Digitale Souveränität als Wachstumsbeschleuniger

KWCON 2026

09.11.2026

Andreas Stemick





Andreas Stemick

Wegbereiter für Digitale Souveränität in Europa

> „Der Engpass ist selten die Technologie.
> Es ist die Fähigkeit, Optionen zu schaffen und Risiken aktiv zu steuern."

Managing Partner

BDO DIGITAL & BDO Cyber Security

Equity Partner

AG Wirtschaftsprüfungsgesellschaft

Advisory Leadership

Mitglied im Advisory Leadership Team der BDO AG WPG

Digital Sovereignty Program

Wegbereiter des DSP für Europa

© BDO

Die Reise in 5 Schritten

Agenda

01

Die Cloud-Realität

Mainstream trifft auf Konzentration

02

Das Kill-Switch-Risiko

Ø 11–12 Monate Überlebensdauer

03

KI verändert die Regeln

Automatisierte Exploits als neue Dimension

04

Souveränität — wie?

Drei Handlungsebenen, ein Ziel

05

Der Weg nach vorn

BDO & kwsoft® als Anker

© BDO

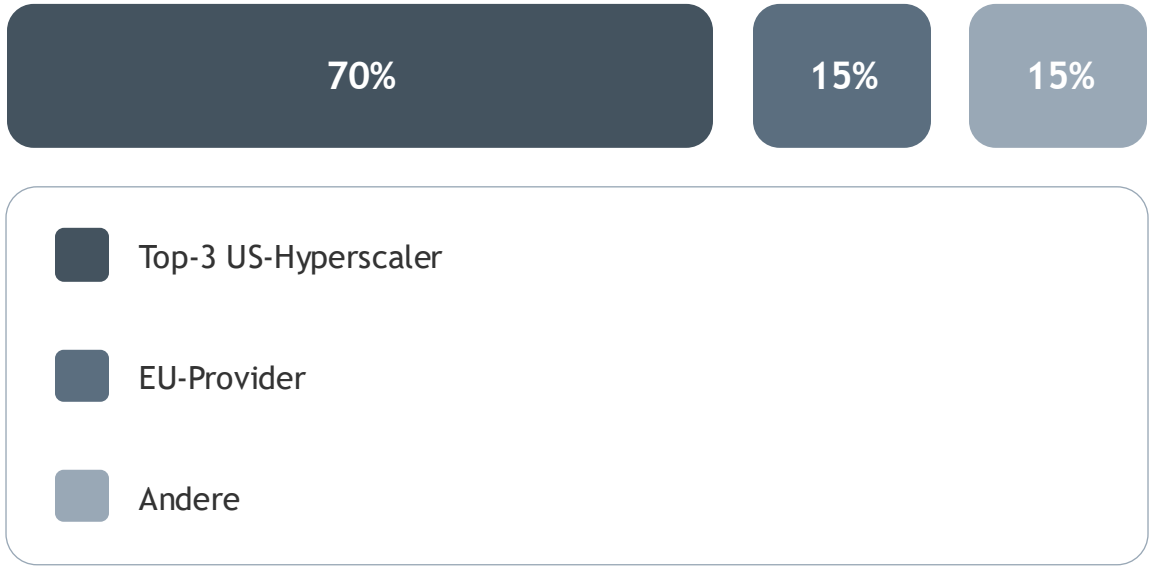
Cloud ist Mainstream — und Abhängigkeit

Die Cloud-Realität

52,74%

der EU-Unternehmen nutzen bezahlte Cloud-Services
+7,42 % -Punkte gegenüber 2023
84,67 % bei Großunternehmen

Marktanteil Cloud-Infrastruktur in Europa (2024)



61 Mrd. € Cloud-Markt —
Wertschöpfung fließt ab.

Quellen: Eurostat, ICT-Erhebung 2025 · Synergy Research Group (Marktanteile 2024)

© BDO

Ein Jahr, bis die Lichter ausgehen

Das „Kill Switch“-Risiko

Wie lange kann Ihr Unternehmen überleben, wenn digitale Leistungen nicht mehr aus dem Ausland bezogen werden können?

