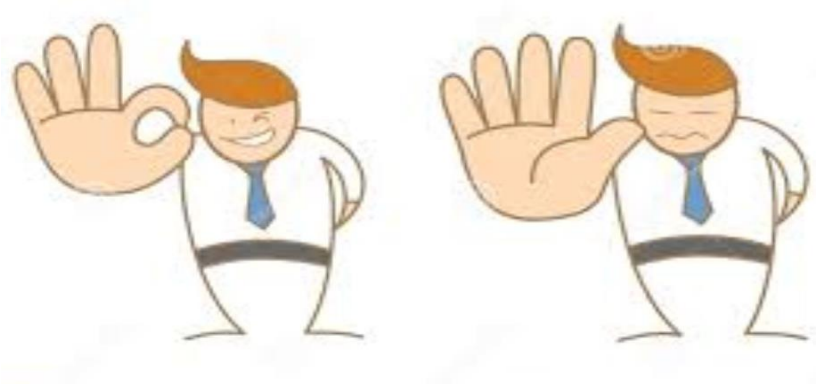
Todas las grandes compañías como Twitter, Google, LinkedIn o Dropbox, entre otras, ya ofrecen esta característica como un opcional (y algún caso de manera obligatoria) de seguridad para sus cuentas o sus accesos, pero independientemente del tamaño o criticidad de las empresas es una medida que se implementa cada día en más compañías.

Debido al gran numero de ataques dirigidos y de vulnerabilidades conocidas, a lo que se tiende es a la autenticación en múltiples factores, en el que un usuario combina dos o más factores para poder completar el proceso de acceso a cualquier aplicación.

Algunos de los ejemplos que se pueden combinar en cualquiera de los casos comentados podrían ser:

- Una tarjeta inteligente
- Introducir un PIN
- Certificado digital cliente
- Contraseña
- Código de un solo uso (OTP)
- Token aleatorio de seguridad
- Escanear una huella digital
- Reconocimiento facial
- Pregunta de seguridad
- Introducir un USB de autenticación
- Etc.

Para acabar el presente artículo, es importante reseñar que no hay un método infalible y que: los sistemas de doble factor o de factor múltiple son mejores que la contraseña sola, pero los atacantes o usuarios malintencionados pueden encontrar el modo de vulnerar todos los mecanismos y por ende tener nuestro sistema de autenticación comprometido.



Fernando Saavedra

Cybersecurity Manager

Áudea Seguridad de la Información