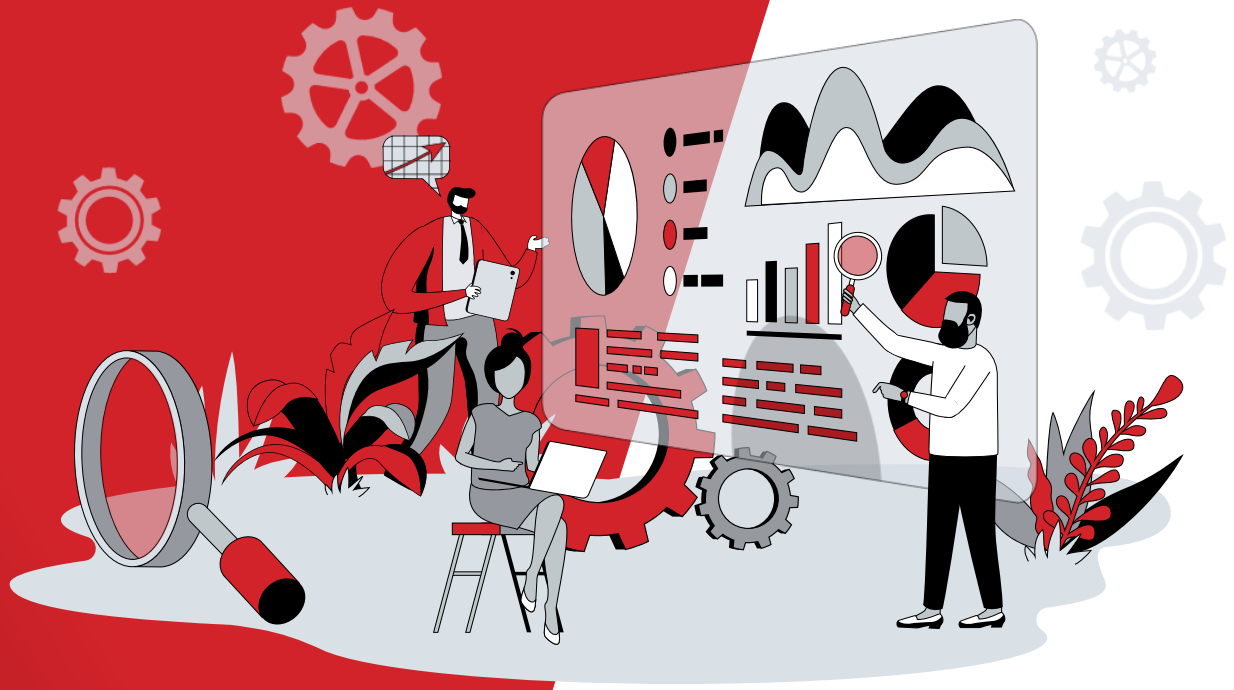
CYBERSECURITY & DIGITALE SOUVERÄNITÄT

FÜR MITTELSTAND UND MEDIEN



RIEDEL

Vertraulichkeitsstufe: Offen, Autor: Michael Martens, Version 1.0

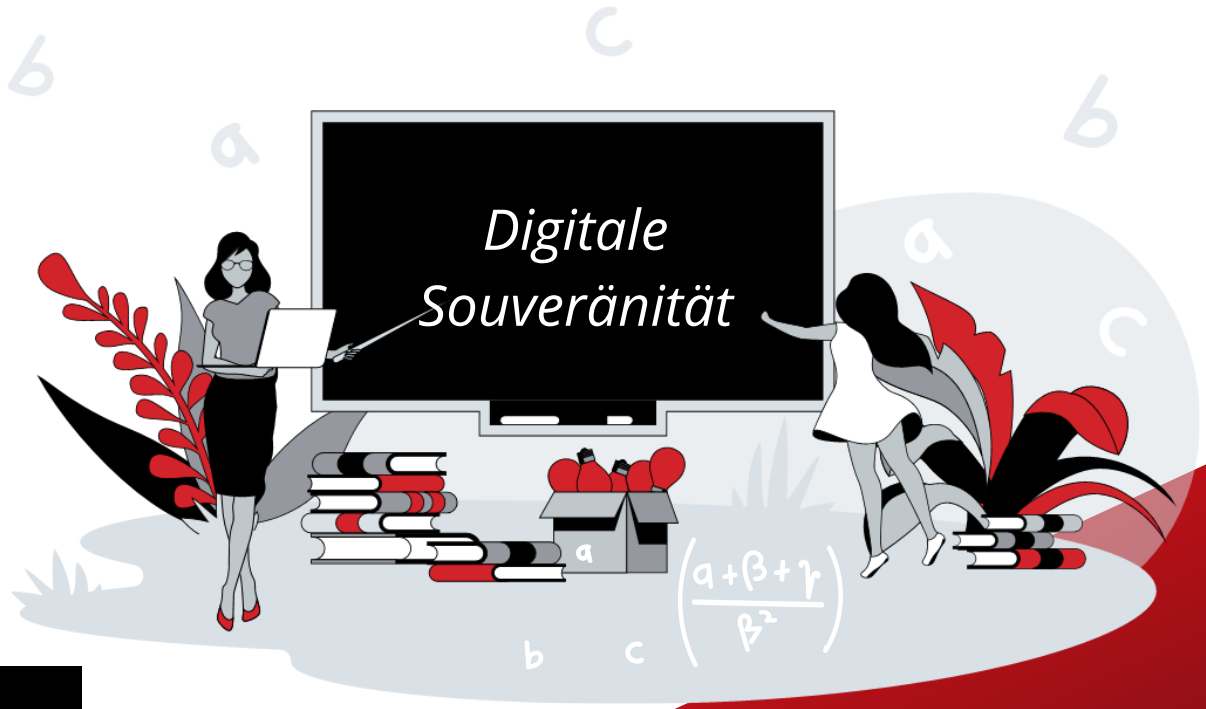
Digitale Souveränität

Wichtiger Baustein der Cybersecurity

Eigenständig über Daten, Systeme und digitale Prozesse verfügen:

technisch, rechtlich und organisatorisch

ohne kritische Abhängigkeiten.



Security Service Provider sollten Unternehmen bei der digitalen Souveränität unterstützen und deren Maßnahmen und Richtlinien unterstützen können.

RIEDEL

Cybersecurity Regel #1:

Verleugnung ist keine Strategie

Source: Michael Martens, CEO RIEDEL Networks

TELCO

MEDIA

established

Public Internet (IP)

moving to

establishing

IT Security

have to consider

relying on

Managed Services

relying on

RIEDEL


TELCO
MEDIA
established
moving to
establishing
have to consider
relying on
relying on
RIEDEL
Public Internet (IP)
IT Security
Managed Services
RIEDEL

Ebenen der Souveränität

Generelles Framework

Individuelle Souveränität

Hat die einzelne (Privat-) Person die / das…

- Kontrolle über die eigenen Daten (Datenschutz; Privatsphäre)
- Verständnis über digitale Tools („mündiger“ Nutzer)
- Fähigkeit zur Selbstbestimmung bei der Nutzung digitaler Angebote

Ebenen der Souveränität

Generelles Framework

Individuelle Souveränität

Hat die einzelne (Privat-) Person die / das…

- Kontrolle über die eigenen Daten (Datenschutz; Privatsphäre)
- Verständnis über digitale Tools („mündiger“ Nutzer)
- Fähigkeit zur Selbstbestimmung bei der Nutzung digitaler Angebote

Unternehmerische Souveränität

- Abhängigkeit (von nur einem Anbieter e.g. Hyperscaler)
- Zugriff auf Daten auch im Störfall oder Rechtsstreit?
- Ist ein Technologiewechsel möglich?
- Compliance (NIS-2, DORA…)

