PRESSEMITTEILUNG

TeleTrusT-Positionspapier: "IT-Sicherheit im Deutschland-Stack"

Berlin, 29.05.2026 - Cyber-Sicherheit darf im Deutschland-Stack nicht als nachgelagerter Baustein oder als Sammlung einzelner Sicherheitsprodukte verstanden werden. Sie ist ein durchgängiges Struktur- und Betriebsprinzip des gesamten Stacks und muss in Governance, Architektur, Standards, Zugriffsmodell, Betriebsmodell und Resilienz verbindlich verankert werden. Das TeleTrusT-Positionspapier "IT-Sicherheit im Deutschland-Stack" verdichtet diese Anforderungen zu einem eigenständigen cyberpolitischen und architektonischen Zielbild für den Deutschland-Stack.

www.teletrust.de/publikationen/broschueren/cyber-nation/

TeleTrusT-Forderungen:

1. Der Deutschland-Stack darf nicht als reines Digitalisierungs-, Cloud- oder Plattformprojekt verstanden werden, sondern als sicherheitskritische nationale Infrastruktur.

2. Informations- und Cyber-Sicherheit müssen deshalb von Beginn an als tragende Architektur-, Governance- und Betriebsprinzipien verankert werden.

3. Sicherheit darf nicht auf klassische IT-Sicherheit einzelner Systeme reduziert werden, sondern muss Identitäten, Zugriffe, Daten, Infrastruktur, Lieferketten, Betrieb, Resilienz und Wiederherstellbarkeit ganzheitlich umfassen.

4. Digitale Souveränität entsteht nur dann, wenn kritische Abhängigkeiten technisch, organisatorisch und betrieblich beherrschbar bleiben.

5. Der Deutschland-Stack benötigt daher überprüfbare Mindestanforderungen an Architektur, Beschaffung, Betrieb, Auditierbarkeit und Krisenfähigkeit.

6. Zero Trust ist ein wichtiger Ausgangspunkt, sollte für staatliche und kritische Infrastrukturen jedoch nicht als Endzustand verstanden werden.

7. Für besonders schutzbedürftige Bereiche sollten vom BSI überprüfte Systeme zum Einsatz kommen, die den Umsetzungen z.B. der vollumfänglichen Anforderungen nach VSA genügen und die aktuellen Entwicklungen zu (Post)-Zero-Trust, Identitäten, Authentifizierung etc. bestmöglich berücksichtigen.

8. Entscheidend ist, dass Nutzer und Endgeräte keinen allgemeinen Netzwerkzugang erhalten, sondern nur kontrollierten Zugriff auf konkret freigegebene Anwendungen und Dienste.

9. Resilienz muss außerdem durch belastbare Backup-/Restore- und Site-Recovery-Plattformen ergänzt werden, damit kritische Systeme im Ernstfall nicht erst neu beschafft, installiert und wiederhergestellt werden müssen, sondern kurzfristig weiterbetrieben werden können.

10. Der Erfolg des Deutschland-Stacks wird sich letztlich daran messen lassen, ob er nicht nur im Regelbetrieb funktioniert, sondern auch unter Angriffen, Ausfällen, Lieferkettenstörungen und Krisen souverän, sicher und wiederherstellbar bleibt.

Die aktuelle Bedrohungslage durch staatliche Akteure, organisierte Kriminalität, komplexe Lieferketten, Schwachstellen in Cloud- und Software-Ökosystemen sowie steigende Abhängigkeiten von nicht-europäischen Plattformen macht deutlich: Der Deutschland-Stack muss von Beginn an als Sicherheits- und Souveränitätsarchitektur gedacht werden.

Der Deutschland-Stack verfolgt das richtige strategische Ziel: digitale Handlungsfähigkeit, Nachnutzbarkeit, Interoperabilität, Resilienz und Souveränität im öffentlichen Sektor zu stärken. Aus Sicht der Cyber-Sicherheit reicht es jedoch nicht aus, Technologien und Standards aufzuzählen. Entscheidend ist, wie diese in einem beherrschbaren, auditierbaren und resilienten Gesamtmodell zusammenwirken. Cyber-Sicherheit ist dabei kein eigener Layer neben anderen, sondern eine Querschnittsanforderung an alle Layer des Stacks sowie an Governance und Betrieb, die zudem der regelmäßigen Aktualisierung und Anpassung an den Stand der Technik unterliegt.

Der Deutschland-Stack muss zu einem zentralen Baustein digitaler Souveränität und Sicherheit in Deutschland werden und zugleich auch als sicherheitskritische nationale Infrastruktur verstanden werden. Dafür muss Cyber-Sicherheit jedoch als Ordnungsprinzip verstanden werden: nicht als isolierter Sicherheitsblock, sondern als verbindende Logik von Architektur, Betrieb, Kontrolle und Wiederherstellung.

Ein souveräner Deutschland-Stack ist nicht der Stack mit den meisten Technologien, sondern der Stack mit der höchsten Beherrschbarkeit, der klarsten Verantwortungsstruktur und der nachweisbarsten Resilienz. Entscheidend ist, dass der Deutschland-Stack nicht nur funktional, sondern auch im Krisen-, Angriffs- und Ausfallszenario belastbar bleibt. Das ist die Voraussetzung dafür, dass öffentliche digitale Infrastrukturen auch unter Krisenbedingungen vertrauenswürdig, belastbar funktionsfähig und weiterentwickelbar bleiben.

Das Positionspapier wurde in der TeleTrusT-Arbeitsgruppe "Cyber-Nation" unter der Leitung von TeleTrusT-Vorstand Dr. Kim Nguyen (Bundesdruckerei) erarbeitet.

Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breitgefächerte Mitgliederschaft und die Partnerorganisationen verkörpert TeleTrusT den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrusT bietet Foren für Fachleute, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrusT ist Träger der "TeleTrusT European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Personenzertifikate "TeleTrusT Information Security Professional" (T.I.S.P.) und "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) sowie der Vertrauenszeichen "IT Security made in Germany" und "IT Security made in EU". TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

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