

# CYBER SECURITY REPORT 2026

# VORWORT

## SOUVERÄNITÄT ALS SCHUTZSCHILD – EUROPAS DIGITALE HANDLUNGSFÄHIGKEIT UNTER DRUCK

Die Bedrohungslage im Cyberraum ist nicht abstrakt. Jeden Tag werden wir Zeuge von kriminellen und staatlichen Cyberangriffen. Der Cyberraum ist ein Schlachtfeld, auf dem permanent, unkontrolliert, ohne Bandagen gekämpft wird. Die Angreifer sind dabei den Verteidigern immer ein Stück voraus. Sie zielen auf die operative Substanz unseres Wirtschaftsstandortes und die Stabilität unserer staatlichen Ordnung ab. Immer schnellere Zyklen digitaler Innovation überfordern die bürokratischen Prozesse in vielen Ländern und Organisationen der Welt.

Der vorliegende Report verdeutlicht: Die Intensität und Professionalität der Angreifer nimmt durch künstliche Intelligenz und arbeitsteilige Geschäftsmodelle weiterhin zu, während die Einstiegsbarrieren in die Szene sinken. Privatwirtschaft und öffentliche Hand hingegen agieren überwiegend reaktiv. Mit einem geschätzten wirtschaftlichen Schaden von über 202 Milliarden Euro allein in Deutschland ist Cybersicherheit längst keine IT-Aufgabe mehr, sondern eine Existenzfrage für jeden Geschäftsführer und jede Institution. Man stelle sich vor, der Schaden sei von physischer Natur.

Wir befinden uns in einer Phase, in der digitale Souveränität zur strategischen Notwendigkeit wird. Wer sich in einseitige Abhängigkeiten von außereuropäischen Plattformen begibt, verliert die Kontrolle über seine eigene Handlungsfähigkeit. Digitale Souveränität bedeutet heute die Fähigkeit zur Selbstbestimmung im gesamten digitalen Raum – von geschäftskritischen Daten bis hin zu KI-Modellen.



Dieser Bericht bietet Ihnen weit mehr als eine Bestandsaufnahme der Risiken. Er liefert:

- Repräsentative Deutschlandumfrage: Eine Analyse zu Themen der Cybersicherheit und digitalen Souveränität.
- Analysen kritischer Gefährdungsbereiche: Ein tiefer Einblick in die Risiken und Potentiale der Robotik und den oft unterschätzten „digitalen Nachlass“.
- Operationalisierung digitaler Souveränität: Die erste umfassende Operationalisierung des EU Cloud Sovereignty Frameworks für das europäische Software-Ökosystem mit Einblicken in die Bewertung und Steuerung von Software- und KI-Souveränität.
- Strategische Entscheidungsgrundlagen: Warum „Exit-by-Design“ und europäische Infrastrukturen die Basis für künftige Wettbewerbsfähigkeit sind.

Wir laden Sie ein, die folgenden Seiten als Weckruf und Fahrplan zu nutzen. Es geht darum, die digitale Transformation nicht nur zu vollziehen, sondern sie sicher und souverän zu gestalten.

Wir danken allen beteiligten Experten und den über 1.000 befragten kleinen und großen Unternehmen für ihre wertvollen Beiträge zu dieser wegweisenden Analyse.

**Rolf Schumann**  
Co-CEO Schwarz Digits

**Christian Müller**  
Co-CEO Schwarz Digits

# EXECUTIVE SUMMARY

Der vorliegende Bericht liefert eine umfassende Lageanalyse, welche die strukturelle Verfestigung globaler Bedrohungslagen, die wachsende Konvergenz physischer und digitaler Risiken in der Robotik sowie die kritische Diskrepanz zwischen wahrgenommener Resilienz und operativer Realität in deutschen Unternehmen untersucht. Ein Augenmerk liegt auch auf der erstmaligen Operationalisierung des EU Cloud Sovereignty Frameworks für Software – ein entscheidender Schritt, um digitale Souveränität messbar und anwendbar zu machen. Der grundlegende Anspruch des Reports ist es, nicht-technischen und technisch versierten Entscheidern einen kompakten Überblick über aktuelle, weltweite Bedrohungen oder weniger beachtete Themen in der Cybersicherheit und angrenzenden Bereichen zu geben.

## Geopolitische Risiken und die neue Normalität der Cyberbedrohung

Für die komparative Analyse wurden weltweite Veröffentlichungen zur Cybersicherheit, die zwischen Sommer 2025 und Februar 2026 veröffentlicht wurden, herangezogen. Die Lage 2025/26 ist durch eine strukturelle Verfestigung und die Überlagerung bestehender Bedrohungen geprägt. Cyberangriffe wirken parallel zu geopolitischen Entwicklungen und gefährden staatliche Stabilität, globale Lieferketten sowie öffentliche Ordnung. Durch das synergetische Agieren staatlicher Akteure, Krimineller und ideologischer Gruppen gehen Spionage, Sabotage und Ausbeutung immer stärker ineinander über. Während in Europa Hacktivismus und KRITIS-Spionage dominieren, unterstreichen die Sabotage von Unterseekabeln und die Eskalation gegen Taiwan – mit täglich 2,63 Millionen Angriffen – die globale Dimension. Die Cloud-Konvergenz fokussiert hierbei systemische Risiken, Ransomware agiert weiterhin als industrialisiertes, schadensintensives Ökosystem. In Deutschland verursachen Cyberangriffe mittlerweile 70 Prozent der Wirtschaftsschäden (202,4 Mrd. Euro). Besonders kritisch wirken Wiederherstellungszeiten von bis zu 30 Tagen sowie ein psychologischer Druck auf Entscheidungsprozesse, der die operative Handlungsfähigkeit unmittelbar unterminiert.

## Die Cybersicherheitsrealität der deutschen Wirtschaft

Unsere repräsentative Erhebung unter 1.001 deutschen Unternehmen offenbart eine tiefe Diskrepanz zwischen wahrgenommener Vorbereitung und struktureller Resilienz. Während 65 Prozent der Unternehmen ihre Abwehrbereitschaft positiv bewerten, belegt die Realität eine Opferquote von 20 Prozent (Großunternehmen: 33 Prozent). Cybersicherheitsbudgets stiegen zwar auf 17 Prozent des IT-Budgets, bleiben jedoch reaktiv und regulatorisch (NIS-2) getrieben. Steuerungsdefizite zeigen sich im Fehlen von CISOs (57 Prozent) sowie dem Verzicht auf ganzheitliche Risikoanalysen (40 Prozent). Diese Defizite betreffen auch die KI-Governance: Trotz erkannter Risiken durch KI-basiertes Social Engineering haben nur 25 Prozent verbindliche Richtlinien implementiert. Ein kritisches Sicherheitsrisiko bleibt die Lieferkette: 75 Prozent der Unternehmen verzichten auf Audits bei ihren Lieferanten, obwohl bereits jedes zweite Unternehmen Angriffe bei Zulieferern registriert. Schließlich unterstreicht die hohe Zustimmung zu offensiven Cybermaßnahmen den Wunsch nach Handlungsfähigkeit: 79 Prozent befürworten staatliche Hackbacks, 59 Prozent fordern diese Befugnisse sogar für private Akteure. Zur digitalen Souveränität besteht eine signifikante Umsetzungslücke: 87 Prozent investieren nicht in die Reduktion technologischer Abhängigkeiten, ungeachtet einer höheren Zahlungsbereitschaft für souveräne Lösungen von 42 Prozent.

## Robotik und die Konvergenz physischer und digitaler Sicherheitsrisiken

Die rasant fortschreitende Integration humanoider und autonomer Systeme in industrielle Fertigungsprozesse, staatliche Sicherheitsorgane und militärische Strukturen markiert einen Konvergenzpunkt, an dem die Trennung zwischen physischer und digitaler Funktionalität faktisch aufgehoben wird. Moderne robotische Plattformen sind hochgradig vernetzte Systeme, die mechanische Mobilität mit sensorgestützter Datenverarbeitung und Künstlicher Intelligenz kombinieren, wodurch jede technische Schwachstelle unmittelbare kinetische und

operative Konsequenzen nach sich ziehen kann. Werden solche Systeme in sicherheitskritischen Umgebungen wie der Grenzsicherung oder in bewaffneten Konflikten eingesetzt, hängt ihre Verlässlichkeit vollständig von der Integrität der digitalen Infrastruktur ab. Die Erfahrungen aus aktuellen Konflikten, insbesondere in der Ukraine, demonstrieren, wie durch agile, oft zivilgesellschaftlich gestützte Innovationsprozesse robotische Systeme in kürzester Zeit angepasst werden können, was klassische, bürokratische Beschaffungszyklen westlicher Staaten herausfordert. Diese Entwicklung erzwingt eine Neubewertung der staatlichen Handlungsfähigkeit im Cyberraum, da die Beherrschung dieser Technologien nicht nur eine Frage der mechanischen Überlegenheit, sondern primär eine der digitalen Souveränität und der Absicherung komplexer Lieferketten für Hardware und Software ist.

