

Deutschland-Stack und Cybersicherheit - Von der Governance zum sicheren Betrieb

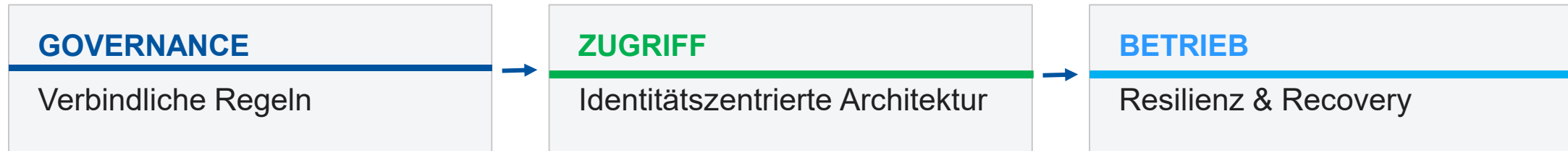
Prof. Dr. Norbert Pohlmann, TeleTrust Vorstandsvorsitzender

Dr. André Kudra, TeleTrust Vorstand

Yakup Saygin, Mitglied TeleTrust-AG "Cyber-Nation"

Deutschland-Stack und Cybersicherheit

Von der Governance zum sicheren Betrieb



Sicherer Zugriff statt Sicherheits-Flickenteppich

Sicherer Zugriff statt Sicherheits-Flickenteppich

AUFGABENSTELLUNG

Brauchen wir immer mehr Sicherheitsprodukte?

Oder eine Architektur, in der bestimmte **Angriffsflächen gar nicht erst entstehen?**

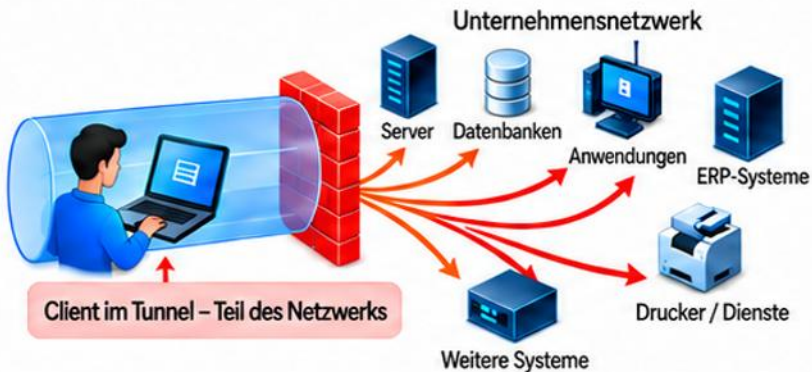
Mehr Komponenten bedeuten nicht automatisch mehr Sicherheit.

GESTERN

VPN

Zugang zum Netzwerk

Der Client wird Teil des Unternehmensnetzwerks.



GEGENWART

Zero Trust

Einschränkungen und Schwachstellen

Zugriff nur nach Identitätsprüfung – aber weiterhin Netzwerkzugang und Angriffsfläche vorhanden.

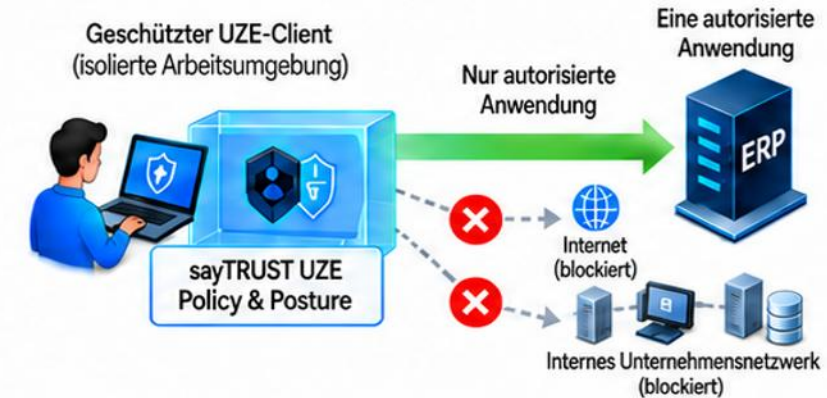


ZUKUNFT

Post Zero Trust

Gezielte Kommunikationsbeziehung

Nur die autorisierte Anwendung. Kein Netzwerkzugang.