Ausland (gesamt)

57 %

Überleben max. 12 Monate

USA

Ø 12

Monate Überlebensdauer

China

Ø 11

Monate Überlebensdauer

Nur 4 % der Unternehmen kämen dauerhaft ohne ausländische Digitalimporte aus.

Quelle: Bitkom Research, Nov. 2025 (605 Unternehmen ab 20 Beschäftigten) · Basis: Unternehmen, die digitale Technologien importieren

© BDO

Fünf Fakten zur Dringlichkeit

Cloud-Souveränität · Handlungsbedarf

Das Bewusstsein wächst — die Handlungsfähigkeit noch nicht. Fünf Fakten, die den Handlungsbedarf in Deutschland & Europa auf den Punkt bringen.



Marktkonzentration

Top-3 US-Anbieter halten rund 70 % Marktanteil in Europa.



KRITIS & Verwaltung

Für Behörden und kritische Infrastrukturen hoch, wenn nicht in europäischer Cloud.



Regulatorischer Konflikt

US Cloud Act vs. DSGVO/GDPR — strukturell unvereinbar.



EU-Initiativen

GAIA-X und Verwaltungscloud sind gestartet — Wirkung bislang begrenzt.



Strategisches Risiko

US-Abhängigkeit wirkt als „Kill Switch“ mit geopolitischer Hebelwirkung.



Europas Zeitfenster schließt sich.

Jetzt strukturieren — nicht reagieren.

© BDO

Souveränität ist, wenn

der Exit aus dem Kill Switch ein kontrollierter Prozess ist.

Kein panischer Not-Aus — ein kontrollierter, geprüfter, auditierbarer Exit.

Was passt zu Ihrem Umfeld?

© BDO

Zwischenbefund

Das Bewusstsein wächst — die Handlungsfähigkeit noch nicht.

Europas Zeitfenster schließt sich. Jetzt strukturieren — nicht reagieren.

Andreas Stemick · BDO

© BDO

Wenn KI selbst Exploits schreibt

Die neue Dimension

Claude Mythos Preview (April 2026) fand autonom über 10.000 kritische Lücken im ersten Monat. Seit Juni ist die Mythos-Klasse als „Fable“ öffentlich verfügbar – mit Sperren für Cyber-Anfragen.

Bisher		Jetzt	
1990er	Automatisches Suchen bekannter Schwachstellen	**2026**	KI findet unbekannte Lücken UND entwickelt Exploits autonom
2000er	Automatisches Suchen unbekannter Schwachstellen	**Skalierbar**	>10.000 Schwachstellen in einem Monat — industriell
Manuell	Ausnutzen und Exploit-Entwicklung durch Menschen	**0-Day by KI**	Politische & technische Kontrolle werden existenziell

