Curso de Especialización de Ciberseguridad en Entornos de Tecnología de la Información (CETI)

Bastionado de redes y sistemas

UD03. Ventajas e inconvenientes de los factores de autenticación.
Tarea Online.

JUAN ANTONIO GARCIA MUELAS

INDICE

1.- Descripción de la tarea.

Caso práctico

Tendrás que realizar un pequeño trabajo de investigación acerca de las ventajas y desventajas de los mecanismos de autenticación tanto 2FA como MFA, justificando brevemente las respuestas y aportando ejemplos.

¿Qué te pedimos que hagas?

✓ **Apartado 1: tarea de investigación**

Una vez que conoces los diferentes factores de autenticación, deberás llevar a cabo una investigación para:

➢ Determinar cuáles son sus ventajas con respecto a los mecanismos convencionales.

Los mecanismos de autenticación 2FA (dos factores) y MFA (multifactor) nos ofrecen respecto a los mecanismos tradicionales de contraseña, ventajas como:

- **Mayor seguridad:** dos o más factores, dificultan el acceso a posibles atacantes, que incluso conozcan la contraseña.
- **Menor riesgo de fraude:** derivado del punto anterior.
- **Mayor protección de datos sensibles**: cuentas bancarias, tarjetas, cuentas de email.

Estas ventajas podemos implementarlas mediante:

- **Biometría:** añade una capa de protección mediante el uso de voz, huella dactilar o iris, algo personal único e intransferible en cada persona y muy difícil de falsificar. Podemos ver su uso en accesos a centros de trabajo.
- **Notificaciones Push, SMS.** Seguros al ser envíos de un solo uso, imposibles de utilizar luego por un tercero, y que ya estamos acostumbrados a utilizar en banca online o plataformas de pago.
- **Tokens de hardware, certificados digitales o tarjetas físicas:** los tokens nos generan código aleatorios. Los certificados digitales y las tarjetas inteligentes son elementos difíciles de falsificar. Su llegada nos ha permitido firmar contratos de manera remota, o acceder a tramites online de forma segura.
- **Ubicación, hora:** se puede vincular como factor una determinada ubicación o zona geográfica o unos husos horarios, que impidan iniciar sesiones fuera de esos rangos. No es muy común todavía, pero ya hay servicios de Microsoft o de Cloudflare, por ejemplo, que los incorporan.

➢ Identificar aquellos inconvenientes que los pueden hacer inseguros o poco usables para los usuarios.

A pesar de las ventajas comentadas también tienen algunos inconvenientes para los usuarios, como:

- **Peor usabilidad**: ya que requiere que se recuerden dos o más factores de autenticación.
- **Coste:** La implementación puede ser costosa para las empresas y organizaciones.
- **Vulnerabilidades:** como ataques de phishing o de fuerza bruta, en casos en los que no se combinen correctamente los factores.

Esta serie de desventajas las observamos en:

- **Biometría:** cada vez hay una mayor oferta de acceso a estos servicios, pero la implementación de dicho factor sigue teniendo un coste alto por infraestructura según el tipo de empresa, por lo que acaba pesando en la decisión de no incorporarlo como medida de seguridad.
- **Tokens, certificados, tarjetas físicas:** Debemos estar muy seguros al elegir el proveedor de dicho servicio, para poder garantizar la integridad de este tipo de factor. Hoy día, es relativamente común ver las bandejas de entrada de nuestro correo empresas que facilitan su generación, y que no siempre van a ser fiables.
- **Los ataques son posibles** si consiguen nombre y contraseña por un lado, gracias a phishing y/o fuerza bruta, y redirigiendo el tráfico del inicio de sesión cuando se pide un tercer factor como un código único, donde el usuario pensaría que está introduciendo dicho código en el lugar correcto, pero los atacantes lo aprovecharían para iniciar una sesión real y acceder.
- Por último, hay que pensar en la **dificultad** que puede suponer su **uso**, cuando puede fallar alguno de los factores, ya sea por olvido (puede ser el caso de frases de paso como contraseña), pérdida o sustracción del elemento físico (un DNIe, un USB con un certificado o la tarjeta de chip).

Webgrafía.

https://www.microsoft.com/es-es/security/business/security-101/what-is-two-factor-authentication-2fa

https://www.cloudflare.com/es-es/learning/access-management/what-is-multi-factor-authentication/

https://www.lastpass.com/es/solutions/authentication/mfa-vs-2fa

https://gblogs.cisco.com/la/ciberseguridad1-marcom2-diferencias-entre-2fa-y-multi-factor-authenticator/