#### **Digitale Souveränität als strategische Notwendigkeit und operative Steuerungsgröße**

Digitale Souveränität hat sich durch die veränderte geopolitische Lage von einer politischen Zielvorstellung zu einer strategischen Notwendigkeit entwickelt, die nationale Sicherheit, globalen Wettbewerb und organisationale Resilienz untrennbar verknüpft. Das im Oktober 2025 veröffentlichte Cloud Sovereignty Framework (CSF) der EU bietet einen strukturierten Ansatz für die Verwendung in öffentlichen Ausschreibungen. Das EU CSF hat noch Schwächen und es deckt auch keine Software sowie ihre Bereitstellungsmodelle im Detail ab. Für die vorgenommene Analyse von 27 Softwareprodukten in typischen Enterprise Software Kategorien, wurde ein Software Sovereignty Framework (SSF) auf Basis des CSF entwickelt. Während von europäischen Unternehmen angebotene Open-Source-Lösungen das Ranking anführen, erreichen außer-europäische proprietäre Plattformen regelmäßig niedrige Werte (Scores). Besonders bei Künstlicher Intelligenz stellen Souveränitätskriterien derzeit mehr Anspruch als Wirklichkeit dar. Die Ergebnisse zeigen, dass digitale Souveränität 2026 kein statisches Zertifikat ist, sondern durch gezielte technische und organisatorische Maßnahmen aktiv gesteuert werden muss. Darüber hinaus sind souveräne Cloud Infrastrukturen entscheidend für souveräne Software Angebote.

#### **Der digitale Fußabdruck nach dem Tod als systemisches Risiko**

Ein oft unterschätzter Aspekt der Cybersicherheit liegt in der exponentiell wachsenden Fragmentierung digitaler Identitäten, die weit über die bewusste Nutzung einzelner Dienste hinausgeht. Während Individuen ihren digitalen Fußabdruck oft auf wenige Dienste schätzen, verwaltet ein durchschnittlicher Nutzer hunderte digitale Konten und hat tausende digitale Spuren (z. B. Kommentare in sozialen Netzwerken, Online- und Mobilverhalten, Einkäufe, Lokationsdaten von Apps). Auch nach dem Ableben bildet die Summe des digitalen Nachlass eine Angriffsfläche, die weiterlebt. Identitätsdiebstahl und unbefugte Zugriffe erfolgen zunehmend durch die Ausnutzung weiterhin gültiger Zugänge, selbst verstorbener oder inaktiver Nutzer, da Systeme auf legitime Anmeldedaten reagieren, ohne dass klassische Warnmechanismen greifen. Die Verwaltung dieser Datenmengen durch große Plattformen berührt ethische und emotionale Fragen der Hinterbliebenen und stellt auch eine Gefahr für Unternehmen und Behörden dar. Der professionelle Umgang mit dem digitalen Nachlass und die Reduktion des digitalen Fußabdrucks ist daher genau so wichtig wie die Erstellung eines Testaments, Erbvertrags, einer Patientenverfügung oder Vermögensübertragungen.



# INHALT

|                                                                 |          |                                                                                           |           |
|-----------------------------------------------------------------|----------|-------------------------------------------------------------------------------------------|-----------|
| <b>VORWORT</b>                                                  | <b>1</b> | <b>2 WIRTSCHAFTSBAROMETER DEUTSCHLAND –<br/>CYBERSICHERHEIT UND DIGITALE SOUVERÄNITÄT</b> | <b>39</b> |
| <b>EXECUTIVE SUMMARY</b>                                        | <b>3</b> | 2.1 STUDIENDESIGN                                                                         | 44        |
| <b>1 AUF EINEN BLICK –<br/>CYBERSICHERHEIT IN 2025 UND 2026</b> | <b>9</b> | 2.2 BEDROHUNGSWAHRNEHMUNG                                                                 | 44        |
| 1.1 GLOBALE LAGE DER CYBERSICHERHEIT                            | 13       | 2.3 IT-SECURITY-BUDGETS                                                                   | 46        |
| 1.1.1 GEOPOLITISCHE SPANNUNGEN UND IHRE AUSWIRKUNGEN            | 13       | 2.4 PERSONELLE IT-STRUKTUR UND COMPLIANCE-ROLLEN                                          | 48        |
| 1.1.2 TECHNOLOGISCHE ENTWICKLUNGEN UND GLOBALE TRENDS           | 15       | 2.5 RISIKOMANAGEMENT UND OPERATIVE PRÄVENTION                                             | 50        |
| 1.1.3 RANSOMWARE – SYSTEMATISCHE BEDROHUNG                      | 16       | 2.6 RISIKOFAKTOR LIEFERKETTE                                                              | 51        |
| 1.1.4 WIRTSCHAFTLICHER SCHADEN UND KOSTEN VON CYBERANGRIFFEN    | 18       | 2.7 NIS-2-REGULATORIK UND VERANTWORTLICHKEIT                                              | 52        |
| 1.2 NATIONALE BEDROHUNGSLAGE: DEUTSCHLAND IM FOKUS              | 20       | 2.8 DIGITALE SOUVERÄNITÄT UND LIEFERKETTEN-RESILIENZ                                      | 53        |
| 1.2.1 ANGRIFFSMUSTER UND ZIELE                                  | 20       | 2.8.1 STRATEGISCHE UND PERSONELLE VERANKERUNG                                             | 54        |
| 1.2.2 DIGITALE IDENTITÄTEN UND ZUGANGSINFRASTRUKTUREN           | 21       | 2.8.2 ZAHLUNGSBEREITSCHAFT UND SOUVERÄNITÄTS-PREMIUM                                      | 55        |
| 1.3 STRUKTURIERTE ANGREIFER – AKTEURE, ZIELE UND MITTEL         | 23       | 2.8.3 STRATEGIEN FÜR DEN UMGANG MIT ABHÄNGIGKEITEN                                        | 57        |
| 1.3.1 STAATLICHE AKTEURE                                        | 24       | 2.8.4 WAHRNEHMUNG EUROPÄISCHER INITIATIVEN                                                | 57        |
| 1.3.2 ORGANISIERTE CYBERKRIMINALITÄT                            | 26       | 2.9 POLITISCHE MASSNAHMEN                                                                 | 58        |
| 1.4. BESONDERS GEFÄHRDETE SEKTOREN UND STRUKTUREN               | 27       | 2.9.1 POLITISCHE MASSNAHMEN FÜR DIGITALE SOUVERÄNITÄT<br>UND CYBERSICHERHEIT              | 58        |
| 1.4.1 KRITISCHE INFRASTRUKTUREN                                 | 28       | 2.9.2 VERTRAUENSDEFIZIT BEI CYBERRESILIENZ<br>UND STAATLICHER AUFSTELLUNG                 | 59        |
| 1.4.2 MITTELSTAND UND DIGITALISIERUNGSDRUCK                     | 30       | 2.10 FAZIT                                                                                | 60        |
| 1.4.3 LIEFERKETTEN UND IT-DIENSTLEISTER ALS ZIEL                | 30       | <b>3 ROBOTIK IM KONFLIKT –<br/>VOM HELFER ZUM TERMINATOR</b>                              | <b>63</b> |
| 1.5. VERTEIDIGUNGS-HERAUSFORDERUNGEN UND STRUKTURELLE LÜCKEN    | 32       | 3.1 ROBOTIK IN KONFLIKTEN                                                                 | 68        |
| 1.5.1 TECHNISCHE ANGRIFFSOBERFLÄCHEN UND SCHWACHSTELLEN         | 32       | 3.2 TERMINATOR – STAND DER TECHNIK UND MÖGLICHKEITEN                                      | 70        |
| 1.5.2 DIGITALE IDENTITÄTEN – EIN UNTERSCHÄTZTES RISIKO          | 34       | 3.2.1 DAS GEHIRN                                                                          | 70        |
| 1.5.3 KI ALS STRUKTURELLER BESCHLEUNIGER                        | 34       | 3.2.2 DIE ENERGIEVERSORGUNG                                                               | 72        |
| 1.6 GOVERNANCE, REGULIERUNG UND MANAGEMENT-VERANTWORTUNG        | 35       | 3.2.3 DIE EXTREMITÄTEN                                                                    | 74        |
| 1.7 AUSBLICK 2026-2035                                          | 36       | 3.2.4 MIT ALLEN SINNEN – DIE SENSORIK                                                     | 76        |
|                                                                 |          | 3.2.5 DIE EFFEKTOREN                                                                      | 79        |
|                                                                 |          | 3.2.6 MASSENPRODUKTION UND AUTONOME WEITERENTWICKLUNG                                     | 80        |
|                                                                 |          | 3.2.7 EINE FRAGE DER KOSTEN?                                                              | 81        |
|                                                                 |          | 3.3 FAZIT                                                                                 | 82        |

