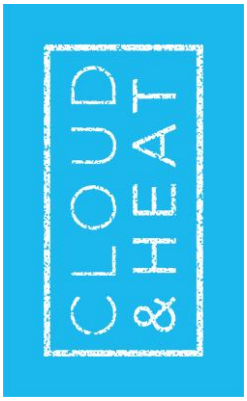

Digitale Souveränität unter der Lupe – Wie kann die Analyse einer IT-Infrastruktur aussehen?

Machen Sie den Selbstcheck – Wie souverän ist Ihre Infrastruktur (Auszug)?

Machen Sie den Souveränitäts-Selbstcheck anhand untenstehender Fragestellungen. Die Checkliste ist eine strukturierte, verständliche Möglichkeit, den Reifegrad digitaler Souveränität Ihrer Infrastruktur initial einzuschätzen. Sie hilft Organisationen, relevante Kriterien zu erkennen, versteckte Abhängigkeiten aufzudecken und oberflächliche Versprechen kritisch zu hinterfragen.

1. Technologische Unabhängigkeit

Einsatz von Open Source:

☐ Sind die Komponenten der IT-Infrastruktur quelloffen und unterliegen vereinbarten Standards der Open Source Community?

Stabilität der Open-Source-Community:

☐ Werden die eingesetzten Open Source Komponenten von einer stabilen und aktiven Community gepflegt und weiterentwickelt?

Vermeidung von Blackbox-Komponenten:

☐ Systeme, deren Funktionsweise und Abhängigkeiten nicht einsehbar sind, werden vermieden?

Migrationsmöglichkeit zu alternativen Komponenten:

☐ Gibt es kompatible Alternativen für wichtige Software, Hardware oder Services mit vergleichbarer Funktionalität?

Autonom steuerbare Build-Pipeline:

☐ Werden eigene CI/CD oder kontrollierbarer Build aus vertrauenswürdigen Quellen verwendet?

2. Unabhängigkeit von Anbietern

Vermeidung von Vendor Lock-ins:

☐ Sind proprietäre Technologien oder Datenformate im Einsatz, die einen Wechsel deutlich erschweren?

Offene Schnittstellen und APIs:

☐ Werden offene Schnittstellen und Austauschformate genutzt?

Absicherung kritischer Systeme:

☐ Werden unternehmenskritische Komponenten explizit betrachtet und sind notfalls eigenständig betrieb- und wartbar?

3. Support und Krisenmanagement

Qualität des Supports:

☐ Wird ein (deutschsprachiger) Support angeboten und ist die Reaktion lösungsorientiert und hilfreich?

Reaktion des Supports:

☐ Ist der Support gut erreichbar, reagiert zügig und ist flexibel?

Vorbereitung Krisenmanagement:

☐ Liegen dedizierte Notfallpläne und Kontaktmöglichkeiten für diverse Zwischenfälle wie z.B. Ausfall einzelner Komponenten vor?

Umsetzung Krisenmanagement:

☐ Kennen beteiligte Personen entsprechende Notfallpläne und können diese umsetzen?

4. Kompetenz und Wissen im Unternehmen

Verantwortungsvolle Nutzung der IT-Infrastruktur:

☐ Ist die IT-Infrastruktur und deren Prozesse inklusive der Sicherheitskonzepte nachvollziehbar aufgebaut, personenunabhängig dokumentiert und für alle umsetzbar?

Betrieb der IT-Infrastruktur:

☐ Verfügen Mitarbeiter oder Dienstleister über ausreichendes technologisches Wissen, um den Betrieb unabhängig sicherzustellen?

Stack-Kenntnis:

☐ Kennen beteiligte Personen gegebenenfalls den Plattform-Stack vollständig?

Exit-Strategie:

☐ Gibt es einen Maßnahmenplan inkl. Datenmigration und Dokumentation für Wechsel-/Austauschszenarien?

Strategie digitaler Souveränität:

☐ Gibt es eine umfassende Strategie für die Erhöhung der digitalen Souveränität, die bei allen technologischen und organisatorischen Entscheidungen einbezogen wird?

5. Vertragsbedingungen

Transparenz über Vertragsdetails und Änderungen:

☐ Sind Vertrags- und Lizenzbedingungen für die eingesetzten Komponenten transparent formuliert und werden Änderungen rechtzeitig kommuniziert?

Rechtssicherheit im Problemfall:

☐ Sind rechtliche Grauzonen ausgeschlossen, die im Falle eines Problems zu Schwierigkeiten führen könnten?

Controlling:

☐ Gibt es Monitoring für die Kostenentwicklungen und ein Aktionsszenario für Preissteigerungen von mehr als 20 % jährlich?

6. Rechtliche Aspekte

Jurisdiktion:

☐ Unterliegen die IT-Komponenten ausschließlich europäischem und deutschem Recht?

Zwang zur Offenlegung:

☐ Gibt es Drittstaatenregelungen, die Anbieter zu Offenlegung zwingen?

Ausstiegsvereinbarungen:

☐ Gibt es geregelte Ausstiegs- und Übergabevereinbarungen, die auch in der IT-Planung und im Notfallmanagement Beachtung finden?

7. Datenhoheit & Schutz

Standort der Daten:

☐ Werden die Daten ausschließlich in Deutschland oder der EU gespeichert?

Datenschutz:

☐ Werden personenbezogene Daten DSGVO-konform verarbeitet?

Zugriffskontrolle:

☐ Ist detailliert geregelt und dokumentiert, wer Zugriff hat, wozu dieser benötigt wird und ist diese Zugriffskontrolle digital unabhängig aufgebaut?

Datenverschlüsselung:

☐ Sind die Daten während der Speicherung und Übertragung mit einem eigenen Schlüssel (kein Drittanbieter Service) verschlüsselt?

Vermeidung Exfiltration:

☐ Ausschluss von Exfiltration durch Upstream-Dienste (z.B. Entzug von Lizenzen, die permanent über Online-Lizenzserver validiert werden müssen) möglich?

8. Backup und Archivierung

Regelmäßige Backups:

☐ Werden regelmäßige Backups der Daten erstellt?

Datensicherung:

☐ Werden Backups an einem sicheren Ort unter souveräner Zugriffskontrolle aufbewahrt?

Archivierung:

☐ Werden Daten, die nicht mehr aktiv genutzt werden, geschützt archiviert?

Löschung:

☐ Werden Daten, die nicht mehr benötigt werden, korrekt und nachvollziehbar gelöscht?

9. Monitoring

Systemüberwachung:

☐ Werden die Systeme regelmäßig auf Veränderungen überwacht?

Leistungsüberwachung:

☐ Wird die Leistung der Systeme konstant überwacht?

Sicherheitsüberwachung:

☐ Werden die Systeme auf Sicherheitslücken überwacht?

Souveränitäts-Check:

☐ Wird regelmäßig der Souveränitätsstatus überprüft?

10. Zertifizierung und Standardisierung

Standards:

☐ Werden Standards eingesetzt (u.a. BSI, ISO-Zertifizierung, NIS2, SCS)?

Zertifizierung:

☐ Ist die IT-Infrastruktur zertifiziert und wird sie regelmäßig aktualisiert?

Audits:

☐ Werden regelmäßige Audits sicherheitsrelevanter Komponenten und Prozesse durchgeführt?