Ebenen der Souveränität

Unternehmerische Souveränität

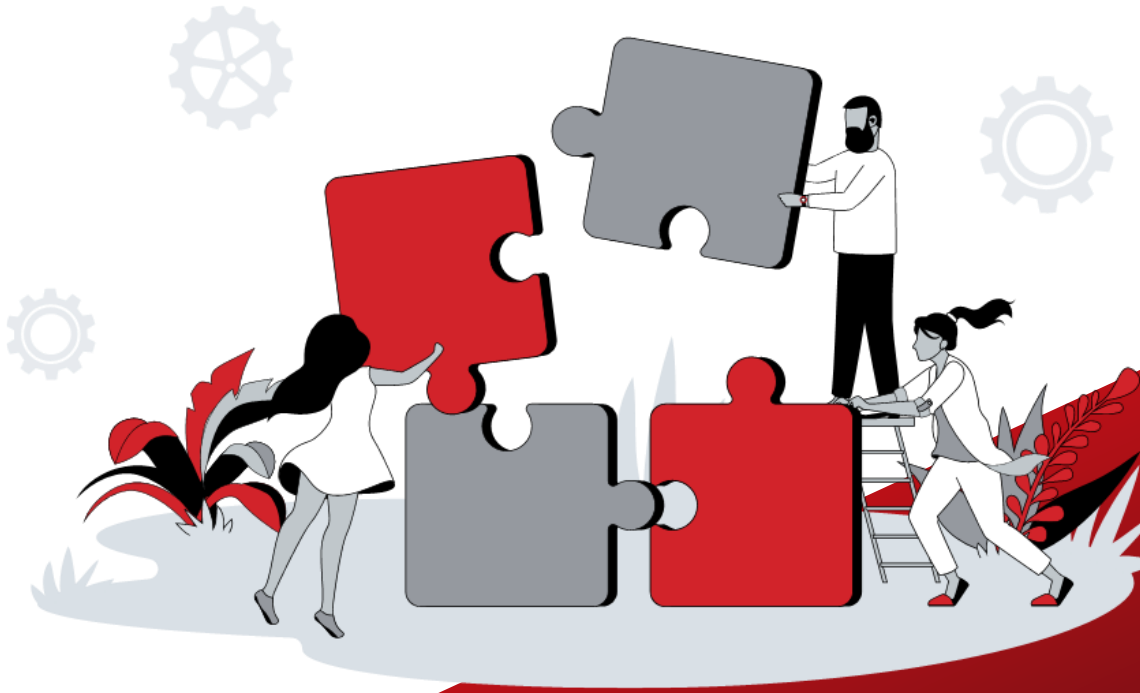
Folgende Bereiche sind hier für Unternehmen zu nennen:

Technologische Souveränität – Kontrolle über Infrastruktur, Software, Schnittstellen…

Datensouveränität – Zugriff, Speicherort- und zeit, Verschlüsselung…

Operationelle Souveränität – Business Continuity Pläne, Notfallpläne…

Rechtliche Souveränität – Verträge, Haftung, Audits…



Ebenen der Souveränität

Generelles Framework

Individuelle Souveränität

Hat die einzelne (Privat-) Person die / das…

- Kontrolle über die eigenen Daten (Datenschutz; Privatsphäre)
- Verständnis über digitale Tools („mündiger“ Nutzer)
- Fähigkeit zur Selbstbestimmung bei der Nutzung digitaler Angebote

Unternehmerische Souveränität

- Abhängigkeit (von nur einem Anbieter e.g. Hyperscaler)
- Zugriff auf Daten auch im Störfall oder Rechtsstreit?
- Ist ein Technologiewechsel möglich?
- Compliance (NIS-2, DORA…)

staatliche / geopolitische Souveränität

- Unabhängigkeit von anderen Staaten/Ländern/Monopolen
- Kontrolle über kritische Infrastruktur
- Schutz vor Druck (staatlich/wirtschaftlich)

Aktuelle Initiativen sind z.B. GAIA-X oder der Cyber Resilience Act der EU)

Missverständnis

Digitale Souveränität = Alles selbst hosten

Missverständnis

Open Source = Souverän

Missverständnis

Hyperscaler = nicht souverän

Missverständnis

Einhaltung der DSGVO = wir machen alles richtig

Souveräne Cloud-Nutzung

Was man im Blick behalten sollte

Kriterium	Souverän	Nicht Souverän
Datenzugriff	Kunde hat vollständige Kontrolle (z. B. eigene Schlüssel, Zero-Trust)	Anbieter kann technisch/juristisch auf Daten zugreifen
Verschlüsselung	Kundenseitige Verschlüsselung mit eigenem Key-Management (KMS)	Provider verwaltet Schlüssel, Kunde nur „Nutzer“
Rechtlicher Geltungsbereich	Daten & Betrieb unter EU-/DSGVO-Recht, kein extraterritorialer Zugriff	Risiko durch z. B. US Cloud Act, FISA, NDAA etc.
Exit-Strategie	Vertraglich geregelter, zeitlich definierter, technisch machbarer Exit	Kein realistischer Exit, proprietäre APIs, keine Datenportabilität
Auditierbarkeit	Audit-Rechte, Logs, Supply-Chain-Transparenz, Zertifikate → nachweisfähig	„Black Box“-Cloud: keine Prüf- oder Kontrollrechte
Vendor-Lock-In-Risiko	Nutzung offener Standards / Multi-Cloud-fähigkeit	Starke Abhängigkeit von einem Anbieter / proprietären Services
Betriebsfähigkeit im Ernstfall	Notfall- & Wiederanlaufkonzept unabhängig vom Anbieter	„Wenn Cloud down → Betrieb steht“
Compliance (z. B. NIS-2 / DORA)	Vollständig evidenzfähig: Verträge, Prozesse, Risikoanalyse vorhanden	Pflichten werden auf Cloud-Provider „abgeschoben“
Vertragliche Klarheit	SLA mit Haftung, Audit, Datenlokalität, Exit, Security-Pflichten	Standard AGB, „best effort“, Haftung exkludiert
Lieferketten-Transparenz	Offenlegung von Subprozessoren & Hosting-Standorten	Keine Kontrolle über Subanbieter / Untervergaben
Betriebsmodell	Kunde entscheidet: Cloud only / Hybrid / Sovereign Tenant / On-Prem-Fallback	Anbieter entscheidet → Kunde konsumiert
Governance-Modell	Rollen, Verantwortlichkeiten, Dokumentation, Security-Ownership definiert	„Wir hosten in der Cloud, also ist es sicher“