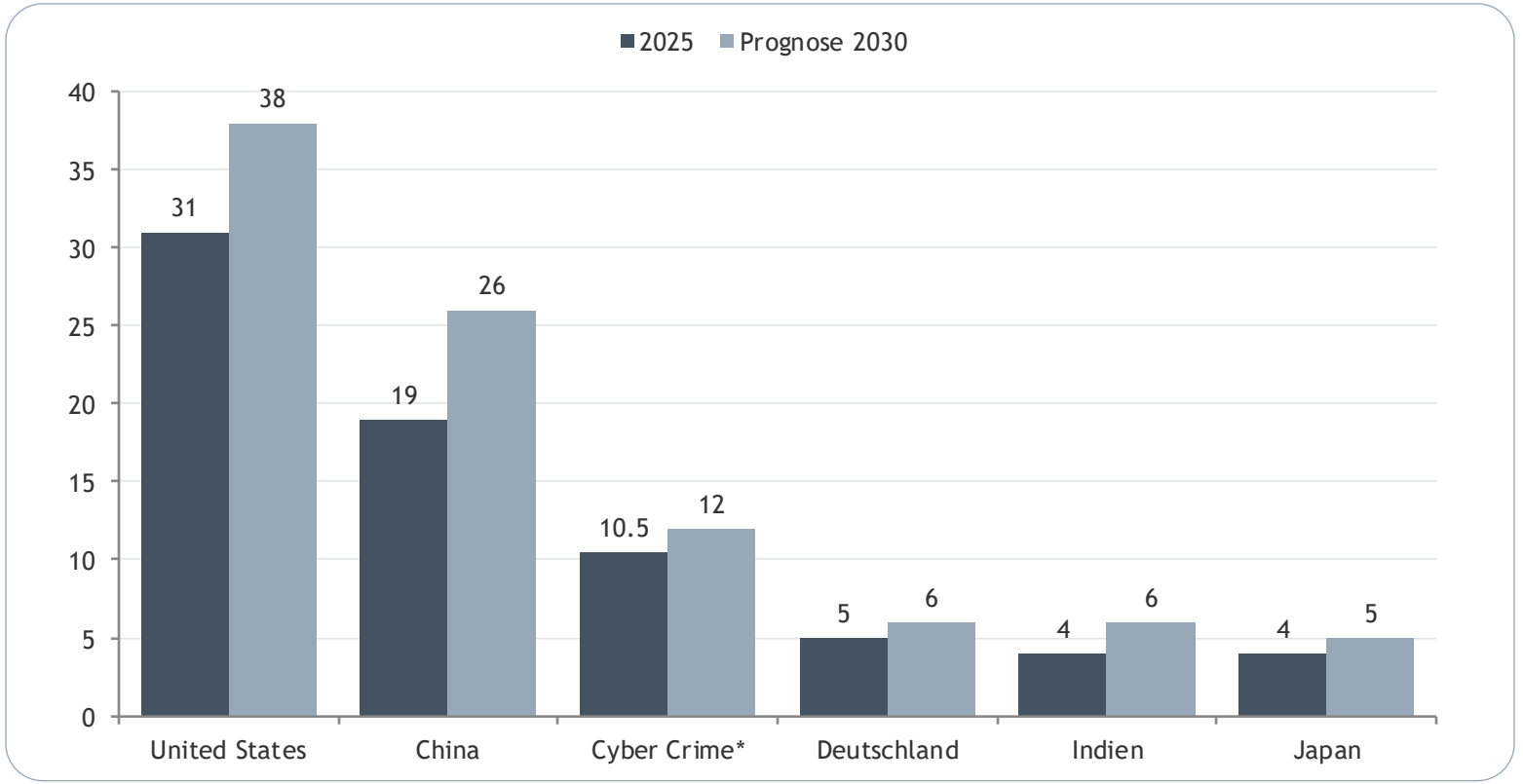
Strategische Ableitung: nicht mehr in Services denken — sondern in Funktionalitäten.

© BDO

Cyber Crime als dritte „Volkswirtschaft“

Die Ökonomie des Risikos

Weltweit geschätzte Kosten von Cyber Crime im Verhältnis zum nominalen BIP der wichtigsten Wirtschaftsnationen (in Billionen US-$).



Cyber Crime

12

Billionen US-$ bis 2031

Schon 2025 rund 10,5 Bio. US-$ — mehr als dreimal so viel wie 2015 (3 Bio. US-$).

Quellen: IWF World Economic Outlook (April 2026); Cybersecurity Ventures, Cybersecurity Almanac (Dez. 2025). *Cyber Crime: Prognose für 2031.

© BDO

Wenn Geräte zur Angriffsfläche werden

Aktuelle Fälle · Oktober 2026

Zwei Vorfälle aus derselben Woche: Angreifer übernehmen vernetzte Anlagen im Betrieb – oder manipulieren Geräte, bevor sie beim Kunden ankommen.

Vernetzte Anlagen · Frankreich

50 °C

In Kühltruhen hunderter Supermärkte

Hacker manipulieren über Nacht vernetzte Kühlsteuerungen (Danfoss) bei Intermarché, Coopérative U, Carrefour u. a.: Abtaumodus erzwungen, Solltemperatur auf 50 °C.

Folge: Ware verdorben, Millionenschaden. Laut Hersteller liefen die Anlagen mit veralteter Firmware.

Lieferkette · Hardware-Wallets

93 Mio.

US-$ aus über 300 Wallets entwendet

Manipulierte Ledger Nano X im Handel in Asien und Europa: Ein Zusatz-chip liest die Seed Phrase vom Display, LTE-Modem und eSIM funken sie an die Täter.

Nicht ab Werk: Die Geräte wurden in der Lieferkette abgefangen und umgebaut.

