#BarcelonaIdentidadDigital

Los 10 errores más habituales en AD y Entra

Oscar Tortosa

linkedin.com/in/oscartbcn

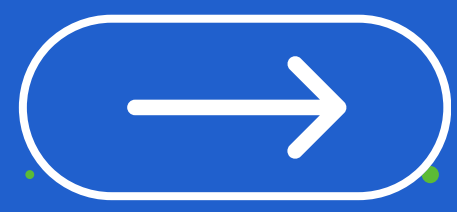
#BarcelonaIdentidadDigital

1 Usuarios sin privilegios Owners de aplicaciones críticas

Asignar usuarios no administrativos como propietarios de aplicaciones críticas en Entra ID es una puerta de entrada para atacantes.

🔎 Riesgo: Control total de la APP si la cuenta se ve comprometida.

✓ **Recomendación:** Solo cuentas administradas bajo políticas de alto control (MFA, monitorización, segmentación) deben tener estos privilegios.



linkedin.com/in/oscartbcn

#BarcelonaIdentidadDigital

2 Permisos de correo en aplicaciones

Aplicaciones en Entra ID con permisos Mail.ReadWrite o Mail.Send pueden acceder a todos los buzones de la organización.

🔎 Riesgo: Acceso masivo a información sensible; envío de correos desde identidades críticas.

✔ **Recomendación:** Aplica el principio de mínimo privilegio. Usa políticas de acceso específicas con ApplicationAccessPolicy.

linkedin.com/in/oscartbcn

#BarcelonaIdentidadDigital

3 Cuentas de servicio activas tras desmantelar servidores

Dejar cuentas de servicio activas tras apagar un servidor crea puntos ciegos críticos.

🔎 Riesgo: Persistencia del atacante mediante cuentas invisibles a la monitorización.

✔ **Recomendación:** Establece protocolos de decomisión que incluyan revisión y eliminación de cuentas de servicio.

linkedin.com/in/oscartbcn

#BarcelonaIdentidadDigital

4 Tratar Entra Connect como un activo no crítico

Entra Connect tiene permisos DCSync y acceso a hashes NT. No tratarlo como un entorno crítico es un error común.

🔎 Riesgo: Compromiso total de AD desde una única cuenta.

✓ **Recomendación:** Clasifícalo como activo de Tier 0. Protege con LAPS, Credential Guard y controles reforzados.

linkedin.com/in/oscartbcn

#BarcelonaIdentidadDigital

5 AdminSDHolder desprotegido

AdminSDHolder controla permisos de cuentas privilegiadas. Si su ACL es manipulada, el acceso malicioso se hereda.

🔎 Riesgo: Persistencia de privilegios indebidos incluso tras su eliminación.

✓ **Recomendación:** Limita quién puede modificarlo, configura alertas y monitoriza todos los cambios.

linkedin.com/in/oscartbcn

#BarcelonaIdentidadDigital

6 Acceso de administradores a equipos no privilegiados

Permitir que administradores usen dispositivos estándar eleva el riesgo de robo de credenciales.

🔎 Riesgo: Robo de credenciales mediante malware o técnicas de scraping.

✓ **Recomendación:** Implementa modelos de administración escalonados como PAW. Aísla y protege los entornos de administración.

linkedin.com/in/oscartbcn

#BarcelonaIdentidadDigital

7 Cuentas privilegiadas en OU´s inseguras

Vincular cuentas de Tier 0 a GPO´s fuera del Tier 0 expone toda la jerarquía.

🔎 Riesgo: Escalada de privilegios a través de GPOs mal protegidas.

✔️ **Recomendación:** Reubica cuentas en OUs Tier 0. Revisa y ajusta las GPOs asociadas.

linkedin.com/in/oscartbcn

#BarcelonaIdentidadDigital

8 Nesting de grupos privilegiados

La anidación de grupos puede ocultar permisos excesivos y dificultar la trazabilidad.

🔎 Riesgo: Asignaciones de privilegios indirectos no detectadas.

✔️ **Recomendación:** Mantén la estructura de grupos privilegiados plana y documentada.

linkedin.com/in/oscartbcn

#BarcelonaIdentidadDigital

9 Grupos sin propietario ni propósito

Grupos sin administración clara promueven el sobre aprovisionamiento.

🔎 Riesgo: Accesos heredados innecesarios y difícil auditoría.

✓ **Recomendación:** Define propietarios, documenta propósito y establece revisiones periódicas.

linkedin.com/in/oscartbcn

#BarcelonaIdentidadDigital

10 Cuentas OnPremise en roles administrativos de Entra

Entra Connect tiene acceso a los hashes de contraseñas debido a la sincronización.

🔎 Riesgo: Si un atacante accede a Entra Connect, tendría la capacidad de comprometer tanto el AD local como Entra ID.

✔ **Recomendación:** Utiliza usuarios nativos de Entra (No OnPremises) para las asignaciones de roles administrativos de Entra ID

Además, implementar MFA para todas las cuentas administrativas.

linkedin.com/in/oscartbcn

#BarcelonaIdentidadDigital

Comparte
Comenta
Me gusta

Oscar Tortosa

linkedin.com/in/oscartbcn/