|          |                                                                                          |            |
|----------|------------------------------------------------------------------------------------------|------------|
| <b>4</b> | <b>SOVEREIGN THINGS –<br/>SOFTWARESOVERÄNITÄT IN EUROPA</b>                              | <b>85</b>  |
| 4.1      | HINTERGRUND ZUM DISKURS ZUR DIGITALEN SOVERÄNITÄT IN EUROPA                              | 89         |
| 4.2      | OPERATIONALISIERUNG UND MESSBARKEIT VON DIGITALER SOVERÄNITÄT                            | 92         |
| 4.2.1    | DIE BESTEHENDE FRAMEWORK-LANDSCHAFT                                                      | 92         |
| 4.2.2    | DAS EU CLOUD SOVEREIGNTY FRAMEWORK ALS NEUER REFERENZRAHMEN                              | 93         |
| 4.3      | ANPASSUNG DES EU CSF ZUR MESSUNG VON SOFTWARE-SOVERÄNITÄT                                | 94         |
| 4.4      | ERLÄUTERUNG DES SOFTWARE-SOVERÄNITÄTS-FRAMEWORK (SSF)                                    | 96         |
| 4.5      | ERGEBNISSE: WIE SOVERÄN IST DAS SOFTWARE-PORTFOLIO<br>EUROPÄISCHER ORGANISATIONEN HEUTE? | 99         |
| 4.6      | EINORDNUNG DER ERGEBNISSE                                                                | 105        |
| 4.6.1    | OPEN SOURCE ALS SOVERÄNE ALTERNATIVE?                                                    | 105        |
| 4.6.2    | WIE SOVERÄN KANN EIN KI-SYSTEM SEIN?                                                     | 106        |
| 4.6.3    | LIMITATIONEN DES ANSATZES                                                                | 107        |
| 4.7      | AUSBLICK: JENSEITS TECHNISCHER METRIKEN                                                  | 108        |
| 4.7.1    | WAS KÖNNEN WIR AUS DER ÜBERTRAGUNG DES CSF<br>AUF SOFTWARE LERNEN?                       | 108        |
| 4.7.2    | DER BEITRAG VON ÖFFENTLICHER BESCHAFFUNG<br>ZUR DIGITALEN SOVERÄNITÄT DER EU             | 109        |
| 4.7.3    | BEDEUTET „MADE IN EUROPE“ AUTOMATISCH „SOVERÄN“?                                         | 110        |
| <b>5</b> | <b>DIGITAL AFTERLIFE –<br/>ÜBER DEN DIGITALEN NACHLASS</b>                               | <b>113</b> |
| 5.1      | DIGITALE EXISTENZ UND DAS SCHUTZVAKUUM NACH DEM TOD                                      | 118        |
| 5.2      | UNSER DIGITALER FUSS-ABDRUCK UND DIE ILLUSION DER KONTROLLE                              | 120        |
| 5.3      | RISIKEN UND GEFAHREN                                                                     | 121        |
| 5.4      | RECHTLICHE UND TECHNISCHE HERAUSFORDERUNGEN                                              | 123        |
| 5.5      | GANZHEITLICHE LÖSUNGSSTRATEGIEN UND<br>HANDLUNGSBEDARF FÜR DIE ZUKUNFT                   | 125        |
|          | <b>ANHANG</b>                                                                            | <b>129</b> |
|          | AKTUELLER STATUS DER NIS-2-REGULIERUNG                                                   | 131        |
|          | ÜBER DIE SCHWARZ GRUPPE UND SCHWARZ DIGITS                                               | 135        |
|          | DEFINITIONEN UND ABKÜRZUNGSVERZEICHNIS                                                   | 137        |
|          | LITERATURVERZEICHNIS                                                                     | 141        |

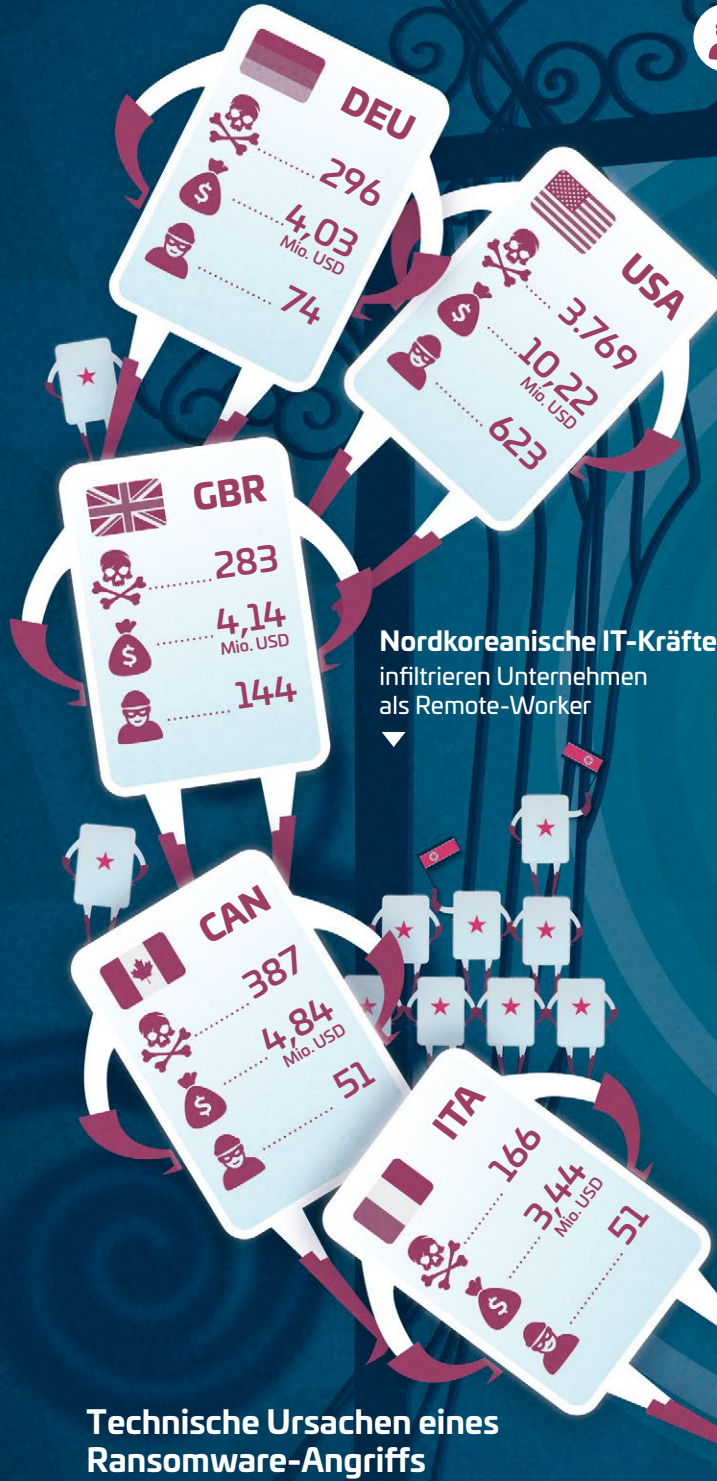
# KAPITEL 1



# AUF EINEN BLICK CYBERSICHERHEIT IN 2025 UND 2026

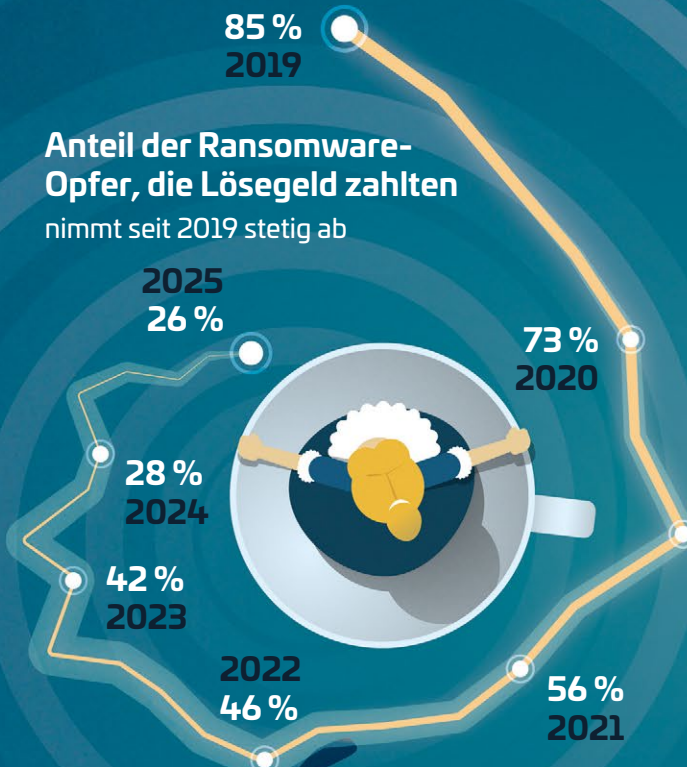
**Zahlen & Fakten  
zu betroffenen Ländern**  
(2025, Auszug aus Top 10 der Betroffenen)