Wer Firmware und Lieferkette nicht kontrolliert, kontrolliert seine Geräte nicht.

Quellen: Reuters, AFP, Franceinfo via ORF und Berliner Zeitung (13.10.2026) · heise online, Tom's Hardware, Tibane Labs (Okt. 2026)

© BDO

Drei Ebenen. Ein Ziel.

Wie Souveränität entsteht

Vollständige Souveränität ist unrealistisch. Risikoproportionale Souveränität ist das Ziel — auf drei Handlungsebenen.

01 **Technisch**
Infrastruktur & Architektur

- Open-Source-Stack: SCS, OpenStack, Kubernetes
- EU-eigenes Key Management — kein US-KMS
- Confidential Computing / TEEs für sensible Workloads

02 **Organisatorisch**
Infrastruktur & Architektur

- Exit-Strategie, Monitoring, Audit-Rechte
- Datenklassifizierung nach Souveränitätsbedarf
- IR-Fähigkeit ohne US-Anbieter-Abhängigkeit

03 **Industriepolitisch**
Rahmen & Ökosystem

- Staat als Anker-Kunde für EU-Anbieter
- EU Chips Act, Glasfaser, Fachkräfte
- EUCS mit echten Souveränitätsanforderungen

Souveränität = Wahlmöglichkeiten + Nachweisbarkeit. Nicht Ideologie — Architektur.

© BDO

Zusammenspiel: KI, Cyber Security und ISVs

Souveränität als Produktmerkmal

Souveränität als zwingendes Produktmerkmal — drei aufeinander aufbauende Ebenen, die ISVs neue Marktchancen öffnen.



Chancen für ISVs

Marktvorteil

„Sovereignty-Ready“ öffnet Türen zu regulierten Branchen.

