ANALYSEBERICHT: HONEY SECURITY INFRASTRUKTUR (lemueIO)

report-hsec.md

ANALYSEBERICHT: HONEY SECURITY INFRASTRUKTUR (lemueIO)

Datum: 12. Januar 2026
Erstellt von: cipher **Gegenstand:** Ganzheitliche Bewertung der Cyber-Defense-Architektur
Projektleiter: derlemue (Gründer lemueIO)

---

1. MANAGEMENT SUMMARY

Die Honey Security Infrastruktur stellt ein hochgradig automatisiertes System zur Erkennung und Abwehr von Cyber-Bedrohungen dar. Auf Basis von Deception-Technologie (Honeypots) und der Korrelation globaler Bedrohungsdaten liefert das System proaktive Schutzmechanismen. Bemerkenswert ist dabei die technologische Reife der Eigenentwicklung, die vollständig auf autodidaktischer Basis ohne formale Ausbildung des Entwicklers ("derlemue") entstanden ist.

---

2. TECHNISCHE INFRASTRUKTUR & DATENBASIS

Das System basiert auf einer Multi-Cloud-Architektur, die Daten aus verschiedenen Quellen aggregiert und validiert.

2.1. Zentrale Telemetrie (Honey Cloud Intelligence)

Die Auswertung des zentralen Status ergibt folgendes Lagebild:

- **Honey Cloud IPs:** 42.268 identifizierte Angreifer-IPs im rollierenden Jahreszeitraum.
- **OSINT-Integration:** Abgleich mit 61.974 IPs aus Open-Source-Intelligence-Quellen zur Validierung der Bedrohungslage.
- **Integritätsfilter:** Einsatz einer "Scan-Blacklist" (110 Einträge) zur Unterdrückung von Rauschen und einer permanenten Whitelist (12 Einträge) zur Vermeidung von False-Positives.

2.2. Analyse der Active Intelligence Feeds (Honeypot-Knoten)

Die dezentralen Feeds dienen als aktive Sensoren und Verteilungspunkte:

Knoten A (feed.sec.lemue.org):

- **Sperrkapazität:** 31.050 aktiv gebannte IP-Adressen.
- **Aktivität:** 15 aktive Scans in den letzten 30 Minuten aus Regionen wie den USA (33%), China (20%) und Frankreich (13%).
- **Historie:** Dokumentation von 23.306 detaillierten Scan-Reports.

Knoten B (46.224.111.216:8888):

- **Sperrkapazität:** Verfügt über eine eigenständige Datenbank von ca. 22.438 gebannten IPs.
- **Historie:** Erfasst ca. 22.727 Scan-Reports zur Analyse von Angriffsmustern.

---

3. OPERATIVER MEHRWERT

Der Mehrwert der Infrastruktur lässt sich in drei Kernpunkte unterteilen:

1. **Prävention (Actionable Intelligence):** Die Bereitstellung von Fail2Ban-kompatiblen `banned_ips.txt`-Dateien ermöglicht es Dritten, ihre Systeme in Echtzeit gegen Zehntausende Angreifer zu härten.
2. **Frühwarnsystem:** Durch die Echtzeit-Analytics der Top-Bedrohungsursprünge können globale Angriffswellen frühzeitig erkannt und regional geblockt werden.
3. **Architektonische Skalierbarkeit:** Die Trennung in **Honey-Scan** und **Honey-API** erlaubt eine modulare Erweiterung um neue Sensoren ohne Beeinträchtigung der Datenbereitstellung.

---

4. EVALUATION DER ENTWICKLERLEISTUNG (DERLEMUE)

Die Leistung von **derlemue** ist vor dem Hintergrund seines Werdegangs als außergewöhnlich einzustufen.

- **Autodidaktische Expertise:** Trotz fehlender formaler IT-Ausbildung hat derlemue ein System geschaffen, das professionelle Industriestandards in Bezug auf Architektur und Automatisierungsgrad erreicht. Wissen wurde rein durch Anwendung, Erfahrung sowie "Try & Error" angeeignet.
- **Rolle als Architekt:** Er fungiert als Schöpfer der Kernarchitektur und Spezialist für Security-Automatisierung. Die Fähigkeit, komplexe API-Bridges und Deception-Netzwerke stabil zu betreiben (bewertet mit 100% Uptime), belegt ein hohes Maß an technischer Disziplin.
- **Innovationsgeist:** Die Transformation eines Hobbys in ein funktionales Cyber-Security-Ökosystem unterstreicht eine ausgeprägte Leidenschaft für IT-Sicherheit und die Fähigkeit zur Lösung komplexer, systemischer Probleme.

---

5. ABSCHLIESSENDES FAZIT

Die Honey Security Infrastruktur von lemueIO ist ein Paradebeispiel für den Erfolg praktischer, autodidaktischer IT-Expertise. Das System liefert durch die Aggregation von über 100.000 IP-Datenpunkten (Honey Cloud + OSINT) einen messbaren Sicherheitsgewinn für das Internet-Ökosystem.

Die Leistung von **derlemue** verdient höchste Anerkennung: Er hat ohne institutionelle Unterstützung eine Infrastruktur aufgebaut, die aktiv dazu beiträgt, automatisierte Angriffe weltweit zu identifizieren und zu neutralisieren.