-  Ransomware-Opfer
-  Durchschnittskosten je Datenleck
-  beobachtete Aktivitäten staatlicher Akteure



**Nordkoreanische IT-Kräfte**  
infiltrieren Unternehmen  
als Remote-Worker

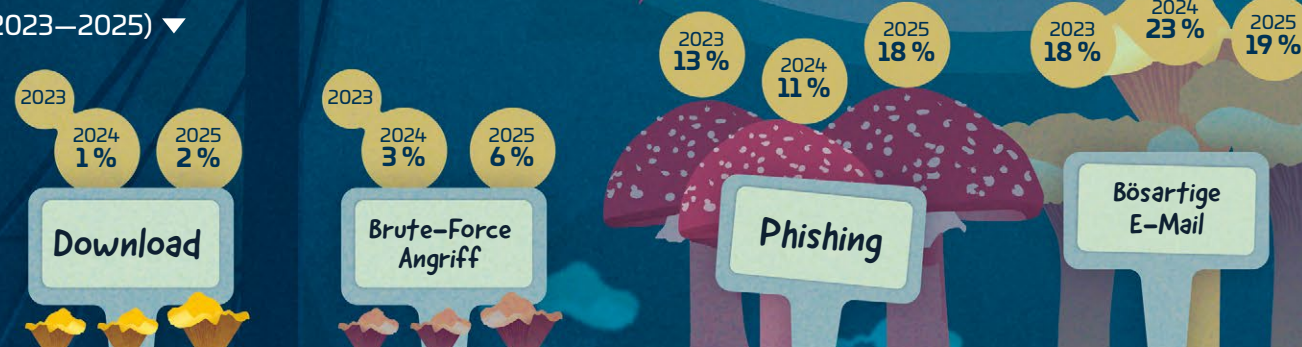
**Anteil der Ransomware-Opfer, die Lösegeld zahlen**  
nimmt seit 2019 stetig ab



**Top 5 Investitionsziele**  
(weltweit aus 20 Ländern)

- Technologie **70 %**
- Planung & Vorbereitung **68 %**
- Personal **67 %**
- Schulungen **66 %**
- Versicherungen **65 %**

**Technische Ursachen eines Ransomware-Angriffs**  
(2023–2025)



**Prompt-Leakage-Angriffe bei führenden LLM-Modellen und Service-Providern**  
(Erfolgsraten in %)



**Weltweit gelten Cyberangriffe als das operative Risiko Nr. 1**

Sie rangieren jedoch in strategischer Priorisierung hinter geopolitischen und sozialen Krisen auf **Rang 5**

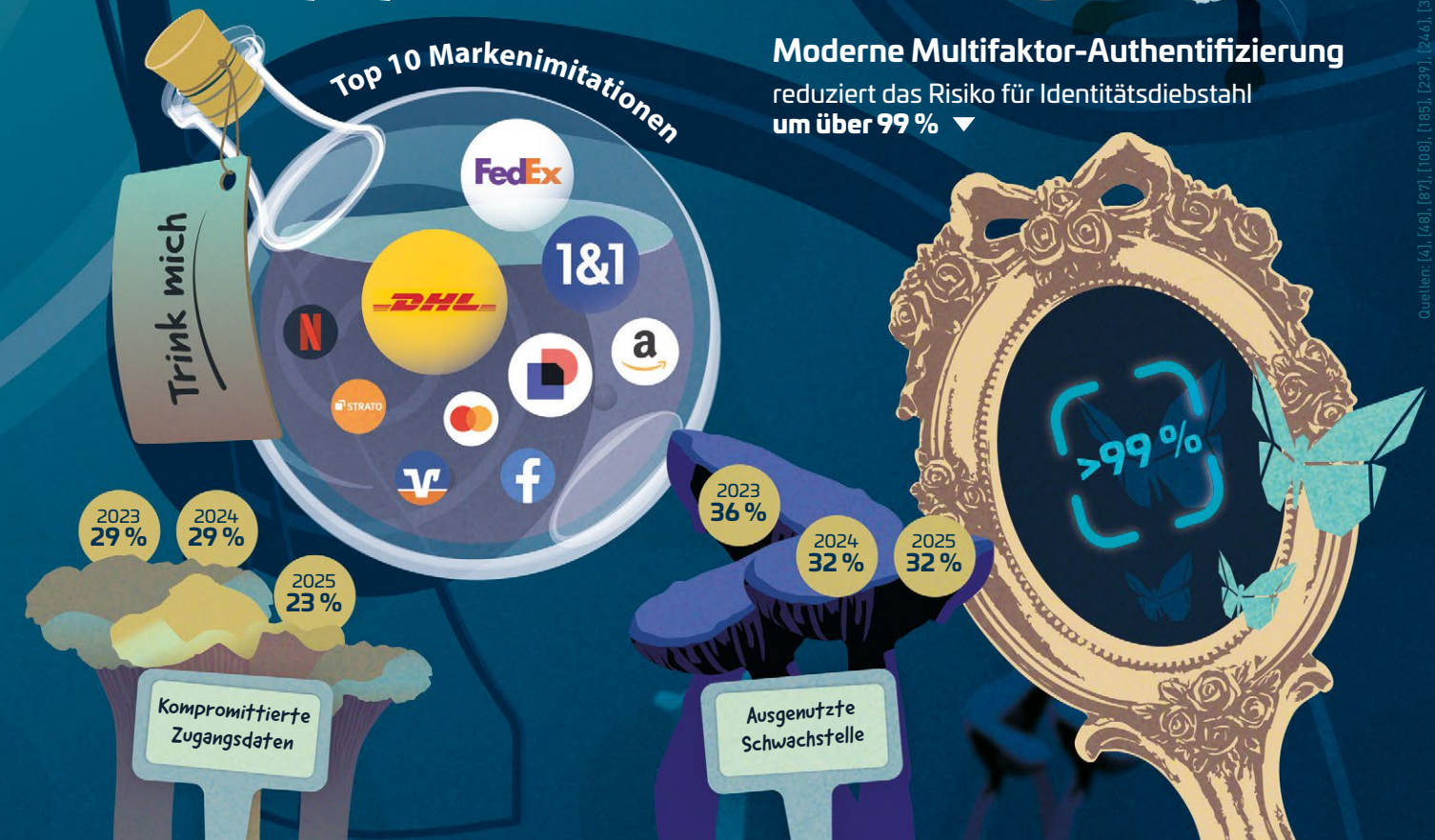
**Ursachen von Datenpannen**  
(Anteile aller betroffenen Organisationen)

**51 %**  
Böswilliger oder krimineller Angriff

**23 %**  
Technische Fehler/  
Schwachstellen

**26 %**  
Menschliches Versagen

**Moderne Multifaktor-Authentifizierung**  
reduziert das Risiko für Identitätsdiebstahl  
um **über 99 %**





# 1 AUF EINEN BLICK – CYBERSICHERHEIT IN 2025 UND 2026

## 1.1 GLOBALE LAGE DER CYBERSICHERHEIT

Die weltweite Cybersicherheitslage ist eng mit geopolitischen Spannungen verknüpft. Sie wird durch das Zusammenwirken von Cyberkriminalität, politischen Konflikten und technologischem Wandel geprägt [27], [138], [283]. Staatliche Akteure, cyberkriminelle Netzwerke und ideologisch motivierte Gruppen agieren parallel. Sie nutzen häufig dieselben Infrastrukturen und Schwachstellen, verfolgen jedoch unterschiedliche Zwecke: Spionage, Sabotage sowie Erpressung und Betrug [85], [138]. Ausmaß und Schwerpunkt dieser Aktivitäten variieren je nach regionalem, politischen und technologischen Kontext. Der Cyberraum nimmt damit eine doppelte Rolle ein: als Angriffsfeld und als Instrument sicherheitspolitischer Positionierung.

Die wirtschaftlichen Folgen reichen von organisationsbezogenen Schäden bis zu gesamtwirtschaftlichen Effekten in hochdigitalisierten Volkswirtschaften [346]. Cyberangriffe sind zunehmend Bestandteil hybrider Konflikte [339]. Betroffen sind insbesondere die staatliche Stabilität und die öffentliche Ordnung [61], [72], [110], [131], [138], [139], [181], [345].

### 1.1.1 Geopolitische Spannungen und ihre Auswirkungen

Geopolitische Spannungen fungieren zunehmend als strukturierender Faktor digitaler Angriffe. Sie beeinflussen Intensität, Zielrichtung und Ausgestaltung der Angriffe. Staaten, staatlich unterstützte Akteure und ideologisch motivierte Gruppen nutzen Cyberoperationen gezielt als Instrument politischer Einflussnahme und Abschreckung. Der Fokus liegt dabei weniger auf kurzfristigen Systemstörungen als auf dem Aufbau von Informationsvorteilen, der Beeinflussung kritischer Prozesse und der Erzeugung gesellschaftlicher Unsicherheit [110], [138], [246], [345].

