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

TeleTrusT-Konferenz

Berlin, 26.06.2026

Deutschland-Stack

Dr. Kim Nguyen, Bundesdruckerei / TeleTrusT-Vorstand

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

Warum der Deutschland-Stack mehr ist als ein Technologieprojekt

Eine Sicherheits- und Souveränitätsfrage für die staatliche Digitalisierung

Digitale Handlungsfähigkeit
Öffentliche Dienste müssen auch unter Störung, Angriff und Krisenbedingungen funktionieren.

Vertrauen
Bürgerinnen, Bürger und Unternehmen müssen sich auf digitale Verwaltungsinfrastrukturen verlassen können.

Kontrolle
Souveränität entsteht durch kontrollierbare Daten, Zugriffe, Schlüssel, Betrieb und Wechselpfade.

Krisenfestigkeit
Der Stack muss nicht nur im Regelbetrieb, sondern auch im Vorfall belastbar bleiben.

Die entscheidende Frage ist nicht: „Welche Tools nutzen wir?“

Sondern: Wie sichern wir Kontrolle, Sicherheit und Wechselfähigkeit über den gesamten Lebenszyklus?

Souveränität ist kein Label – sondern eine Steuerungsleistung.

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

Kernthese des Positionspapiers

Vom Technologiekatalog zum verbindlichen Sicherheits- und Betriebsmodell

Cybersicherheit darf im Deutschland-Stack nicht als nachgelagerter Baustein oder Sammlung einzelner Sicherheitsprodukte verstanden werden. Sie ist ein durchgängiges Struktur- und Betriebsprinzip des gesamten Stacks.

Governance
Verantwortung & Zielbild

Architektur
Security by Design

Betrieb
Kontrollierter Betrieb

Resilienz
Recovery & Nachweis

D-Stack secure by design

Basierend auf dem TeleTrusT Positionspapier „Cybersicherheit im Deutschland-Stack"

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

Leitbild: Informations- und Cybersicherheit

Der Sicherheitsbegriff muss weiter gefasst werden als klassische IT-Sicherheit

Informationen & Daten
Schutzbedarf, Klassifizierung, Integrität und Vertraulichkeit

Identitäten & Zugriffe
starke Authentisierung, privilegierte Zugriffe, Least Privilege

Infrastruktur & Betrieb
Segmentierung, Monitoring, Logging und technische Kontrollpunkte

Recovery & Krisenfähigkeit
Wiederherstellung, Notfallprozesse und belastbare Nachweise

Sicherheit muss alle Layer des Stacks und alle Betriebsphasen durchdringen.

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

Souveränität entsteht durch Kontrolle

Nicht durch Labels – sondern durch nachweisbare Steuerungsfähigkeit

Daten
Speicherung, Verarbeitung, Zugriff

Schlüssel
Kryptographie, Key Management, HSM

Zugriffe
Identitäten, Geräte, Kontexte, Rollen

Betrieb
Prozesse, Logs, Privilegien, Audits

Schnittstellen
Offene Standards, API-first, Interoperabilität

Wechselpfade
Portabilität, Exit, Anbieteroptionen

Leitfrage

Was muss der Staat auch unter Druck selbst steuern, prüfen und wechseln können?

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

Governance-Modell: Der Stack braucht ein Target Operating Model

Rollen, Verantwortlichkeiten und Nachweise müssen föderal tragfähig werden

1 **Sicherheitszielbild**
verbindliche Architektur- und Betriebsanforderungen

2 **Rollen & Verantwortung**
Auftraggeber, Betreiber, Prüfer, Fachverfahren

3 **Kontrollpunkte**
Identität, Segmentierung, Logging, Schlüssel, Recovery

4 **Nachweise**
Audits, Tests, RTO/RPO, Compliance, Reifegrad

5 **Weiterentwicklung**
Standards, Bedrohungslage, Lessons Learned

Ohne Governance bleibt der Deutschland-Stack ein Technologiekatalog. Mit Governance wird er zu einem betreibbaren, auditierbaren und resilienten System.

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

Architektur: Keine Sicherheit im Flickenteppich

Komplexität ist ein Sicherheitsrisiko – Beherrschbarkeit ist ein Sicherheitsziel

Leitprinzip: Nur so komplex wie nötig – funktional nur so umfangreich wie erforderlich.

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

Cloud und Managed Services richtig einordnen

Betriebsformen – keine Sicherheits- oder Souveränitätsgarantie

Cloud
ist eine Frage von Betriebsort

Managed Services
ist eine Frage von Betriebsform

Souveränität
ist eine Frage von Kontrolle

Entscheidend ist, ob die Sicherheitslogik unabhängig vom Betriebsort erhalten bleibt:

- **Zugriffskontrolle & Segmentierung**
- **Protokollierung & Prüfbarkeit**
- **Recovery & Exit-Fähigkeit**

Verträge ersetzen keine technische Kontrolle, aber technische Kontrolle ersetzt auch keine Verträge.