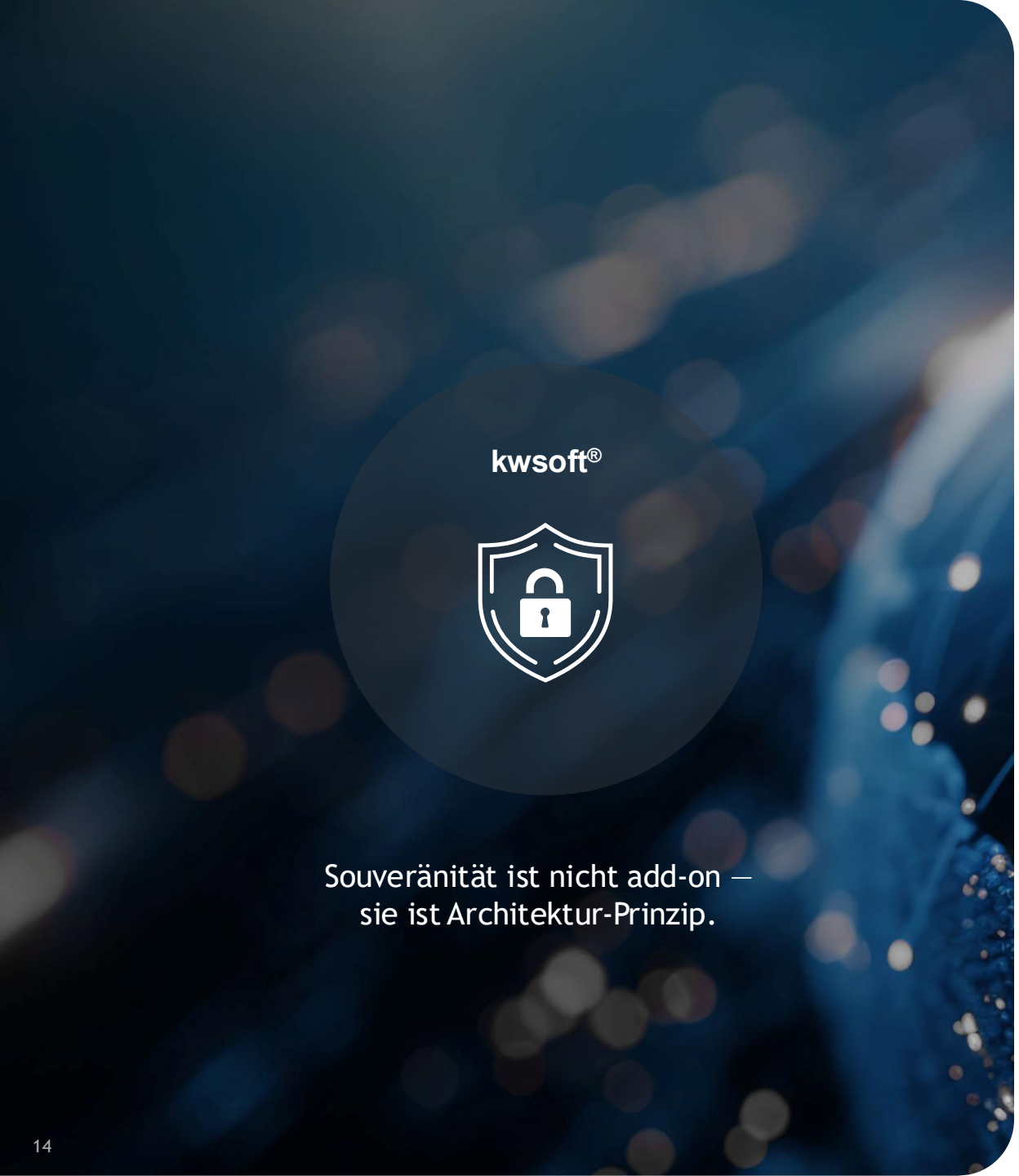
Effizienz

XaaS ermöglicht schnelle, skalierbare Implementierungen.

Vertrauen

Audit-Evidenz und Portabilität sichern die Kundenbindung.

© BDO



Souveränität ist nicht add-on –
sie ist Architektur-Prinzip.

kwsoft® – souverän per Design

Positionierung

Unabhängig

100 % eigentümergeführt – kein Investorendruck, kein Übernahmerisiko.

Made in Europe

Vollständig in Deutschland und Tschechien entwickelt

AnyPrem und nahtlos migrierbar

Daten bleiben in der von Ihnen gewählten Infrastruktur – DSGVO, DORA, Bankgeheimnis.

ISO 27001, EcoVadis, ISO 9001, ISAE 3402

Organisationen der kwsoft® Group erfüllen alle relevanten Zertifizierungen

Souveräne KI-Verarbeitung

Sämtliche KI-Funktionen mit lokalen oder privat gehosteten Modellen nutzbar

© BDO

BDO + kwsoft® — messbar souverän

Die Partnerschaft

Sichere Enterprise Content Cloud Services — vom zertifizierten Betrieb bis zum objektiven Reifegrad.



Sovereignty Maturity Level
zertifiziert durch BDO & StackIT

Transparent
Objektiver Nachweis des Souveränitätsgrads

Regulatorisch
DSGVO · NIS-2 · DORA — belastbar dokumentiert

Investitionsarm
Weniger Hürden — besonders Public Sector & KRITIS

Schnell
Beschleunigte Entscheidungen dank klarer Nachweise

© BDO

Fünf Sätze zum Mitnehmen

Key takeaways

01

Cloud ist Standard

Die Cloud-Entschei-dung ist gefallen. Der Differen-ziator ist Governance.

02

Souveränität = Wahl + Nachweis

Unternehmen brauchen echte Optionen — und müssen sie auditieren können.

03

KI macht Security zur Pflicht

Automatisierte Exploits verändern das Risiko-Profil fundamental.

04

Stack + Betriebs-modell

Europäischer Hyperscaler + kwsoft® + BDO = skalierbar und auditfähig.

05

Kontrollierter Exit aus dem Kill Switch

Nicht panischer Not-Aus — sondern kontrollierter, auditierbarer Exit.

© BDO



BDO AG Wirtschaftsprüfungsgesellschaft, eine Aktiengesellschaft deutschen Rechts, ist Mitglied von BDO International Limited, einer britischen Gesellschaft mit beschränkter Nachschusspflicht, und gehört zum internationalen BDO Netzwerk voneinander unabhängiger Mitgliedsfirmen.
BDO ist der Markenname für das BDO Netzwerk und für jede der BDO Mitgliedsfirmen. © BDO