RIEDEL

Gesundheitscheck

Einmal husten bitte …

RIEDEL

Überwachung

Lach- und Schießgesellschaft oder Wach- und Schließgesellschaft

Datensouveränität

- MDR speichert zwischen 10-20 Tage auf schnellem Speicher und bildet kein Archiv
- SIEM speichert zwischen 30-90 Tage auf schnellem Speicher und archiviert
- On-prem, Cloud oder Hybrid?

RIEDEL

Die optimale Wahl

Hausarzt oder Facharzt

- **Generalist oder Spezialist?**
- **Angriff oder Verteidigung?**
- **Diagnose oder Forensik?**
- **DIY oder Managed Service?**

RIEDEL

Beispiele

Der RIEDEL Networks OOPS-Report

Der „hätte ich das mal früher gewusst“-Report

Aus Vorfällen Anderer lernen!

>400 Cases voller Wissen zu:

- Schadensfeldern
- Verteidigungsansätzen
- Sicherheitslücken

u.v.m.

RIEDEL

Beispiele

Hacking-Tools aus dem Internet – Plug&Play

OMG Cable

Bash Bunny

Rubber Ducky

Shark Jack

... u.v.m.

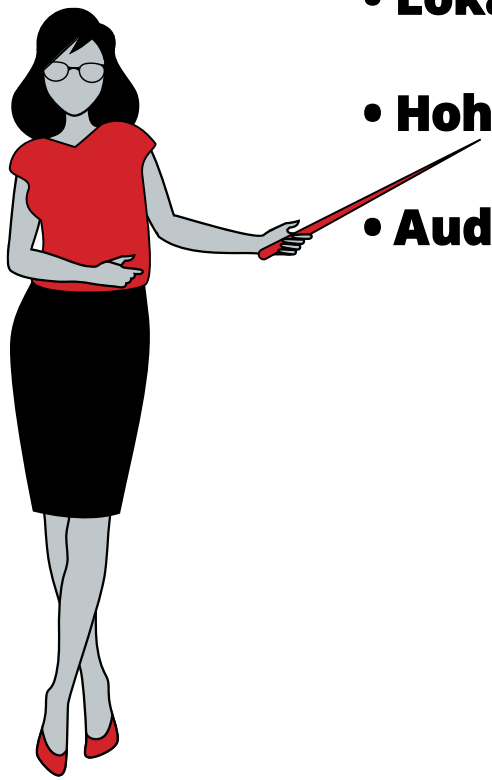
RIEDEL

Beispiele

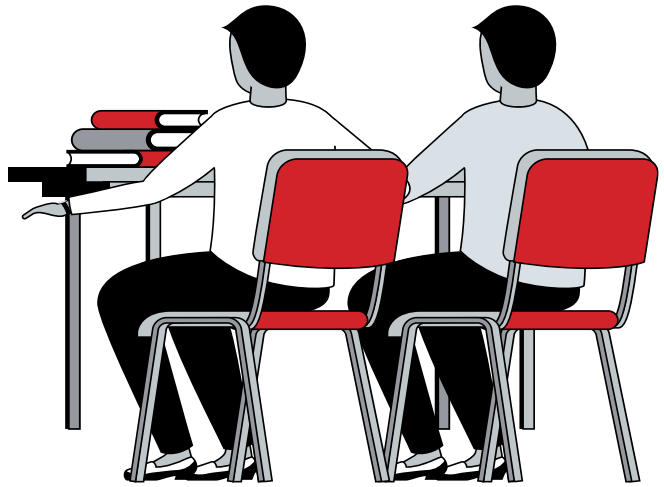
Home Office Arbeitszeitbetrug als Use-Case

