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

TeleTrusT + GovTech Kooperations-Workshop

Berlin, 16.06.2026

Sicherer Zugriff und resilienter Betrieb im Deutschland-Stack

Yakup Saygin, SAYTEC

Die vorhandenen Impulse liegen richtig – jetzt braucht es die technische Zielarchitektur

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

Unsere Arbeitsgruppe sollte daraus konkrete Mindestanforderungen für Zugriff, Betrieb und Resilienz ableiten.

1

Identitätsmanagement

Digitale Identitäten, föderierte Vertrauensinfrastruktur, SSO, OTP, Rollen/Vollmachten und EUDI-Wallet-Anbindung sind die Basis für Vertrauen.

2

Sicherer Betrieb

ISMS, Risikoanalysen, Monitoring, SOC, DevSecOps, Härtung, Standards, Backup und Wiederherstellung bilden das organisatorische Rückgrat.

3

Fehlende Verbindung

Entscheidend ist die technische Referenzarchitektur: Wie entstehen Kommunikation, Zugriff, Verschlüsselung, Datenintegrität und Wiederanlauf wirklich?

Unsere Aufgabe ist, daraus eine verbindliche Sicherheits- und Betriebsarchitektur abzuleiten.

Leitproblem: Komponentensicherheit ist noch keine Betriebsarchitektur

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

Der Deutschland-Stack braucht verbindliche technische Leitplanken über Zugriff, Betrieb und Wiederanlauf.

1 · Zugriff

VPN verbindet Netze. Hochsicherheit braucht kontrollierte Kommunikation zu Anwendungen.

2 · Betrieb

Virtualisierung, Storage, Netzwerkdienste und Kubernetes dürfen keine getrennten Silos bleiben.

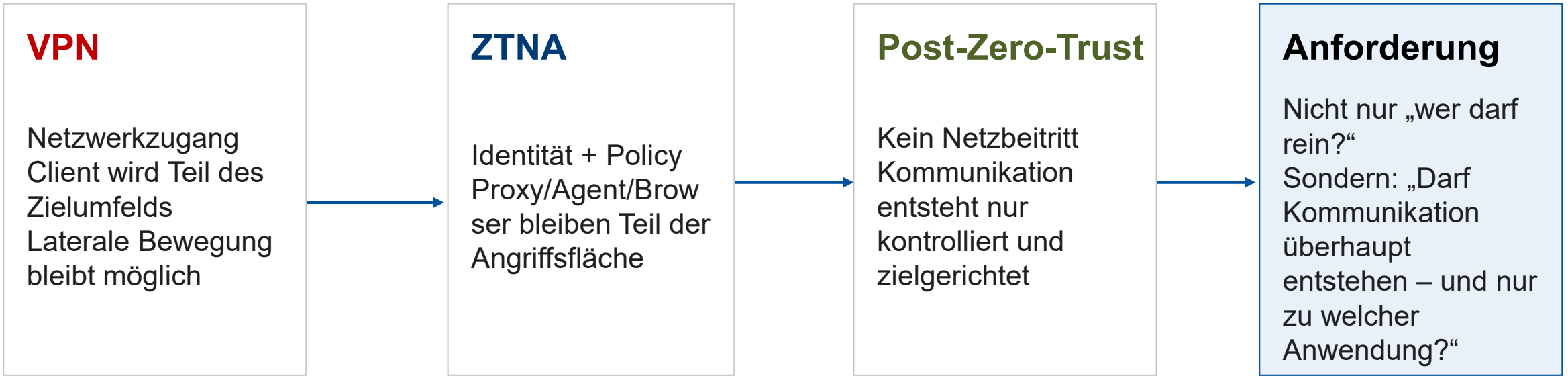
3 · Wiederanlauf

Backup allein ist kein Wiederanlaufkonzept. Resilienz braucht Restore, Disaster Recovery und Integritätsnachweis.

Aus einzelnen Schutzbausteinen muss eine durchgängige Sicherheits- und Resilienzarchitektur entstehen.

Grenze klassischer Zugriffsschutz: VPN und klassische ZTNA reichen für Hochsicherheit alleine nicht aus

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



Für Hochsicherheit reicht Zugriffskontrolle allein nicht. Der kritische Punkt ist die Entstehung der Kommunikation vor der ersten Verbindung.

Definition der Schutzanforderungen entlang der gesamten Kommunikationsstrecke – von der Entstehung bis zum Zielzugriff.

Mindestanforderungen an Hochsicherheits-Zugriff: Zugriff als kontrollierte Kommunikationsarchitektur

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

Der Nutzer arbeitet nicht im Netzwerk — sondern ausschließlich in autorisierten Anwendungen.

1	2	3	4
Identität vor Kommunikation Keine Sichtbarkeit, kein Tunnel, kein Datenfluss ohne erfolgreiche Authentisierung.	**Zero Device Trust** Das Endgerät wird nie Teil des Zielnetzes und erhält keine Netzwerkinformationen.	**Isolierter Start** Kommunikation entsteht aus kontrolliertem Kontext, nicht aus unkontrollierter OS-/Browser-Logik.	**Anwendung statt Netz** Nur definierte Anwendungen und Zielkommunikation werden freigegeben.