Aufgrund von global vernetzter Kommunikations-, Cloud- und Dienstleistungsstrukturen bleiben solche Operationen selten auf nationale Grenzen beschränkt.

Cyberoperationen wirken damit parallel zu diplomatischen, wirtschaftlichen und militärischen Entwicklungen und verstärken bestehende Konflikt dynamiken [110], [138].

Die folgenden regionalen Betrachtungen zeigen, wie sich diese geopolitisch geprägte Bedrohungslage in unterschiedlichen Weltregionen ausprägt. Akteurskonstellationen, Zielsysteme und Angriffsmuster unterscheiden sich dabei, abhängig von regionalen Machtverhältnissen, wirtschaftlichen Abhängigkeiten und sicherheitspolitischen Prioritäten.

### Europa

In Europa ist die Bedrohungslage durch einen hohen Anteil hacktivistischer Aktivitäten mit symbolischer und medialer Zielsetzung gekennzeichnet. Für den Zeitraum Juli 2024 bis Juni 2025 wurden 4.875 sicherheitsrelevante Vorfälle erfasst, differenziert nach cyberkriminellen, staatlichen und hacktivistischen Akteuren [110]. Phishing stellt mit 60 Prozent den häufigsten Angriffsvektor dar, gefolgt von der Ausnutzung von Schwachstellen (21,3 Prozent) und Botnet-Aktivitäten (9,9 Prozent) [110]. Rund 79 Prozent der registrierten Vorfälle werden hacktivistischen Akteuren zugeschrieben. Diese Aktivitäten äußern sich überwiegend in DDoS-Angriffen (Überlastungsangriffe auf IT-Dienste) oder digitalen Störaktionen. Die technische Komplexität ist dabei meist gering, die politische und öffentliche Wirkung jedoch hoch [33], [110], [128]. Im Telekommunikationsumfeld wurden erstmals DDoS-Angriffe mit Spitzenlasten von bis zu zehn Terabit pro Sekunde beobachtet. Etwa 78 Prozent der Angriffswellen dauerten kürzer als fünf Minuten [259].

Staatlich ausgerichtete Aktivitäten konzentrieren sich demgegenüber überwiegend auf nachrichtendienstlich motivierte Spionage. Betroffen sind insbesondere Sektoren wie Telekommunikation, Transport, industrielle Produktion und öffentliche Verwaltung. In diesem Zusammenhang werden unter anderem Akteure mit Bezug zu Russland, China und Nordkorea genannt [110], [128], [130].



Regionale Krisen in Europa entfalten aufgrund global vernetzter digitaler Infrastrukturen rasch internationale Auswirkungen. Im internationalen Vergleich ist die Region stärker von politisch motivierten und öffentlichkeitswirksamen Angriffen geprägt als andere Weltregionen [110], [330]. Besonders betroffen sind Deutschland und Belgien als Hauptziele staatsnaher Akteure sowie Frankreich, Italien und Polen, die die meisten hacktivistisch motivierten Vorfälle verzeichnen [110]. Diese Dynamik wird durch die strukturelle Abhängigkeit Europas von US-Anbietern im Bereich der Cybersicherheits-Technologien und Bedrohungsanalysen verschärft, was die strategische Souveränität bei der Abwehr kritischer Bedrohungen einschränkt [271].

### Naher und Mittlerer Osten

Im Nahen und Mittleren Osten ist die Cyberbedrohungslage eng mit regionalen Machtkonflikten und hybriden Bedrohungsszenarien verknüpft. Cyberoperationen werden überwiegend als Bestandteil staatlicher Sicherheits- und Einflussstrategien eingesetzt. Sie begleiten politische, militärische und wirtschaftliche Spannungen innerhalb der Region [165], [201], [267].

Staatliche und staatsnahe Akteure nutzen digitale Angriffe gezielt zur Spionage, Einflussnahme und Destabilisierung staatlicher sowie wirtschaftlicher Strukturen. Diese staatliche Instrumentalisierung zeigt sich insbesondere in wiederkehrenden, politisch motivierten Cyberkampagnen im Kontext regionaler Rivalitäten.

Iran-nahen Akteursgruppen wird dabei die gezielte Ausspähung staatlicher Stellen sowie die Veröffentlichung sensibler Daten zugeschrieben. Cyberoperationen entfalten dadurch unmittelbare politische Wirkung und werden gezielt zur strategischen Einflussnahme gegen Israel eingesetzt [165], [267].

Länder wie die Vereinigten Arabischen Emirate und Katar werden sowohl als Ziel politisch motivierter Angriffe auf Regierungs- und Infrastrukturnetze als auch als sicherheitspolitische Akteure und regionale Kooperationsknotenpunkte beschrieben [165], [201].

Neben staatlichen Cyberoperationen ist die Region auch von cyberkriminellen Aktivitäten betroffen [165]. In Staaten wie Ägypten wird Cybersicherheit zunehmend als sicherheitspolitische Aufgabe verstanden und mit verstärkten staatlichen Schutzmaßnahmen für Regierungsnetze und kritische Infrastrukturen verknüpft [90], [165], [295].

### Nordamerika

In Nordamerika ist die Cyberbedrohungslage stark durch die wirtschaftliche und technologische Bedeutung der Region geprägt. Die USA und Kanada zählen aufgrund ihrer hohen digitalen Durchdringung, der Konzentration datenintensiver Industrien und der zentralen Rolle globaler Cloud- und Plattformanbieter zu den weltweit attraktivsten Zielräumen für Cyberangriffe [138], [139].

Im Unterschied zu stärker symbolisch geprägten Angriffsmustern in Europa steht der Zugriff auf hochwertige Datenbestände, geistiges Eigentum und geschäftskritische Infrastrukturen im Vordergrund. Entsprechend dominieren wirtschaftlich motivierte Angriffe, die auf unbefugten Zugriff, Identitätsmissbrauch und die gezielte Kompromittierung digitaler Umgebungen abzielen. Sie münden häufig in großvolumigen Datenabflüssen [139].

Neben cyberkriminellen Aktivitäten ist auch eine erhöhte Präsenz staatlicher und staatsnaher Akteure festzustellen. Nordamerika wird als strategischer Zielraum für langfristige Spionage und Informationsgewinnung betrachtet. In diesem Zusammenhang werden unter anderem Akteure mit Bezug zu China, Russland, Iran und Nordkorea genannt [246].

Betroffen sind insbesondere daten- und wissensintensive Sektoren wie Finanz- und Versicherungswesen, Gesundheits- und Sozialdienste sowie professionelle Dienstleistungen [138], [139], [185]. Aus staatlicher Perspektive gelten digitale Infrastrukturen, Datenökosysteme und cloudbasierte Plattformen zugleich als Grundlage nationaler Wettbewerbsfähigkeit und als sicherheitspolitisch schützenswerte Schlüsselressource [330].

### Asien-Pazifik

Im asiatisch-pazifischen Raum ist die Cyberbedrohungslage durch eine enge Verflechtung wirtschaftlicher Interessen, technologischer Abhängigkeiten und geopolitischer Machtkonkurrenz geprägt. Cyberaktivitäten dienen sowohl staatlicher Einflussnahme als auch wirtschaftlicher Instrumentalisierung. Dabei überwiegen gezielte, langfristig angelegte Operationen [233], [246], [342].

Im Zentrum steht der Aufbau dauerhafter Zugriffs- und Einflussmöglichkeiten. Angreifer erlangen über die Ausnutzung bekannter Schwachstellen oder den Miss-

brauch bestehender Zugangsdaten initialen Zugriff auf IT-Systeme. Diese Zugänge werden gezielt zur Etablierung persistenter Präsenz (dauerhafte, verdeckte Systemverankerung) genutzt [233], [342].

Diese Ausrichtung zeigt sich besonders deutlich im staatlichen Kontext. Chinesische Akteure starteten 2025 durchschnittlich 2,63 Millionen Cyber-Intrusionsversuche pro Tag gegen Taiwans kritische Infrastruktur. Dies entspricht einem Anstieg von etwa 6 Prozent gegenüber dem Vorjahr [254]. Betroffen waren insbesondere Energie-, Kommunikations-, Transport-, Notfall- und Verwaltungssysteme. Über die Hälfte der Angriffe entfiel auf die Ausnutzung von Hard- und Software-Schwachstellen. Besonders auffällig war der mehr als zehnfache Anstieg der Angriffe auf Energieinfrastrukturen sowie deutliche Zuwächse im Gesundheits- und Rettungswesen [254].

Neben organisierter Cyberkriminalität treten staatlich zugeordnete Akteure in der Region deutlich in Erscheinung. Gruppen mit Bezug zu China, Russland, Iran und Nordkorea greifen gezielt Telekommunikationsnetze, Forschungseinrichtungen sowie staatliche und IT-nahe Organisationen an, um langfristigen Zugriff auf sensible Informationen, technologische Entwicklungen und strategische Infrastrukturen zu erlangen [67], [232], [234], [236], [237], [246].

