C i b e r c o n s e j o s

¿Cómo prevenir la Escalabilidad de privilegios?

¿Qué es?

Tipo de ataque con el que los ciberdelincuentes logran, tras acceder sin autorización a un sector relativamente poco sensible de un sistema, alcanzar otros, explotando fallas en la configuración del mismo o vulnerabilidades de software.

O sea, pueden conseguir mayores privilegios definidos en computación como la capacidad de realizar cambios en el sistema y ver y modificar datos contenidos en él de los que tenían al penetrar el sistema.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ciberconsejos

¿Cómo prevenir la Escalabilidad de privilegios?

¿Cómo funciona?

Para lograrlo, existen dos principales mecanismos:

1

Escalamiento horizontal (o movimiento lateral): Los delincuentes ganan acceso a distintos sectores del sistema, pudiendo robar otro tipo de datos, por ejemplo, pero con el mismo nivel de privilegios.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ciberconsejos

¿Cómo prevenir la Escalabilidad de privilegios?

¿Cómo funciona?

Para lograrlo, existen dos principales mecanismos:

2

Escalamiento vertical:
Ganan privilegios de mayor rango, pudiendo, tomando el control de una cuenta de usuario, por ejemplo, alcanzar el rol de administrador de un sistema.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ciberconsejos

¿Cómo prevenir la Escalabilidad de privilegios?

¿Qué ganan los ciberdelincuentes?

Mientras más privilegios gane el atacante, puede acceder a robar o alterar más datos, o tomar control de distintos dispositivos y funciones, pudiendo tomar el control total si accede a los privilegios de administrador del sistema.

Si hay indicios de escalamiento de privilegios dentro de un sistema, esto debe ser tratado como un problema grave dentro de la ciberseguridad de la organización.

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

C i b e r c o n s e j o s

¿Cómo prevenir la Escalabilidad de privilegios?

¿Cómo protegerse?

- Mantener actualizados los sistemas: muchas de las vulnerabilidades que los proveedores de software usualmente parchan son de este tipo.

- Escanear regularmente sus redes, sistemas y aplicaciones para detectar si un ataque de escalamiento de privilegios no está teniendo lugar ya en sus sistemas.

- Dar privilegios solo a los usuarios que lo necesiten y por el tiempo requerido.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

C i b e r c o n s e j o s

¿Cómo prevenir la Escalabilidad de privilegios?

¿Cómo protegerse?

- Monitorear el comportamiento de los usuarios con distintos niveles de privilegios.

- Contar con políticas de seguridad y de contraseñas seguras, que sean de conocimiento de la organización y verificar que sean implementadas en la práctica

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática