Honeypot

Inhaltsverzeichnis

Ein Honeypot ist ein bewusst exponiertes Ködersystem. Angriffe darauf liefern Frühwarnungen und Einblicke in Taktiken – ohne echte Produktivdaten preiszugeben.

1 Funktionsweise

Der Dienst wirkt verwundbar oder interessant, ist aber isoliert und intensiv überwacht. Jede Interaktion gilt als verdächtig, weil niemand legitim dort arbeiten sollte.

- **Low-/High-Interaction:** Simulation vs. echtes System
- **Isolation:** kein Pfad zu Produktivnetzen
- **Telemetry:** IPs, Payloads, Timing erfassen

2 Typische Einsatzbereiche

- Früherkennung von Scans und Angriffen
- Threat Intelligence und Research
- Ablenkung und Verlangsamung von Angreifern

3 Wichtige Hinweise

- Schlecht isolierte Honeypots werden selbst zum Risiko.
- Rechtliche und datenschutzrechtliche Rahmen prüfen.
- Alerts brauchen klare Reaktionsspielregeln.

4 Fazit

Honeypots sind Detektions- und Lernwerkzeuge – wertvoll in der Tiefe der Abwehr, niemals Ersatz für Hardening und Patching.