Vom Netzwerkzugang ...

... zum kontrollierten Ressourcenzugriff ...

... zur ausschließlich autorisierten Kommunikationsbeziehung.

Schematischer Architekturvergleich. Auch moderne Zero-Trust-/ZTNA-Modelle können anwendungsbezogene Zugriffe ermöglichen.

Die entscheidende Frage

**Warum sollte ein autorisierter Nutzer einen
allgemeinen Netzwerkzugang erhalten,
wenn er nur eine Anwendung benötigt?**

Kein allgemeiner Netzwerkzugang. Nur die benötigte Anwendung autorisieren.

VPN verbindet. Zero Trust kontrolliert. Post Zero Trust isoliert.

Von der Identität zur Anwendung – ausschließlich autorisierte Kommunikation.



KEIN ALLGEMEINER NETZWERKZUGANG. NUR DIE AUTORISIERTE KOMMUNIKATIONSBEZIEHUNG.

Unsichtbare interne Strukturen. Minimale Angriffsfläche. Maximale Sicherheit.



Identität zuerst

Sicherheit beginnt vor dem Verbindungsaufbau.



Prüfung vor Verbindungsaufbau

Policy-Prüfung vor jeder Kommunikation.



Minimale Angriffsfläche

Keine seitlichen Bewegungen, keine Parallelkanäle.



Zero Footprint

Keine dauerhaften Spuren auf dem Client.



Sicher & resilient

Für Unternehmen, Behörden und kritische Infrastrukturen.

Erst prüfen. Dann schützen. Dann verbinden.

Sicherer Zugriff allein genügt nicht.

CYBERRESILIENZ

Was geschieht im Ernstfall?

SYSTEMAUSFALL

Ein kritischer Dienst ist nicht mehr verfügbar.

KOMPROMITTIERUNG

Daten oder Systeme sind nicht mehr vertrauenswürdig.

