TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

TeleTrusT + GovTech Kooperations-Workshop

Berlin, 16.06.2026

Sicherer Betrieb im Deutschland-Stack

Steffen Heyde, secunet

Sicherer Betrieb

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Ein ganzheitliches Informationssicherheitsmanagement bildet das Fundament für einen resilienten und vertrauenswürdigen Deutschland-Stack Betrieb.

Risikomanagement

Risikoanalysen, Sicherheitskonzepte und kontinuierliches Monitoring als Basis aller Maßnahmen

Technische Absicherung

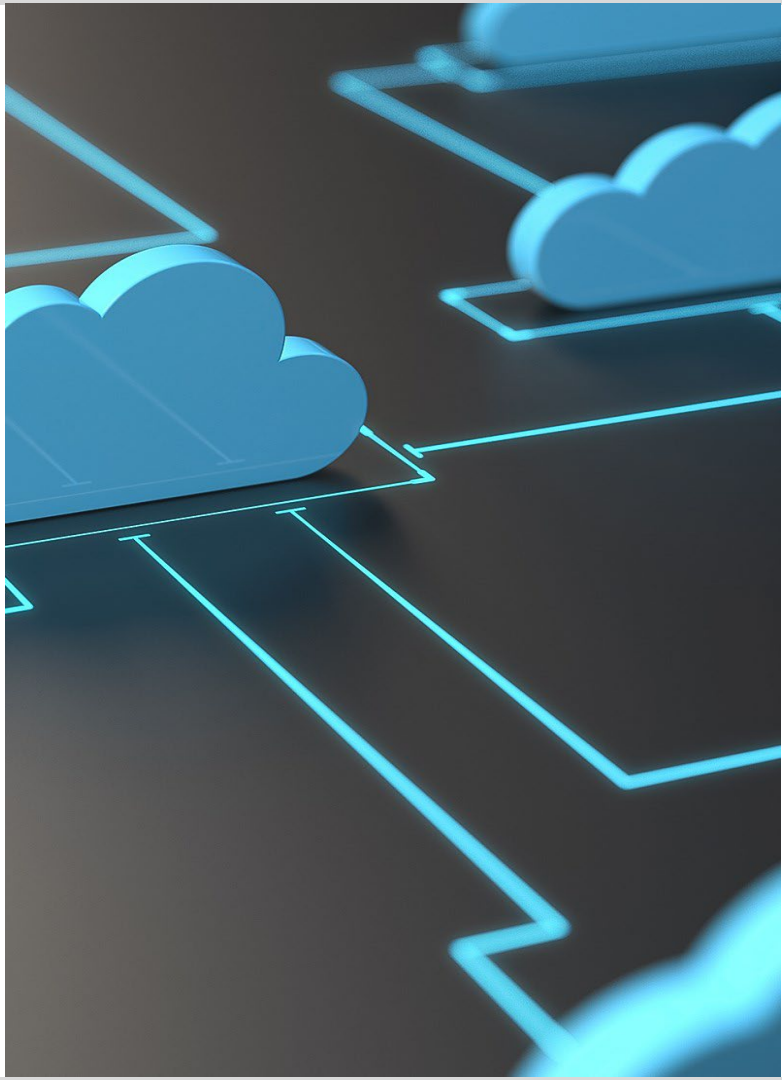
u.a. Starke Authentisierung, Kryptographie, SIEM/IDS/IPS, Firewall- und Key-Management-Systeme

DevSecOps & Standards

Automatisierte Betriebsprozesse nach ISO 27001, BSI-Grundschutz, C5, ISO 27017 + 27018

Policies & Härtung

Komponentenspezifische Härtungsvorgaben und standardisierte Sicherheitsrichtlinien



Sicherheitsmanagement und Governance als organisatorisches Rückgrat des Deutschland-Stacks

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

1

Umfassende Risikoanalyse

Als Grundlage aller Sicherheitsmaßnahmen ist eine strukturierte Risikoanalyse durchzuführen, die Bedrohungen, Schwachstellen und Auswirkungen systematisch bewertet.

2

Lebenszyklus-Sicherheitskonzepte

Sicherheitskonzepte sind zu erstellen, regelmäßig zu pflegen und über den gesamten Lebenszyklus fortzuschreiben – von der Spezifikation bis zur Außerbetriebnahme.

3

Frühzeitige Integration von Sicherheitsanforderungen

Sicherheitsanforderungen müssen bereits in Spezifikation, Umsetzung, Test und Betrieb aktiv berücksichtigt werden – nicht nachträglich hinzugefügt.

4

Kontinuierliche Verbesserung

Regelmäßige Audits, Penetrationstests und Schwachstellenanalysen sichern eine dauerhafte Erhöhung des Sicherheitsniveaus.