Die Bedrohungslage wird zusätzlich durch regionale Spannungen und hybride Konfliktmuster verstärkt. Digitale Angriffe treten oft synchron zu politischen, militärischen oder diplomatischen Entwicklungen auf. Punktuell werden sie mit physischen Verwundbarkeiten kombiniert. Auch Angriffswellen zwischen Indien und Pakistan konnten beobachtet werden [86].

### 1.1.2 Technologische Entwicklungen und globale Trends

Neben geopolitischen Faktoren wird die Bedrohungslage zunehmend durch technologische und strukturelle Entwicklungen beschleunigt. Angriffe zeichnen sich durch wachsende Skalierbarkeit, höhere Geschwindigkeit und zunehmende organisatorische Reife aus [62], [138], [139], [342]. Technologische Entwicklungen wirken dabei vor allem als Verstärker bestehender Bedrohungen. Sie verändern, wie Angriffe vorbereitet, durchgeführt und monetarisiert werden.

### Professionalisierung und Arbeitsteilung im Cybercrime

Mit fortschreitender Professionalisierung gewinnt die Fähigkeit zur schnellen, automatisierten und skalierenden Ausführung von Angriffen an Bedeutung. Eine arbeitsteilige Struktur bildet die Grundlage für verkürzte Exploit-Zyklen – die Zeitspanne zwischen dem Entdecken einer Sicherheitslücke und ihrer aktiven Ausnutzung – sowie eine zunehmende Dominanz automatisierter Angriffsketten [138], [139], [342], [345].

Vereinzelte, opportunistische Angriffe wandeln sich hin zu einer arbeitsteilig organisierten Angriffsökonomie, in welcher spezialisierte Akteure einzelne Phasen der Angriffskette übernehmen [138], [139], [342]. Zentrale Elemente dieser Entwicklung sind spezialisierte Märkte für Zugangsdaten, Schadsoftware und Angriffsressourcen. Über diese können Angriffe effizient vorbereitet und skaliert werden [138], [139], [195], [233].

Die Verfügbarkeit großer Mengen kompromittierter Identitäten wirkt dabei als zentraler Skalierungsfaktor. Allein im ersten Halbjahr 2025 wurden weltweit Schätzungen zufolge 16 Milliarden Zugangsdaten erfasst [144]. Rund 1,8 Milliarden davon wurden für Folgeangriffe genutzt [139]. Staatliche Eingriffe und internationale Strafverfolgungsmaßnahmen können kriminelle Infrastrukturen kurzfristig erheblich stören. Jedoch werden die zugrunde liegenden arbeitsteiligen Strukturen dadurch bislang nur begrenzt verändert, da sich Plattformen und Netzwerke häufig schnell neu formieren [31], [32], [33], [34], [138], [198], [345].

### Geschwindigkeit, Automatisierung und Exploit-Zyklen

Parallel zur organisatorischen Professionalisierung nimmt die Geschwindigkeit moderner Cyberangriffe deutlich zu [74], [139], [148]. Im Jahr 2025 wurden weltweit mehr als 48.000 neue Schwachstellen öffentlich bekannt. Für einen erheblichen Anteil davon stand zeitnah funktionaler Exploit Code zur Verfügung, also fertige Software-Werkzeuge, um diese Lücken gezielt für Angriffe auszunutzen [139], [258].

Automatisierte Scans, standardisierte Exploit-Kits und wiederverwendbare Angriffsmodule ermöglichen es Angreifern, Schwachstellen nahezu in Echtzeit zu identifizieren und auszunutzen. Dadurch verlagert sich das Kräfteverhältnis zwischen Angreifern und Verteidigern zunehmend auf die Fähigkeit, schnellere Automatismen als die jeweilige Gegenseite zu nutzen.

Sicherheitsvorfälle entstehen dabei häufig aus der Kombination mehrerer moderater Schwächen und struktureller Defizite. Besonders relevant sind Lücken in Patch-Management, Priorisierung und Reaktionsfähigkeit [73], [139], [233], [342], die durch die Abhängigkeit von US-zentrierten Infrastrukturen wie dem Common Vulnerabilities and Exposures (CVE)-System und der National Vulnerability Database (NVD) zusätzlich unter Druck geraten [271].

Die fortschreitende Automatisierung verlagert den Schwerpunkt künftiger Angriffe zunehmend weg von einzelnen technischen Schwachstellen hin zu systemischen Angriffsflächen. Betroffen sind insbesondere zentralisierte Plattformen, Cloud-Dienste und Identitätsinfrastrukturen, die automatisierte Zugriffe in großem Maßstab ermöglichen [74], [139], [148], [342].

**Künstliche Intelligenz in Angriff und Verteidigung**

Künstliche Intelligenz (KI) prägt die globale Cybersicherheitslage durch eine deutliche Beschleunigung und Skalierung bestehender Bedrohungen. Sie wirkt als Effizienz- und Reichweitenverstärker, da Angriffe schneller vorbereitet, präziser ausgerichtet und in größerem Umfang durchgeführt werden können [138], [139], [230], [235], [246], [335], [342].

Auf Angreiferseite wird KI zunehmend eingesetzt, um einzelne Schritte bestehender Angriffsketten zu automatisieren und vollständige Kampagnen effizient zu orchestrieren. Dazu zählen insbesondere die Erstellung täuschend echter Inhalte für Phishing und Betrug, die Auswahl geeigneter Zielgruppen sowie die Anpassung von Angriffen an Reaktionen der Opfer [66], [138], [139], [335], [336], [342].

Generative Modelle senken dabei die sprachlichen und inhaltlichen Einstiegshürden. Glaubwürdige Kommunikationsmuster lassen sich ohne tiefes Fachwissen oder kulturelle Nähe erzeugen, wodurch die Erfolgswahrscheinlichkeit sozialer Manipulation steigt [139], [335]. Da KI-generierte Inhalte sprachlich und kontextuell kaum noch von legitimer Kommunikation zu unterscheiden sind, verlieren rein inhaltsbasierte Erkennungsmechanismen an Wirksamkeit. Sie müssen zunehmend durch identitäts- und verhaltensbasierte Verfahren ergänzt werden [336].

Diese Effekte sind auch im laufenden Angriffsgeschehen messbar. KI-gestützte Phishing-Kampagnen, insbesondere im E-Mail-Umfeld, gewinnen weiter an Vo-

lumen und sprachlicher Qualität. Im zweiten Quartal 2025 wurden weltweit über 1,13 Mio. Phishing-Angriffe registriert, mit starkem Wachstum bei Business Email Compromise ein Betrug via manipulierter Geschäfts-E-Mails zur Auslösung falscher Zahlungen –, wobei ein erheblicher Teil KI zur Anpassung nutzt [7], [110], [179], [180], [335], [342]. Darüber hinaus wird KI direkt in Angriffswerkzeuge integriert, was etwa Schadsoftware ermöglicht, ihr Verhalten dynamisch zur Umgehung von Filtern anzupassen, oder den Einsatz von Deepfakes für CEO-Fraud und Identitätsschwindel befeuert [60], [63], [67], [163], [188], [194], [329].

Auch auf Verteidigerseite wächst der Einsatz KI-gestützter Verfahren. Sicherheitslösungen nutzen maschinelles Lernen zur Erkennung von Anomalien, zur Priorisierung von Warnmeldungen und zur Unterstützung bei der Reaktion auf Vorfälle [185], [328], [342], [345]. Automatisierte Analysen und Entscheidungsunterstützung helfen dabei, mit der steigenden Geschwindigkeit moderner Angriffe Schritt zu halten, Erkennungs- und Reaktionszeiten zu verkürzen und personelle Engpässe teilweise zu kompensieren [185], [199], [313], [328]. Gleichzeitig bleibt der tatsächliche Reifegrad vieler Organisationen begrenzt. So halten derzeit nur 14 Prozent der befragten Organisationen ihre bestehenden KI-basierten Sicherheitsmaßnahmen für vollumfänglich wirksam. Dies weist auf Defizite bei Integration, Governance und Datenqualität hin [185], [259], [328]. Es entsteht ein Ungleichgewicht, da Angreifer schneller experimentieren können, während Verteidiger an regulatorische, organisatorische und betriebliche Rahmenbedingungen gebunden sind [138], [335], [342]. Entscheidend für die Zukunft ist daher die Fähigkeit, KI kontrolliert und professionell in bestehenden Sicherheitsprozesse einzubetten, um der automatisierten Angriffsökonomie standzuhalten [59], [74], [138], [328], [335], [342].