RIEDEL

Zusammenfassung



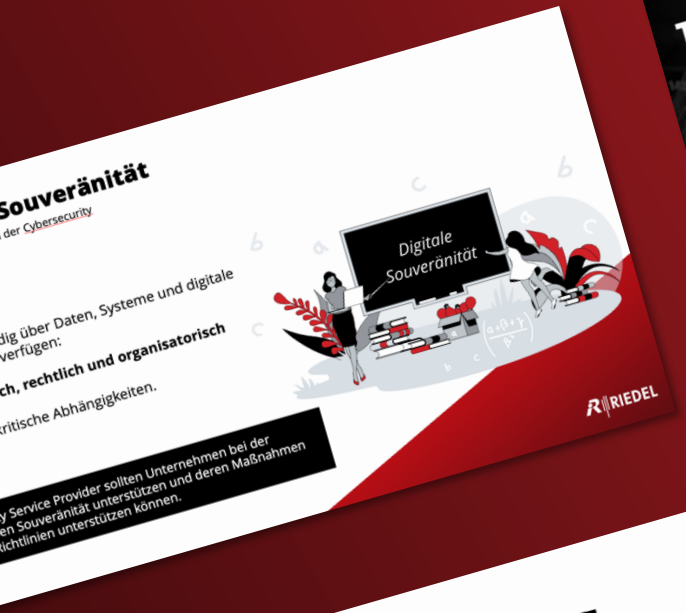
- **Digitale Souveränität, außereuropäischen Anbietern nicht vertrauen**
- **Lokaler Support, egal zu welcher Zeit (24x7)**
- **Hohe Skalierbarkeit und fixe Kostenbasis**
- **Auditierbarkeit und Berichterstattung**

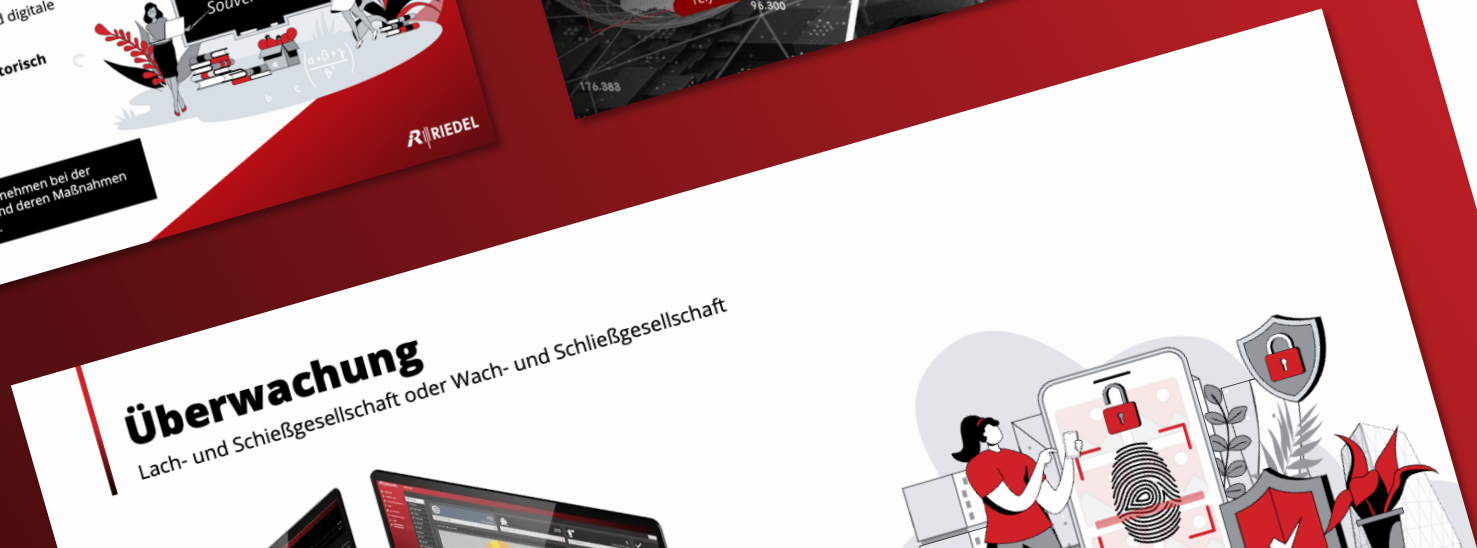


RIEDEL

RIEDEL

Thank You!





Get in Touch

Any questions? We are looking forward to answer them!

Michael Martens, CEO RIEDEL Networks

Michael.Martens@riedel.net

+49 174 9890089

Failure is no option. RIEDEL Networks

RIEDEL


2025-02-28 06:47:34
NDR
1 Direkt-Annahme 2
auer