La seguridad por obscuridad es un concepto que hace referencia a la práctica de proteger sistemas o datos simplemente ocultándolos o manteniéndolos en secreto, en lugar de emplear medidas de seguridad robustas y conocidas. Aquí te explico más detalladamente:

**Definición y Ejemplos**

1. **Principio Básico**:
   * La seguridad por obscuridad implica confiar en que mantener detalles críticos en secreto o difíciles de encontrar proporcionará protección contra amenazas y ataques.
2. **Ejemplos Comunes**:
   * **Nombres de Usuario y Contraseñas por Defecto**: Utilizar nombres de usuario y contraseñas poco conocidos o difíciles de adivinar en lugar de cambiarlos por defecto.
   * **Ocultar Servicios y Puertos**: No revelar la existencia de servicios o puertos abiertos en un sistema, en lugar de protegerlos con firewalls y configuraciones de seguridad adecuadas.
   * **Ofuscación de Código**: Ofuscar el código fuente de aplicaciones o servicios en lugar de implementar técnicas sólidas de seguridad y protección contra vulnerabilidades conocidas.

**Críticas y Limitaciones**

1. **Ineficacia ante Ataques Conocidos**:
   * La seguridad por obscuridad no ofrece protección real contra ataques dirigidos o métodos bien conocidos por los hackers. Por ejemplo, los escáneres de puertos pueden revelar servicios ocultos.
2. **Falta de Sostenibilidad**:
   * Dependiendo únicamente de la obscuridad para la seguridad puede llevar a una falsa sensación de seguridad. Eventualmente, la información oculta puede ser descubierta o filtrada.
3. **Complemento en vez de Solución**:
   * Es más efectivo emplear prácticas de seguridad estándar y bien conocidas (como encriptación, autenticación fuerte y monitoreo activo) en lugar de confiar exclusivamente en la obscuridad.

**Buenas Prácticas de Seguridad**

* **Principio de Defensa en Profundidad**: Implementar múltiples capas de seguridad que se complementen entre sí.
* **Transparencia en la Seguridad**: Revelar detalles críticos mientras se protegen adecuadamente con medidas de seguridad robustas.
* **Actualizaciones y Parches**: Mantener sistemas y software actualizados con los últimos parches de seguridad para mitigar vulnerabilidades conocidas.

En conclusión, mientras que mantener cierta información en secreto puede ser una práctica complementaria en la seguridad global de sistemas y datos, no debe considerarse como la principal estrategia de seguridad. Es crucial implementar medidas de seguridad robustas y bien conocidas para proteger activamente contra amenazas cibernéticas.