Welche Mindestanforderungen definieren wir für Vertraulichkeit, Integrität, Verschlüsselung und Schlüsselkontrolle im Zugriffspfad?

Grenze klassischer Betriebsmodelle: Sicherheitsbausteine ohne Resilienzarchitektur bleiben Silos

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

Der sichere Zugriff braucht ein belastbares Fundament: Betrieb, Daten, Wiederherstellbarkeit und Skalierbarkeit müssen zusammen gedacht werden.

Heute oft getrennt

Virtualisierung
Storage
Netzwerkdienste
Backup / Recovery
Kubernetes / VDI
Monitoring / Betrieb

→

Anforderung

Eine souveräne Betriebsplattform muss die Bausteine gekapselt, kontrolliert, mandantenfähig und wiederherstellbar verbinden.

→

Praxisbeitrag

Praxisbeitrag von sayTEC: sayFUSE zeigt beispielhaft, wie HCI, NaaS, Storage, Backup, Recovery und Mandantenfähigkeit integriert verbunden werden können.

Resilienz ist keine Zusatzfunktion. Sie muss Bestandteil der Betriebsarchitektur sein — inklusive Backup, Integritätsprüfung, Redundanz, Failover und Wiederanlauf.

Was wir gemeinsam festlegen sollten

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

Ziel: eine Referenzarchitektur für sicheren Zugriff und resilienten Betrieb im Deutschland-Stack.

1 · Zugriff

Mindestanforderungen jenseits von VPN und klassischem ZTNA: Identität, Zero Device Trust, kein Netzbeitritt, Anwendung statt Netz.

2 · Vertraulichkeit & Integrität

Verschlüsselung über Zugriff, Transport, Datenhaltung, Verarbeitung, Backup und Wiederherstellung; Schlüsselkontrolle, Confidential Computing und Integritätsnachweis.

3 · Betrieb & Resilienz

Virtualisierung, Storage, Kubernetes, Netzwerkdienste, Backup, Redundanz, Georedundanz und Wiederanlauf als Gesamtsystem.

4 · Nachweisbarkeit

SOC, Monitoring, Audit, DevSecOps, Härtung, Standards und Tests als verbindliche Betriebsnachweise.

Ergebnis sollte sein: GovTech und TeleTrusT eine Empfehlung für eine vertiefende Arbeitsgruppe „Sichere Betriebsarchitektur für Deutschland-Stack“ mit Referenzarchitektur, Schnittstellen und Demonstrator ausarbeiten.

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

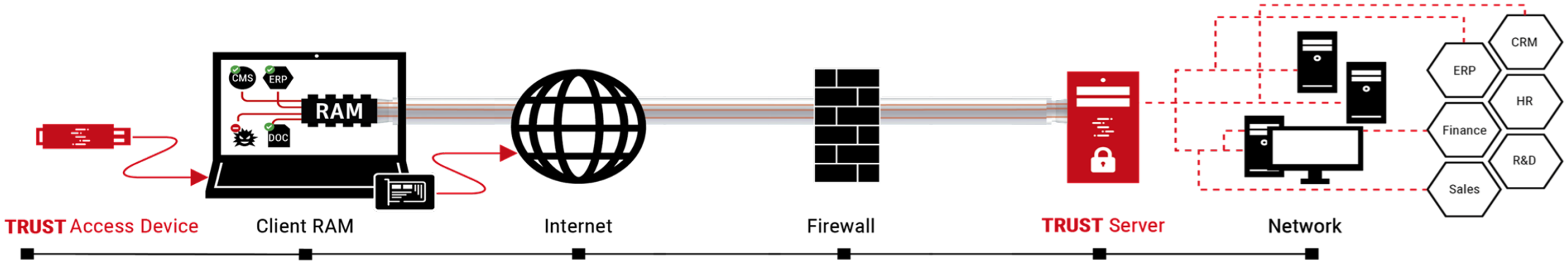
info(at)teletrust.de

Reservefolie zur Vertiefung:
Was bedeutet kontrollierte Kommunikationsentstehung?

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

Viele Ansätze kontrollieren den Zugang — aber nicht konsequent die Entstehung und Isolation der Kommunikation.

VPN - Netzwerkzugang, Client wird Teil des Zielumfelds, laterale Bewegung bleibt möglich.
Klassisches ZTNA - Identität und Policy sind wichtig, aber Proxy, Agent oder Browser bleiben Teil der Angriffsfläche.



1 Identität & Token
Biometrie / PIN / Zertifikat / OTP

2 RAM-Tunnel
Zero Footprint im Client-RAM

3 PFS & Gateway
temporäre Schlüssel, kein Mithören

4 App-Kontrolle
autorisierte Anwendungen statt Netze

Kernaussage:
Nicht der Benutzer kommt ins Netz — nur die freigegebene Anwendung wird kontrolliert erreichbar.