Least Privilege

Inhaltsverzeichnis

Least Privilege bedeutet, dass Benutzer und Systeme nur die Rechte erhalten, die sie für ihre Aufgabe wirklich brauchen. Das Prinzip begrenzt Schaden durch Fehler, Malware oder kompromittierte Konten.

1 Funktionsweise

Rechte werden bewusst eng vergeben und regelmäßig überprüft. Administrative Vollzugriffe sind die Ausnahme, nicht der Alltag – oft zeitlich begrenzt oder über Just-in-Time-Freigaben.

- **Rollen statt Sammelrechte:** klare Aufgabenprofile
- **Trennung:** Admin- und Alltagskonto getrennt
- **Review:** ungenutzte Rechte wieder entziehen

2 Typische Einsatzbereiche

- Server-, Cloud- und Datenbankberechtigungen
- Service-Accounts und CI/CD-Secrets
- Dateifreigaben und Fachanwendungen

3 Wichtige Hinweise

- Zu breite Gruppenmitgliedschaften sind eine häufige Schwachstelle.
- Dokumentation und Ownership verhindern „Rechte-Leichen“.
- Least Privilege wirkt am besten zusammen mit MFA und Logging.

4 Fazit

Least Privilege ist ein grundlegendes Sicherheitsprinzip: Weniger Rechte bedeuten weniger Angriffsfläche – im Alltag wie im Incident-Fall.