Defense in Depth

Inhaltsverzeichnis

- 1 Funktionsweise
- 2 Typische Einsatzbereiche
- 3 Wichtige Hinweise
- 4 Fazit

Defense in Depth bedeutet Sicherheit in mehreren Schichten: Fällt eine Kontrolle aus, greifen weitere. Statt einer einzigen Schutzmaßnahme entsteht ein gestaffeltes Abwehrkonzept.

1 Funktionsweise

Technische, organisatorische und physische Maßnahmen ergänzen sich – von Perimeter und Segmentierung über Identity bis Backup und Monitoring.

- **Prävention:** Härten, Filtern, Least Privilege
- **Detection:** Logs, IDS/SIEM, Alerts
- **Response:** Incident-Prozesse und Wiederherstellung

2 Typische Einsatzbereiche

- Unternehmens- und KMU-Infrastrukturen
- Cloud- und Hybrid-Umgebungen
- Kritische Dienste mit hohem Schadenpotenzial

3 Wichtige Hinweise

- Viele Tools ohne Konzept erzeugen blinden Aktionismus.
- Schichten müssen zusammenpassen und betreibbar bleiben.
- Menschen und Prozesse gehören zur Tiefe dazu.

4 Fazit

Defense in Depth reduziert das Risiko einzelner Ausfälle – Sicherheit entsteht durch sinnvolle Staffelung, nicht durch ein „Allheilmittel“.