

DTS

SELF-ASSESSMENT

16 Punkte, 4 Kategorien:

So souverän ist Ihre IT-Infrastruktur aufgestellt.



Sind Sie auf Kurs? Wie digital unabhängig ist Ihr Unternehmen?

Haken Sie ab, was Sie bereits umgesetzt haben. Jeder gesetzte Haken bedeutet mehr Kontrolle und Schutz. Jeder offene Punkt ist ein konkreter Ansatzpunkt für den nächsten Schritt. Das Ziel: alle 16 Punkte abhaken und Ihre IT lückenlos aufstellen.

OPERATIVE IT-SICHERHEIT

☐ 1. US CLOUD Act – Zugriff unabhängig vom Server-Standort
Rechtsrisiko

Seit 2018 können US-Behörden auf Daten bei US-Anbietern zugreifen und das unabhängig vom Serverstandort. Entscheidend ist die Nationalität des Anbieters, nicht die Adresse des Rechenzentrums.

DTS: deutscher Cloud Provider mit zertifizierten Highperformance-Rechenzentren in Herford & Münster

☐ 2. DSGVO-Konformität nachweisbar gewährleisten
Bußgeldrisiko von bis zu 4 % des Jahresumsatzes

Wer personenbezogene Daten bei nicht-europäischen Anbietern verarbeitet, riskiert Verstöße gegen Art. 44 ff. DSGVO. Beispiele hierfür sind Meta mit 1,2 Mrd. € Strafe (2023) & Uber mit 290 Mio. € (2024).

DTS: DTS SOC ist 24/7/365 besetzt – und mit DTS Aviator sehen Sie alle Managed Security Services transparent auf einem Dashboard: gläserne Services statt Blackbox

☐ 3. NIS-2 erfüllen
Pflicht seit dem 06. Dezember 2025

Das deutsche NIS-2-Umsetzungsgesetz ist seit dem 06. Dezember 2025 in Kraft – ohne Übergangsfrist. Es erweitert den Kreis betroffener Unternehmen massiv und verpflichtet die Geschäftsführung zur persönlichen Haftung.

DTS: DTS-Lösungen, -Plattformen und Services sind absolut NIS-2-kompatibel konzipiert

☐ 4. FISA Section 702 – US-Geheimdienstzugriff
im April 2024 verlängert & ausgeweitet

Neben dem CLOUD Act ermöglicht FISA 702 US-Geheimdiensten den Zugriff auf Kommunikationsdaten. Das EU-US Data Privacy Framework ändert daran strukturell nichts.

DTS: Daten und Kommunikation bleiben im deutschen Rechtsraum und befinden sich somit außerhalb der Reichweite von FISA 702

TECHNOLOGISCHE KONTROLLE & UNABHÄNGIGKEIT

☐ 5. Vendor-Lock-in vermeiden *strategische Unabhängigkeit*

Wer die gesamte IT bei einem Hyperscaler bündelt, verliert Verhandlungsmacht, Flexibilität und im Extremfall den Datenzugang. Wie real diese Gefahr ist, zeigte sich 2025, als das Microsoft-Konto des Chefanklägers des IStGH in Folge von US-Sanktionen nicht mehr nutzbar war.

DTS: offene, modulare Architektur mit über 100 herstellerunabhängigen und kombinierbaren Bausteinen

☐ 6. Lieferkette & Software-Herkunft kennen *Supply-Chain-Risiko*

Backdoors, Schwachstellen und geopolitisch motivierte Updates in Software aus Drittstaaten sind keine Hirngespinnste. BSI-Warnungen verdeutlichen das.

DTS: eigenentwickelte Security-Software (Cockpit, Identity, NAC, Aviator) – Herkunft transparent herstellerunabhängig „Made in Germany“ entwickelt

☐ 7. Eigene Verschlüsselungshoheit sicherstellen *Datenkontrolle*

Standard-Cloud-Verschlüsselung reicht nicht: verwaltet der Anbieter die Schlüssel, hat er Zugang zu Ihren Daten. Nur Verschlüsselung unter eigener Hoheit schützt wirklich.

DTS: Schlüsselhoheit bei Ihnen, Datenhaltung in eigenen Tier-III-Rechenzentren in Herford & Münster

☐ 8. OT/KRITIS-Infrastruktur absichern *Betrieb & Sicherheit*

Industrie- und kritische Infrastrukturen benötigen speziell gehärtete Lösungen, welche Maschinen- und IT-Welt zusammenführen.

