vanilla K8S Was kann schiefgehen?

Als Plattform für containerisierte Applikationen bietet Kubernetes enorme Vorteile - schlecht konfiguriert große Risiken. Das Verständnis der Komponenten von Kubernetes und die Identifikation der in Vanilla Kubernetes enthaltenen Sicherheitsoptionen dienten mir als Basis, um diese mit bekannten Best Practices und Empfehlungen wie dem CIS Benchmark, dem Baustein APP.4.4 des IT-Grundschutz-Kompendiums des BSI und dem NIST SP 800-190 abzugleichen. Der CIS Benchmark und der Baustein APP.4.4 bieten detaillierte Sicherheitsmaßnahmen in drei Stufen, das NIST SP800-190 entspricht der höchsten Stufe dieser Standards. Da jeder Standard unterschiedliche Schwerpunkte und Detailgrade aufweist, ist es wichtig die Absicherung von Entwickler- und Produktions-Umgebungen zu unterscheiden.

DEV Absicherung

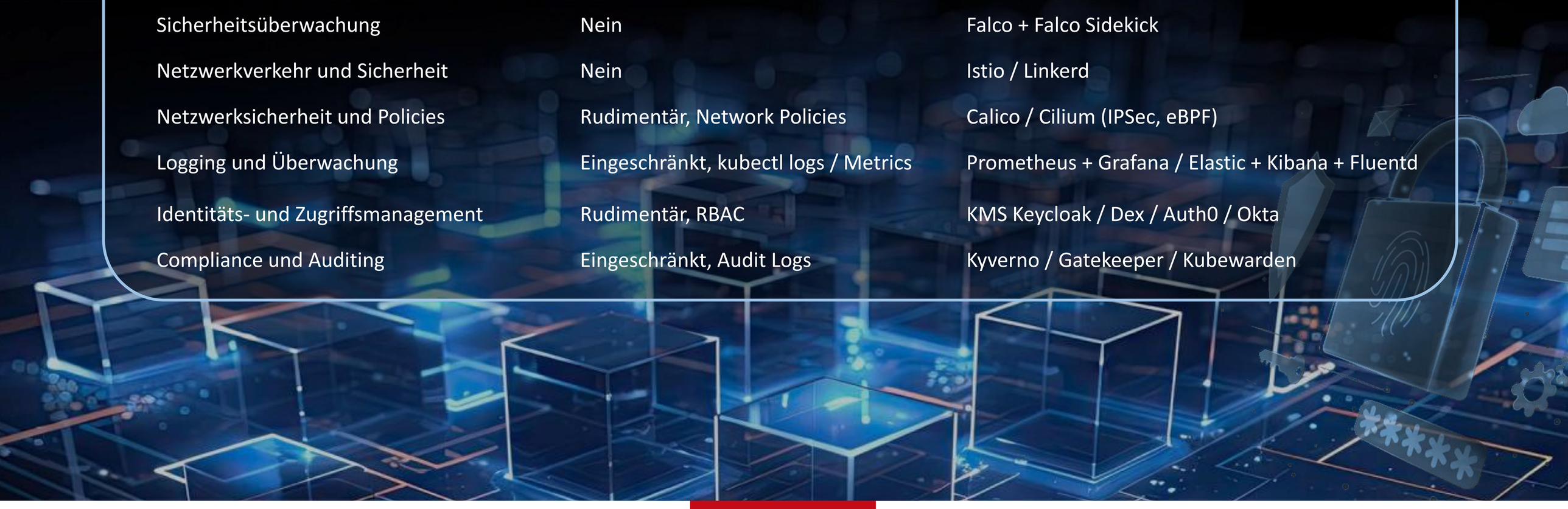
- Vollständige Trennung vom Internet, um Sicherheitsrisiken zu minimieren, oder:
- Nur vertrauenswürdige Quellen (Proxy-Server, Whitelisting).
- Sicherstellen, dass die Kube-API nicht exponiert ist.
- Grundlegende Zugriffskontrollen (kein umfangreiches RBAC erforderlich).

PROD Absicherung

- Implementierung eines Zero-Trust-Modells (kontinuierliche Überprüfung und Verifizierung von Zugriffen).
- Nutzung von RBAC zur granularen Steuerung der Zugriffsrechte.
- Encryption in transit und in rest.
- Netzwerksegmentierung und Sicherheitsrichtlinien für den Datenverkehr zwischen Pods.
- Einsatz von IDS/IPS-Systemen zur Überwachung.
- Regelmäßige Penetrationstests und Schwachstellenanalysen.
- Nutzung von SIEM-Systemen zur Echtzeitüberwachung und Analyse von Sicherheitsvorfällen.

Eine praxisorientierte Vertiefung ermöglichte die Entwicklung einer absichtlich vulnerablen, containerisierbaren Anwendung, ihre Integration in eine CI/CD-Pipeline auf GitLab und das Deployment auf ein Vanilla Kubernetes Cluster. Mit Tools wie Kube-Kov, Kubestriker und Kube-bench wurden Sicherheitsüberprüfungen durchgeführt, um potenzielle Eintrittspunkte, Privilegieneskalation, laterale Bewegungen (Side-Travelling), Discovery und Zugriffe auf externe Infrastrukturen zu erkennen und zu analysieren. Nach den Tests hat sich gezeigt, dass eine Vielzahl an kostenlosen sowie kostenpflichtigen Tools existiert, die Vanilla Kubernetes helfen, abzusichern. Eine Red Hat-Studie aus 2023 zeigt, dass viele Unternehmen Sicherheit als opt-in statt by-design betrachten.

FEATURE	K8S VANILLA	DRITTANBIETER
Geheimnisverwaltung	Rudimentär, Secrets	HashiCorp Vault (EaaS)
Sicherheitsüberwachung	Nein	Falco + Falco Sidekick
Netzwerkverkehr und Sicherheit	Nein	Istio / Linkerd
Netzwerksicherheit und Policies	Rudimentär, Network Policies	Calico / Cilium (IPSec, eBPF)
Logging und Überwachung	Eingeschränkt, kubectl logs / Metrics	Prometheus + Grafana / Elastic + Kibana + Fluentd
Identitäts- und Zugriffsmanagement	Rudimentär, RBAC	KMS Keycloak / Dex / Auth0 / Okta
Compliance und Auditing	Eingeschränkt, Audit Logs	Kyverno / Gatekeeper / Kubewarden



h_da hochschule darmstadt informatik

member of EUT+ EUROPEAN UNIVERSITY OF TECHNOLOGY

MATERNA

Praxisprojekt 2
Informatik Dual
2025

Gruppe B