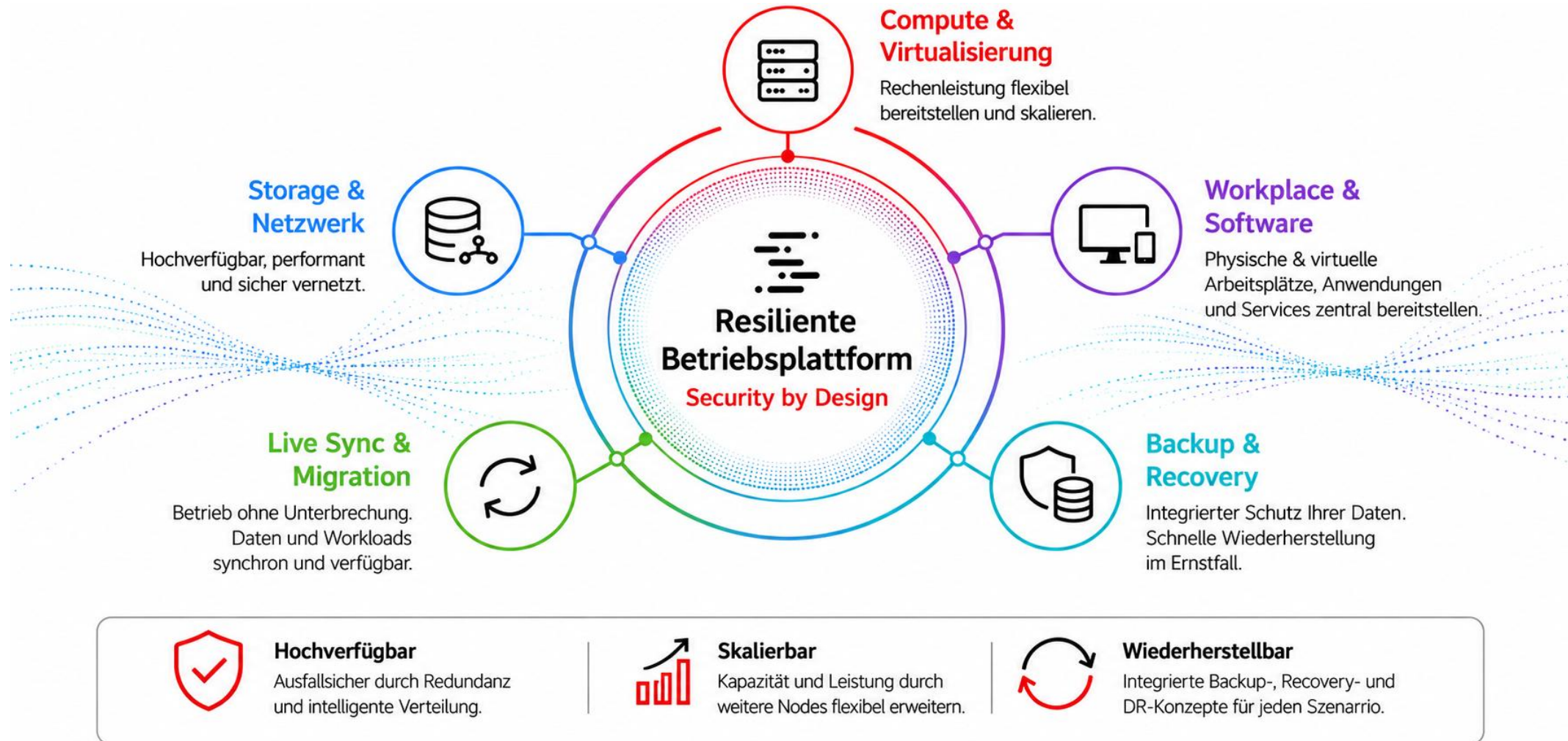
STANDORTAUSFALL

Ein kompletter Betriebsstandort fällt aus.

KRITISCHE DIENSTE AUF VORBEREITETEN ERSATZRESSOURCEN WEITERBETREIBEN

Site-Recovery-Plattform: schneller Wiederanlauf ohne Neubeschaffung und Neuinstallation

Ganzheitlich resiliente IT-Infrastruktur



FAZIT

GOVERNANCE

schafft Verbindlichkeit.

SICHERHEITSARCHITEKTUR

reduziert Angriffsflächen.

RESILIENZ & RECOVERY

sichern Betrieb und Wiederanlauf.

**Digitale Souveränität entsteht durch beherrschbare Architektur –
nicht durch die Anzahl der Technologien.**

Ein gemeinsames Sicherheitsregime für Bund, Länder und Kommunen.



Governance setzt Ziele, klärt Verantwortung und macht Sicherheit überprüfbar.

Sicherer Betrieb: sechs verbindliche Leitplanken

Digitale Souveränität entsteht, wenn Sicherheit über den gesamten Lebenszyklus nachweisbar verankert ist.

1 SECURITY BY DESIGN

Risikoanalysen, Sicherheitskonzepte, Audits, Penetrationstests und kontinuierliche Verbesserung

2 SICHERHEITSARCHITEKTUR

Verfügbarkeitsmonitoring, Perimeter-Schutz, robuste Backups, Key-Management und sichere Protokolle

3 IDENTITÄTEN & MONITORING

Durchgängiges IAM, starke Authentisierung und MFA sowie zentrale Logs, Events und Alarmierung

4 RESILIENZ & RECOVERY

Geo-Redundanz, Failover, Auto-Healing, Wiederherstellung sowie verbindliche Notfall- und Rückfallkonzepte

5 DEVSECOPS & RELEASE-GATES

SAST, SCA, Secret-, Container- und IaC-Scanning, SBOM, signierte Lieferkette und getesteter Rollback

6 STANDARDS & NACHWEISE

ISO/IEC 27001, BSI IT-Grundschutz und C5, NIS-2, eIDAS, DSGVO sowie ISO/IEC 20000 und ITIL

Kein Release ohne Sicherheitsprüfung. Kein Produktivbetrieb ohne Freigabe.

Von der Governance zum sicheren Betrieb

Einladung zu einem Workshop am **Montag, den 14.12.2026** im
GovTech Campus in Berlin mit drei Workstreams zu Governance,
(Hoch)Sicherheit und Infrastruktur & Betrieb
Anmeldung an info@teletrust.de

GOVERNANCE

Verbindliche Regeln
und klare Verantwortlichkeiten

(HOCH)SICHERHEIT

Durchgängiger Schutz
über alle Ebenen

INFRASTRUKTUR & BETRIEB

Verlässliche, resiliente
und wiederanlauffähige Dienste