TAREA 03

CONFIGURACIÓN DE SISTEMAS DE ACCESO Y AUTENTICACIÓN DE PERSONAS

BASTIONADO DE REDES Y SISTEMAS

ALBA MOREJÓN GARCÍA

2024/2025

CETI - Ciberseguridad en Entornos de las Tecnologías de la Información

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.

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

La autenticación de doble factor (2FA) y la autenticación multifactor (MFA) son mecanismos de seguridad que buscan fortalecer la protección de cuentas y sistemas frente a accesos no autorizados. A diferencia de los métodos tradicionales de autenticación, que dependen exclusivamente de una contraseña, estos dos métodos utilizan múltiples capas de seguridad para verificar la identidad del usuario.

- La **autenticación en dos factores** (2FA), es un método de autenticación que requiere dos factores para verificar la identidad de un usuario. Estos factores suelen combinar la contraseña del usuario, con una confirmación en el teléfono, un token o algún factor de biometría.

- La **autenticación multifactor** (MFA), es una versión más avanzada del 2FA, ya que permite utilizar dos o más factores de autenticación para verificar la identidad del usuario. Puede incluir combinaciones de factores adicionales como una clave física (token USB) o una aplicación de autenticación junto con un factor biométrico, incrementando de esta forma la seguridad.

Ventajas de 2FA y MFA

- Presentan mayor seguridad ante ataques de fuerza bruta, al combinar diferentes factores de autenticación, se dificulta que un atacante pueda comprometer una cuenta, incluso si logra obtener la contraseña. Por ejemplo, un código temporal (OTP) enviado a un dispositivo móvil añade una capa de seguridad.
- Tiene protección ante robo de credenciales, aunque un atacante logre acceder a una contraseña mediante phishing, keylogging o fuga de datos, necesitará los factores adicionales para acceder a la cuenta como un dispositivo físico o rasgo biométrico.
- Cumplen los estándares de seguridad, muchas regulaciones (GDPR o PCI DSS) recomiendan o exigen el uso de MFA para proteger los datos sensibles y garantizar la integridad de los sistemas, el no cumplir con los requisitos puede conllevar sanciones legales.
- Ofrecen diferentes opciones a la hora de elegir el método de autenticación, como aplicaciones de autenticación (Google Authenticator), tokens físicos o biometría facial o dactilar. Esto permite a las organizaciones adaptar el mecanismo a sus necesidades y al nivel de sensibilidad de los recursos protegidos.

Inconvenientes de 2FA y MFA

- Dependencia de dispositivos adicionales, algunos métodos como los códigos enviados por SMS o aplicaciones de autenticación, requieren que el usuario tenga un dispositivo móvil al alcance. El mal funcionamiento, la pérdida o robo del dispositivo puede dificultar el acceso a la cuenta.
- Frustración de los usuarios, la necesidad de realizar pasos adicionales para autenticarse puede resultar liosa, especialmente para usuarios menos familiarizados con la tecnología. Esto puede llevar a errores, pérdida de tiempo y rechazo al uso del sistema.
- Los costos de implementación y mantenimiento, configurar un sistema MFA implica inversiones en software y formación, además de soporte técnico continuo. Esto puede ser un desafío para empresas más pequeñas y de recursos limitados.

- Vulnerabilidades residuales, aunque estos mecanismos son más seguros que los métodos convencionales, no son infalibles. Ataques como el SIM swapping pueden comprometer el factor basado en el mensaje por SMS y ciertos métodos biométricos pueden ser vulnerables a réplicas.

Los mecanismos de autenticación 2FA y MFA son herramientas esenciales para mejorar la seguridad de los sistemas en un mundo donde las amenazas son cada vez más sofisticadas. Ofrecen ventajas importantes como la protección frente a ataques de contraseñas, sin embargo, debemos ser conscientes de la dependencia de dispositivos y su adopción debe considerar un equilibrio entre la robustez de la protección y la facilidad de uso para los usuarios. La clave para aprovechar al máximo estos sistemas es elegir los factores adecuados y educar a los usuarios para maximizar su efectividad.