PRESSEMITTEILUNG

Bundesverband IT-Sicherheit e.V. (TeleTrusT) kommentiert aktuelle Konzeption des Deutschland-Stack

Berlin, 16.02.2026 - Der Deutschland-Stack ist aus Sicht des Bundesverbandes IT-Sicherheit e.V. (TeleTrusT) eine strategisch richtige und notwendige Initiative, um die digitale Handlungsfähigkeit des Staates langfristig zu sichern. Auch das gewählte Vorgehensmodell eines Konsultationsverfahrens wird ausdrücklich begrüßt. Gleichzeitig zeigt die TeleTrusT-Analyse: In der aktuellen Ausprägung ist der Deutschland-Stack noch zu stark als technische Bausteinliste gedacht. Für belastbare Wirkung im öffentlichen Sektor ist ein klar geführtes Gesamtbetriebsmodell aus Architektur, Governance, Sicherheit und Verantwortung erforderlich.

https://www.teletrust.de/publikationen/stellungnahmen/2026/

Aus Sicht von TeleTrusT stellt der Deutschland-Stack eine wesentliche Initiative dar, um die digitale Infrastruktur insbesondere im Public Sector resilient, skalierbar und zukunftsfähig aufzustellen. Insofern begrüßt TeleTrusT sowohl das Vorhaben selbst als auch den gewählten Weg der Konsultation mit einer breiten Einbeziehung aller relevanten Stakeholder ausdrücklich. In einem aktuellen TeleTrusT-Positionspapier wird neben zahlreichen inhaltlichen Kommentierungen, Ergänzungen und Anmerkungen dargestellt, dass der Deutschland-Stack mehr sein muss als eine reine "Ansammlung" technischer Standards, Module und Services.

TeleTrusT ist überzeugt, dass die gewünschten Anforderungen an den Deutschland-Stack nur dann erfüllt werden können, wenn neben den erforderlichen technischen Festlegungen auch ein Betriebs-, Governance- und Infrastrukturmodell entwickelt wird, das die unterschiedlichen technischen Elemente verbindet. Dies gilt insbesondere für den Bereich der Informations- und Cyber-Sicherheit, genauso aber auch für notwendige Elemente wie Skalierbarkeit, Verfügbarkeit und Resilienz. Dabei handelt es sich um Eigenschaften, die sich nicht allein durch das Zusammenfügen geeigneter Technologien und Standards ergeben, sondern sie erfordern ein geeignetes Zusammenspiel und Zusammenwirken von Technologie, Infrastruktur und Governance. Dies kann nur erreicht werden, wenn all das bereits von Anfang an konsequent in den Architekturzielen und -prinzipien mitgedacht wird.

Die Ausrichtung von Standards und Technologien passt grundsätzlich zu den strategischen Zielen (Souveränität, Sicherheit, Interoperabilität, Zukunftsfähigkeit, Resilienz), wenn sie nicht als reine Tool-/Bausteinliste verstanden wird, sondern als verbindlich gesteuertes Gesamtmodell.

Es gibt jedoch Lücken in der aktuellen Konzeption:

1. Zu starke Technologiekatalog-Logik
   Es fehlt ein verbindliches Target Operating Model aus Architektur, Governance, Betrieb und Verantwortung.
2. Sicherheitsrahmen nicht durchgängig genug
   Einzelstandards (z.B. AES/RSA, OAuth/OIDC/JWT) reichen nicht; nötig ist ein lifecycle-basiertes Sicherheitsmanagement mit Risiko-, Audit- und Verbesserungszyklus.
3. Teilweise unklare/inkonsistente Standardreferenzen
   Insbesondere bei Kryptografie wird auf bessere Anbindung an aktuelle BSI-Vorgaben (TR-02102) hingewiesen.
4. Komplexitätsrisiko
   Ohne ganzheitliche Infrastruktur droht ein "Flickenteppich", der Sicherheit, Betrieb und Skalierung verschlechtert.
5. Cloud/Managed Services missverstanden
   TeleTrusT betont: Das sind Betriebsmodelle, keine Sicherheitsgarantie. Sicherheit entsteht durch Architektur und technische Kontrollpunkte.

Die priorisierten Technologiefelder sind in Teilen mit relevanten Technologien und Standards unterlegt (vor allem Infrastruktur, Betriebsmodelle, Sicherheitsprinzipien), aber noch nicht vollständig. Es fehlen zentrale Security- und Betriebsbausteine, eine konsolidierte Standardreferenz (insbesondere Kryptografie nach BSI) und eine durchgängige, verbindliche Methodik statt punktueller Nennungen. TeleTrusT empfiehlt eine Klärung der Umsetzungsverbindlichkeit der Vorgaben des Deutschland-Stack für die verschiedenen Stakeholder (insbesondere Bund, Länder und Kommunen). Dabei ist aus Sicht von TeleTrusT die Verbindlichkeit der Vorgaben des Deutschland-Stack zur Informations- und Cyber-Sicherheit von besonderer Relevanz.

Für das weitere Verfahren bietet TeleTrusT dem BMDS aktive Unterstützung und Mitwirkung an.

Bundesverband IT-Sicherheit e.V. (TeleTrusT), Dr. Holger Mühlbauer, Geschäftsführer, Chausseestraße 17, 10115 Berlin, Tel.: +49 30 40054310, holger.muehlbauer@teletrust.de
https://www.teletrust.de