DTS: DTS OT Insights integriert Maschinenlinien in das zentrale Sicherheits-Cockpit

GESCHÄFT & REPUTATION

☐ 9. Vertrauen von Kunden & Partnern sichern *Reputation*

Ein bekannt gewordener Datenzugriff oder eine Datenpanne können Kunden und Partner dauerhaft verunsichern. Digitale Souveränität hingegen ist ein Wettbewerbsvorteil und Vertrauenssignal.

DTS: „Made in Germany“ als belegbares Vertrauensversprechen, mit striktem Fokus auf EU-Rechtsräume und ganzheitliche IT-Security

☐ 10. Geopolitische Abhängigkeiten reduzieren *Resilienz*

Sanktionen, politische Spannungen oder ein Regierungswechsel können den Zugang zu US-Cloud-Diensten oder anderen außereuropäischen IT-Services einschränken. Europäische Souveränität bedeutet Resilienz

DTS: vollständig europäische, tiefe Wertschöpfung – unabhängig von außereuropäischer Politik

☐ **11. Ausschreibungen & Zertifizierungen gewinnen**
Wettbewerbsvorteil

Öffentliche Auftraggeber, KRITIS-Betreiber und hoch-regulierte Branchen fordern zunehmend den Nachweis einer DSGVO-konformen, souveränen IT.

DTS: DSGVO- & ISO-27001-Nachweise plus souveräne Architektur – damit sind Sie absolut ausschreibungsfähig

☐ **12. Versicherungsfähigkeit für Cyber-Policen sichern**
Finanzen

Cyber-Versicherer fordern nachweisbare Sicherheitsarchitekturen. Ohne ein solches Konzept drohen höhere Prämien – oder gar eine Ablehnung.

DTS: strukturiertes Security-Konzept, u. a. mit SOC, MDR und dokumentierten Maßnahmen.

OPERATIVE IT-SICHERHEIT

☐ **13. 24/7 Monitoring & Incident Response**
Reaktionszeit ist entscheidend

Cyberangriffe passieren nachts, am Wochenende, an Feiertagen und in Urlaubs- bzw. Ferienperioden. Ohne ein besetztes SOC entsteht ein gefährliches Zeitfenster.

DTS: DTS SOC ist 24/7/365 besetzt – und mit DTS Aviator sehen Sie alle Managed Security Services transparent auf einem Dashboard: gläserne Services statt Blackbox

☐ **14. Identitäten & Zugriffsrechte zentral verwalten**
Zugangsdaten

Ein Großteil der Sicherheitsvorfälle beginnt mit kompromittierten Zugangsdaten. IAM, MFA und Zero-Trust-Prinzipien sind keine Kür, sondern Pflicht.

DTS: DTS Identity – IAM/CIAM, FIDO2, passwortlose MFA, NIS-2-konform

☐ **15. Netzwerkzugangskontrolle (NAC) implementieren**
Netzwerkzugang

Unkontrollierte Geräte im Netzwerk sind ein offenes Einfallstor. Network Access Control (NAC) stellt sicher, dass nur autorisierte und konforme Geräte wirklichen Zugang erhalten.

DTS: DTS NAC – das einzige Zero Trust Network Access „Made in Germany“

☐ **16. Notfallplan & Business Continuity getestet**
Ausfallsicherheit

Ein Notfallplan, der nie getestet wurde, ist keiner. Regelmäßige Übungen, Backup-Tests und Disaster-Recovery-Szenarien gehören zu einer souveränen IT-Strategie.

DTS: DTS begleitet Business Continuity, Backup-Strategien und Disaster Recovery – inklusive Hosting in eigenen Hochleistungsrechenzentren

DTS

SELF-ASSESSMENT

16 Punkte, 4 Kategorien:

So souverän ist Ihre IT-Infrastruktur aufgestellt.

Richtungsweisend! Ihre Auswertung per Ampelsystem:

- 0–7 Punkte: Kritisches Risiko! Es besteht großes Potenzial. Hier ist am meisten zu gewinnen. Ein DTS-Beratungstermin lohnt sich jetzt unbedingt.
- 8–12 Punkte: Handlungsbedarf! Sie sind auf einem guten Weg. Einige Hebel fehlen noch. Eine DTS-Analyse bringt Sie schnell voran.
- 13–16 Punkte: Gut aufgestellt! Sie sind vorbildlich souverän. Sprechen Sie mit uns über Ihre letzten Lücken.



Offene Punkte? Wir haken sie gemeinsam ab!

DTS deckt alle 16 Punkte dieser Checkliste ab – alles aus einer Hand, „Made in Germany“, 100 % nach EU-Rechtsrahmen, vollumfänglich unabhängig.

Kontakt: dts.de | info@dts.de | 05221 1013000

BERATUNGSGESPRÄCH VEREINBAREN.