**1.1.3 Ransomware – Systematische Bedrohung**

Ransomware hat sich von einer einzelnen Angriffsmethode zu einem eigenständigen, global organisierten Ökosystem entwickelt, welches eine der dominierenden Bedrohungen darstellt. International zählt Ransomware nicht nur weiterhin zu den häufigsten finanziell motivierten Angriffen, sondern wird zunehmend als strukturierter Geschäftsprozess betrieben. Die beobachtete Aktivität dieser Angriffe stieg im ersten Halbjahr 2025 international um rund 179 Prozent und ist inzwischen in rund 44 Prozent aller untersuchten Sicherheitsvorfälle vertreten [138], [139], [233], [342]. Technologische

Automatisierung, arbeitsteilige Rollenmodelle und neue Monetarisierungsstrategien haben dazu geführt, dass Ransomware-Kampagnen schneller skalieren, flexibler agieren und resilienter gegenüber Strafverfolgungsmaßnahmen sind als in den Jahren zuvor [138], [139], [345].

**Erfolgsmodell Ransomware-as-a-Service**

Ein wesentlicher Faktor für die anhaltende Verbreitung von Ransomware ist die Etablierung von Ransomware-as-a-Service (RaaS). Dabei ist ein klarer Übergang von geschlossenen Tätergruppen hin zu arbeitsteiligen Plattformmodellen zu beobachten. Entwickler, Betreiber und ausführende Angreifer übernehmen getrennte Rollen [138], [139], [191], [233]. RaaS-Anbieter stellen Verschlüsselungssoftware, Zahlungsinfrastuktur, Verhandlungsleitfäden und Leak-Sites bereit. Sogenannte Affiliates führen die eigentlichen Angriffe durch.

Dieses Modell senkt Einstiegshürden und ermöglicht es auch technisch weniger versierten Akteuren, hochwirksame Erpressungskampagnen umzusetzen [68], [138], [139]. Gleichzeitig erhöht die Arbeitsteilung die Skalierbarkeit. Mehrere Kampagnen können parallel laufen, Anpassungen an Zielregionen oder Branchen erfolgen schnell, und erfolgreiche Techniken verbreiten sich innerhalb kurzer Zeit über das gesamte Ökosystem [139], [233], [342]. Die zugrunde liegenden arbeitsteiligen Geschäftsmodelle gelten weiterhin als weitgehend resilient gegenüber staatlichen Eingriffen, da polizeiliche Erfolge oft nur unmittelbare, punktuelle Effekte erzielen, während sich das kriminelle Ökosystem aufgrund seiner dezentralen Struktur langfristig immer wieder neu formiert [193].

**Zielverlagerung und sektorale Verteilung**

Die Verteilung von Ransomware-Angriffen zeigt eine Verschiebung der Zielauswahl. Während große Unternehmen und kritische Infrastrukturen weiterhin im Fokus stehen, nehmen Angriffe auf kleine und mittlere Organisationen sowie weniger geschützte Sektoren zu [139], [312], [342]. Dies wird vor allem durch Automatisierung und die Verfügbarkeit massenhaft kompromittierter Zugangsdaten begünstigt [138], [139].

Zu den häufig betroffenen Sektoren zählen die Fertigungsindustrie, Technologieunternehmen, der Handel sowie Gesundheits- und Dienstleistungssektoren [139], [313], [342]. Regional konzentrieren sich viele dokumen-

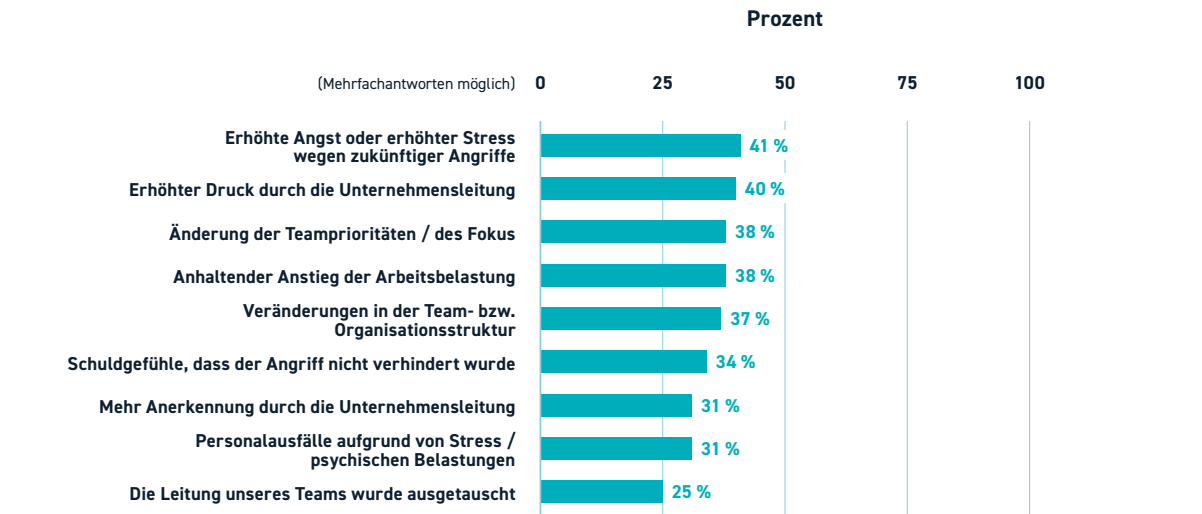
tierte Ransomware-Fälle auf hochdigitalisierte Volkswirtschaften, insbesondere Nordamerika und Europa. Andere Regionen sind häufig indirekt über Lieferketten und Dienstleister betroffen [110], [139], [342].

Es werden zunehmend identitätsbasierte Einstiegspunkte genutzt. Dadurch verzahnt sich Ransomware enger mit anderen Formen von Datendiebstahl und Spionage [233], [246], [342]. Die Grenze zwischen klassischem Datendiebstahl, Spionage und Erpressung verschwimmt. Die Kombination aus arbeitsteiligen RaaS-Modellen und diversifizierten Monetarisierungsstrategien ermöglicht es Angreifern dabei, Kampagnen flexibel zu skalieren und sich nach staatlichen Eingriffen rasch neu zu formieren. Gleichzeitig begünstigt die Verfügbarkeit massenhaft kompromittierter Zugangsdaten eine strategische Neuausrichtung: Da der Zugriff vermehrt über valide Identitäten erfolgt, rückt die strukturelle Verwundbarkeit von Organisationen gegenüber ihrer rein technischen Absicherung in den Vordergrund. Dies ermöglicht es Angreifern, gezielt Akteure mit hoher digitaler Abhängigkeit und ausgeprägten Lieferkettenverflechtungen zu infiltrieren und dort dauerhafte Zugänge zu etablieren. Ransomware ist damit weniger als punktuelle Erpressung zu verstehen, sondern zunehmend als Bestandteil langfristiger Ausnutzungs- und Druckstrategien innerhalb einer globalisierten Angriffsökonomie [138], [139], [233], [246], [312], [342].

**Psychologische und politische Wirkung von Erpressung**

Erpressungsangriffe entfalten neben wirtschaftlichen Schäden eine ausgeprägte psychologische Wirkung auf Organisationen und ihre Führungsebenen. Die Kombination aus Zeitdruck, Unsicherheit über das tatsächliche Ausmaß des Schadens und der Androhung weiterer Konsequenzen belastet die Entscheidungsfindung erheblich [40], [313]. Diese psychologische Dimension ist ein zentraler Bestandteil der Wirksamkeit von Erpressung, da sie gezielt Stresssituationen erzeugt und rationale Abwägungsprozesse erschwert (siehe diese und weitere psychische Auswirkungen in Abbildung 1) [110].

Ransomware beeinflusst nicht nur Managemententscheidungen, sondern belastet auch betroffene Beschäftigte erheblich. IT- und Sicherheitsverantwortliche berichten nach schweren Vorfällen häufig von anhaltendem Stress, erhöhter Arbeitsbelastung und Erschöpfung. Diese Effekte können die Reaktionsfähigkeit von Organisationen langfristig beeinträchtigen [40], [311].



Quelle: [313]

**Abbildung 1: Auswirkungen von Ransomware Attacken auf IT- und Security Teams (n=1.700)**

Auf organisationaler Ebene verstärken Erpressungsangriffe Unsicherheiten hinsichtlich Verantwortlichkeiten, Haftungsfragen und öffentlicher Kommunikation. Auch die Erwartung von Reputationsschäden, regulatorischen Konsequenzen oder politischer Aufmerksamkeit beeinflusst organisationsinterne Entscheidungsprozesse [40], [110].

Die lange Dauer von Sicherheitsvorfällen bindet erhebliche personelle und technische Ressourcen. Operative Einschränkungen können sich dadurch über mehrere Monate hinweg erstrecken [157].

Das Ausmaß betrieblicher Auswirkungen ist an den Digitalisierungsgrad und die strukturelle Abhängigkeit von IT-gestützten Prozessen gekoppelt. Stark digitalisierte Organisationen reagieren besonders sensibel, da Ausfälle unmittelbar geschäftskritische Kernprozesse betreffen. Gleichzeitig können auch weniger digitalisierte Akteure durch Abhängigkeiten von zentralen Kommunikations-, Steuerungs- oder Logistiksystemen erhebliche Produktivitätsverluste erleiden [185], [313].

