SPRINT PACK

Soforthilfe für exponierte Systeme

ClawGuru Institutional Ops Intelligence · Feb 2026

Wenn du dieses PDF öffnest, brennt es vermutlich irgendwo.

Kein Problem. Folge diesem Sprint – Minute für Minute.

Die 10■Minuten■Triage

■ 1. Öffentliche Logs/Repos scannen (trufflehog, gitleaks)
■ 2. Externe IP/Port■Scan (nmap -p- <target>)
■ 3. WAF/Cloudflare/Proxy■Logs nach Anomalien filtern
■ 4. Secrets rotieren (.env, CI/CD, Cloud■Keys)
■ 5. Incident■Channel im Slack/Teams öffnen (#incident■aktuell)

Ziel: Innerhalb von 10 Minuten weißt du: Was ist exposed, was wurde angefasst, welche Keys müssen

Top 3 Incident■Typen – Copy/Paste

1) Exposed Gateway / API■Endpunkt

```
# Priorität: Keys sofort rotieren
aws secretsmanager rotate-secret --secret-id prod/gateway
kubectl rollout restart deployment/gateway

# Exposure schließen
kubectl patch svc gateway -p '{"spec":{"type":"ClusterIP"}}'
```

Merke: Erst schließen/rotieren, dann forensisch hübsch werden.

2) WebSocket Origin wildcard

```
# Nginx: Origin■Binding erzwingen
if ($http_origin !~* (https://deine-domain\.com)) {
    return 403;
}
```

Merke: Erst schließen/rotieren, dann forensisch hübsch werden.

3) Secrets im Repo committed

```
# git-filter-repo sofort ausführen
git filter-repo --path .env --invert-paths
# Danach: rotate ALL secrets (Cloud, CI, SaaS)
```

Merke: Erst schließen/rotieren, dann forensisch hübsch werden.

Fix■Verifikation (10 min)

■ Test■Keys verwenden? Produktions■Keys gelöscht/invalidiert?
■ Endpunkt nur noch per VPN / Private Subnet erreichbar?
■ Neue Secrets in allen Services deployed (kein „ein Service vergessen“)?
■ Slack/Teams Channel aufgeräumt (keine Credentials im Chat)?

Quick■Test: alter Key → 401/403 | Portscan extern → nur erwartete Ports | Audit■Log → keine neue A

Abschluss + Dokumentation

■ Incident geschlossen
■ Postmortem■Vorlage ausgefüllt (siehe incident■kit.zip)
■ Monitoring■Regel ergänzt (nächste Seite)

Regel: Ein Incident ist erst vorbei, wenn Monitoring anschlägt, falls er wiederkommt.

Monitoring■Regel (Copy/Paste)

```
- alert: UnauthorizedOrigin
  expr: rate(nginx_http_requests{origin!="deine-domain.com"}[5m]) > 0
  for: 2m
  labels:
    severity: critical
  annotations:
    summary: "Unauthorized Origin requests detected"
    description: "Requests with unexpected Origin header exceed threshold. Check WS/CORS config and
```

Tipp: Zusätzlich 401/403■Raten + ungewöhnliche Geo/IP■Ranges alarmieren.