Der Deutschland-Stack erfordert einen abgestimmten Werkzeugkasten bewährter Sicherheitstechnologien, u.a.

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

SIEM & IDS/IPS

Zentrale Erfassung und Korrelation von Sicherheitsereignissen mit automatischer Bedrohungserkennung

Firewalls & Netzwerksicherheit

Mehrschichtige Absicherung der Netzwerkinfrastruktur durch segmentierte Firewall-Architekturen und weiteren Netzwerk-Sicherheitsmaßnahmen im Software Defined Network

Kryptographie & Key-Management

Sichere Schlüsselverwaltung, Geheimnisverwaltung und standardisierte Protokolle wie HTTPS, NTP/NTS

Backup & Recovery

Robuste Sicherungsverfahren mit integrierter Wiederherstellungsfähigkeit und Integritätsprüfung

Erkennung, Bewertung und Reaktion auf Sicherheitsvorfälle – bevor sie zu Schäden führen.

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

1

Erfassung

Zentrale Sammlung von Metriken, Logs und Ereignissen aus allen Systemkomponenten des Deutschland-Stacks.

2

Visualisierung

Aufbereitung und Auswertung sicherheitsrelevanter Daten in Echtzeit-Dashboards für schnelle Entscheidungsfindung.

3

Alarmierung

Automatisierte Benachrichtigung bei Störungen oder Sicherheitsvorfällen – ohne manuelle Verzögerung.

4

Auditierung

Kontinuierlicher Überwachungs- und Auditierungsprozess zur nachhaltigen Sicherstellung des Sicherheitsniveaus.

Der Deutschland-Stack muss auch unter Störungs- oder Angriffsszenarien verlässlich funktionieren

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Hohe Verfügbarkeit

Redundanz, Georedundanz und automatisierte Failover-Mechanismen gewährleisten kontinuierlichen Betrieb auch bei Teilausfällen.

Fehlertoleranz & Auto-Healing

Fehlertolerante Systeme mit automatischer Fehlererkennung und Selbstheilungsmechanismen minimieren Ausfallzeiten ohne menschliches Eingreifen.

Backup & Wiederherstellung

Robuste Backup-Verfahren und erprobte Wiederherstellungsprozesse sind regelmäßig zu testen und zu dokumentieren.

Notfallmanagement

Ein etabliertes Verfügbarkeitsmanagement mit klaren Eskalationswegen und Notfallwiederherstellungsplänen ist zwingend vorzuhalten.

DevSecOps verankert Sicherheit als integralen Bestandteil aller Betriebsprozesse des Deutschland-Stacks.

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- Sichere Deployment-Strategien mit Rollback-Fähigkeit
- Sicherheitsprüfungen als verpflichtender Pipeline-Schritt
- Schwachstellenmanagement im laufenden Betrieb
- Vollständige Nachvollziehbarkeit aller Freigaben und Auslieferungen

Rechtzeitige Informationen zur Roadmap an Betreiber und Plattform-Nutzer (Software-Entwickler)

01

Entwicklung

Sicherheitsanforderungen bereits im Design verankern (Secure by Design).

02

Test

Automatisierte Security-Tests und Schwachstellenscans in der Pipeline.

03

Bereitstellung

Standardisiertes Lebenszyklusmanagement mit Härtungsvorgaben.

04

Betrieb

Kontinuierliches Monitoring, Patch-Management und Incident Response.

05

Außerbetriebnahme

Abhängigkeiten bewerten, Berechtigungen ändern, Daten migrieren / sicher löschen.

Compliance und Standards - Basis für die Vertrauenswürdigkeit des Deutschland-Stacks

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Internationale Normen

- **ISO/IEC 27001** – Informationssicherheitsmanagement
- **ISO/IEC 27017** – Cloud-Sicherheit
- **ISO/IEC 27018** – Datenschutz in der Cloud
- **ISO/IEC 20000** – IT-Service-Management
- **ITIL** – Leitfaden für das IT-Service-Management

Nationale & Europäische Regelwerke

- **BSI IT-Grundschutz** – Deutscher Sicherheitsstandard
- **BSI C5** – Cloud Computing Compliance Controls
- **DSGVO & BDSG** – Datenschutzrecht
- **NIS-2** – Netz- und Informationssicherheit
- **eIDAS** – Elektronische Identifizierung & Vertrauen
- **BSI Technische Richtlinien**

Unsere Botschaft an das Digitalministerium

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

„Wenn der Deutschland-Stack wirklich sicher, souverän und vertrauenswürdig *sein soll, braucht es frühzeitig die Perspektive unabhängiger IT-Sicherheitsexpertinnen und Experten – TeleTrusT steht bereit, diese Verantwortung mitzutragen.“*

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Telefon +49 30 400 54 310

info(at)teletrust.de