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

Zero Trust und Defense in Depth als Mindestlogik

Zugriff wird identitäts-, kontext- und ressourcenbezogen entschieden

1	2	3	4	5
Identität **Wer greift zu?**	**Gerät** **Ist der Zustand vertrauenswürdig?**	**Kontext** **Passt Zeit, Ort, Risiko?**	**Ressource** **Welche Anwendung / welches Datum?**	**Privileg** **Minimal, befristet, protokolliert**

- Kein implizites Vertrauen in Netzsegmente oder Standorte
- Keine System- oder Netzwerksichtbarkeit ohne explizite Autorisierung
- Ressourcen- und anwendungszentrierter Zugriff statt pauschalem Netzwerkzugang

Zero Trust ist kein Produkt – sondern eine durchzusetzende Betriebslogik.

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

Resilienz: Wiederherstellung ist Teil des Betriebs

Prävention allein reicht nicht aus – entscheidend ist die Wiederanlauffähigkeit

Getrennte Backup-Domänen
Produktiv- und Sicherungssysteme klar trennen

RTO/RPO-Nachweise
Zielzeiten und Datenverluste messbar machen

Restore-Tests
Wiederherstellung regelmäßig realistisch testen

Krisenorganisation
Meldewege, Eskalation, Kommunikation definieren

Recovery ist kein Zusatzservice, sondern ein verbindliches Kriterium für Betriebsfähigkeit.

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

KI-unterstützte Schwachstellenanalyse

Mehr Geschwindigkeit in der Risikoerkennung – aber nur mit Governance

Werkzeug

- Schwachstellen in Code, Konfigurationen und Abhängigkeiten erkennen
- Findings korrelieren und risikobasiert priorisieren
- Muster und Angriffspfade schneller sichtbar machen

Regelungsgegenstand

- Nachvollziehbarkeit und Auditierbarkeit sicherstellen
- Sensible Daten und Modellzugriffe schützen
- Menschliche Validierung kritischer Ergebnisse verbindlich machen

Für das Governance-Modell ist KI-Analyse zugleich Befähiger und Risikoquelle.

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

Die nächsten Schritte: 12-Monats-Agenda

Vom Positionspapier zur operationalisierten Sicherheits- und Governance-Praxis

Q3/2026

Sicherheitszielbild & TOM
Rollen, Mindestkontrollen, föderale Verbindlichkeit

Q4/2026

Referenzarchitekturen & PoCs
D-Stack Reallabor, sichere Betriebsmodelle, Nachweise

Q1/2027

Recovery- & Resilienzrahmen
Testpflichten, RTO/RPO, Audits und Lessons Learned

Q2/2027

Kontinuierliche Weiterentwicklung
Kryptoagilität, BSI-Referenzen, KI-gestützte Analysen

Ohne verbindliche Umsetzung drohen mehr Komplexität, mehr Abhängigkeiten, höhere Kosten und geringere Krisenfestigkeit.

Diskussionsfrage: Wie viel Verbindlichkeit braucht der Deutschland-Stack, um wirklich sicher und souverän zu sein?

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

IT-Planungsrat 50. Sitzung: Was heißt das für Cybersicherheit?

Beschlüsse vom 17.06.2026: Der Deutschland-Stack wechselt von der Zielrichtung in die föderale Umsetzung.

1

Plattformkern wird konkret

Fünf Basiskomponenten; Konzeption und Entwicklung beim Bund mit Unterstützung der FITKO.

2

Anbindung & Finanzierung verbindlicher

Länder sagen Anbindung und Flächendeckung zu; der Bund finanziert zentrale Komponenten überwiegend.

3

Portfoliomanagement institutionalisiert

Portfolio-Board, Priorisierung, Roll-out, Analysen, Controlling und Wirkungsmessung.

4

D-Architektur fortgeschrieben

Architekturartefakte für Plattformkern und Roll-out: Fähigkeitenlandkarte und Funktionsbausteine.

Konsequenz: Wenn Nutzung, Roll-out und Architektur verbindlicher werden, müssen auch Sicherheitskontrollpunkte verbindlich werden.

Quellen: IT-Planungsrat, 50. Sitzung / Pressemitteilung vom 17.06.2026; Beschlüsse B-2026/17-IT und B-2026/28-IT.

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

Fazit: Nur gemeinsam

Nur gemeinsam können wir IT-Sicherheit im Deutschland-Stack etablieren.

1 **Bund & FITKO**
Zielbild, Plattformkern, Finanzierung und Architekturartefakte

2 **Länder & Kommunen**
Anbindung, Flächendeckung, Betrieb und Nachweis

3 **Wirtschaft & Ökosystem**
sichere Komponenten, offene Schnittstellen, Wechselpfade

4 **Security-Community**
Prüfung, Standards, Kryptoagilität und kontinuierliches Review

Aus Technologiekatalogen werden sichere Infrastrukturen erst durch verbindliche gemeinsame Umsetzung.

Souveränität braucht Kontrolle · Sicherheit braucht Architektur · Resilienz braucht Nachweis · Föderalität braucht Verbindlichkeit

Vielen Dank!

Nur gemeinsam können wir IT-Sicherheit im Deutschland-Stack etablieren.

Dr. Kim Nguyen

Ich freue mich auf die Diskussion.

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