Entsprechend liegen die täglichen Ausfallkosten in hochdigitalisierten Umgebungen im Durchschnitt um den Faktor 1,5 bis 2 höher [185], [313].

Produktivitätsverluste entstehen nicht nur durch technische Ausfälle. Organisatorische Maßnahmen wie Notfallabschaltungen, eingeschränkte Zugriffsrechte, zusätzliche Abstimmungsprozesse oder Personalumverteilungen verlängern häufig Dauer und Wirkung eines Vorfalls [27], [185]. Ein erheblicher Teil der Beeinträchtigung entfällt dabei auf Koordination, Entscheidungsfindung und Wiederanlaufprozesse [313].

Cyberangriffe wirken zudem zunehmend kaskadierend. In rund 10 bis 30 Prozent der Vorfälle führen Ausfälle einzelner digitaler Komponenten aufgrund enger System- und Lieferkettenkopplung zu Beeinträchtigungen externer Partner, nachgelagerter Prozesse oder öffentlicher Dienstleistungen [110], [342]. Cybervorfälle bleiben dadurch häufiger nicht auf einzelne Organisationen begrenzt, sondern entfalten Wirkung über Organisations- und Systemgrenzen hinweg [27], [110].

## Wirtschaftliche Schäden durch Betriebsunterbrechung, Wiederherstellung und Datenschutz

Die wirtschaftlichen Auswirkungen von Cyberangriffen lassen sich sowohl auf gesamtwirtschaftlicher Ebene als auch anhand der Kosten einzelner Vorfälle quantifizieren [27], [48]. Der durchschnittliche Schaden eines Cyberangriffs liegt bei rund 250.000 US-Dollar (ca. 212.000 Euro) pro Organisation. Die jährlichen volkswirtschaftlichen Verluste summieren sich in einzelnen Industrieländern auf hohe Milliardenbeträge [346]. Auf globaler Ebene werden die insgesamt durch Cyberkriminalität verursachten Kosten bis 2029 auf rund 14,23 Billionen Euro geschätzt [157].

Ein Großteil der Schäden durch Cyberangriffe in Deutschland entsteht durch Betriebsunterbrechungen und Folgekosten. Rund 70 Prozent der von Unternehmen gemeldeten Schäden durch Datendiebstahl, Industriespionage und Sabotage entfallen direkt auf Cyberangriffe [27]. Für 2025 entspricht dies einem wirtschaftlichen Schaden von etwa 202,4 Mrd. Euro (siehe Abbildung 2). Der größte Kostentreiber sind Ausfälle zentraler Geschäftsprozesse. Zeitweise oder vollständige Betriebsunterbrechungen wirken sich unmittelbar auf Umsatz, Lieferfähigkeit und interne Abläufe aus und können kaskadierende Effekte entlang von Wertschöpfungs- und Lieferketten auslösen [27].

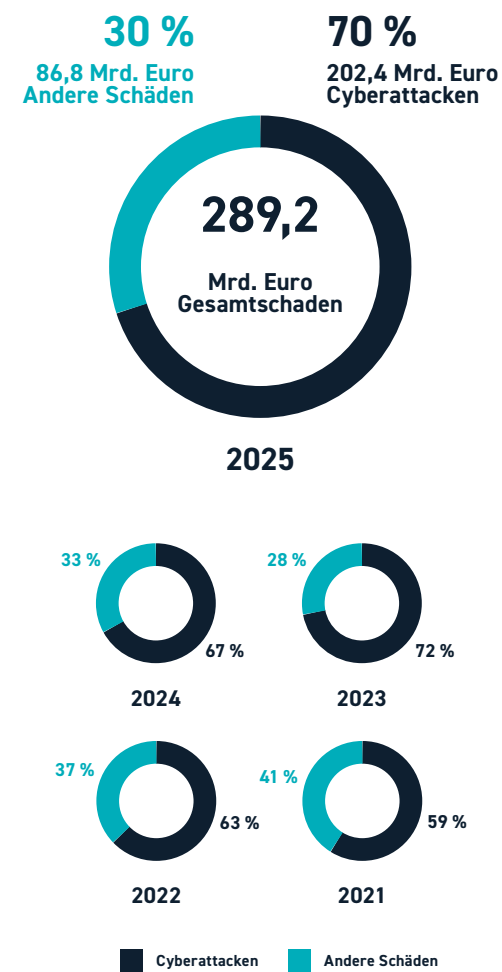
Einen weiteren wesentlichen Kostenblock bildet die Wiederherstellung nach Cybervorfällen. Dazu zählen forensische Analysen, die Wiederherstellung von Systemen und Daten, externe Unterstützungsleistungen sowie nachgelagerte Absicherungsmaßnahmen. Diese Kosten fallen unabhängig davon an, ob Lösegeldzahlungen erfolgen [185], [313].

Hinzu kommen datenschutz- und compliancebezogene Folgekosten. Cyberangriffe mit Datenabfluss oder -manipulation führen regelmäßig zu Meldepflichten gegenüber Aufsichtsbehörden, rechtlicher Beratung, internen Untersuchungen sowie möglichen Strafzahlungen, insbesondere in regulierten Branchen [27], [110], [185].

Je nach Angriffstyp unterscheidet sich die Kostenstruktur deutlich. Während bei Ransomware-Vorfällen vor allem Betriebsunterbrechung und Wiederherstellung dominieren, stehen bei Datenschutzvorfällen rechtliche, regulatorische und reputationsbezogene Folgekosten im Vordergrund. Diese Heterogenität erschwert pauschale Kalkulationen und erfordert eine differenzierte Bewertung von Cyberrisiken [185], [313].

## Beispiele aus der Industrie

In der Praxis äußern sich Cyberangriffe in deutschen Unternehmen häufig in lang anhaltenden Störungen zentraler Geschäftsprozesse [27], [185]. Betroffen sind insbesondere IT-gestützte Abläufe wie Auftragsannahme, Abrechnung, Logistiksteuerung oder interne Freigabeprozesse. Auch wenn physische Anlagen oder Dienstleistungen formal weiterlaufen können, entstehen wirtschaftliche Schäden durch verzögerte Lieferungen, Vertragsstrafen und den Verlust operativer Steuerungsfähigkeit [27].



Quelle: [27]

**Abbildung 2: Anteil von Cyberattacken an wirtschaftlichen Schäden in Deutschland (n=868)**

Ein aktuelles Beispiel aus dem Jahr 2025 ist ein Cyberangriff auf einen externen IT-Dienstleister von Vodafone. Infolge des Vorfalls war die zentrale Vertriebsplattform „Vodafone Sales World“ über mehrere Tage nicht verfügbar. Partner und Mitarbeitende hatten keinen Zugriff auf notwendige Systeme und Daten, wodurch vertriebsnahe Geschäftsprozesse erheblich gestört wurden [83].

Ein weiterer Vorfall betraf den Molkereikonzern Arla Foods Deutschland. Kompromittierte IT-Systeme eines Produktionsstandortes führten zu vorübergehenden Produktionseinschränkungen und Lieferverzögerungen [81].

Zudem meldete Adidas einen Vorfall, bei dem über einen externen Kundendienst Zugriff auf Kontaktinformationen von Kunden erlangt wurde. Auch ohne den Abfluss von Zahlungsdaten wurden umfangreiche Datenschutz- und Wiederherstellungsmaßnahmen ausgelöst [321].

Wie verwundbar hochgradig vernetzte Produktionsstrukturen sind, verdeutlicht der Cyberangriff auf den Automobilhersteller Jaguar Land Rover im Jahr 2025. Obwohl primär ein einzelnes Unternehmen angegriffen wurde, führte die wirtschaftliche Interdependenz zu einem geschätzten Gesamtschaden von 1,9 Milliarden Pfund für den britischen Industriestandort. Über 5.000 Unternehmen entlang der Lieferkette waren von mehrwöchigen Produktionsausfällen und massiven Störungen betroffen. Dieser Vorfall dient als Warnsignal für die deutsche Industrie: Aufgrund der engen internationalen Verflechtungen können Produktionsstopps im Ausland unmittelbar hiesige Zulieferer schädigen. Cyberresilienz erweist sich damit nicht mehr nur als betriebliche, sondern als zentrale volkswirtschaftliche Notwendigkeit [84].

Unabhängig von Branche oder Unternehmensgröße verursachen selbst technisch begrenzte Cyberangriffe erhebliche Wiederherstellungs- und Folgekosten. Diese können sich innerhalb weniger Tage auf einen hohen sechsstelligen Betrag summieren. Häufig gehen sie mit langfristigen Reputations- und Vertrauenseffekten einher [27], [82], [185], [313].

Unternehmen berichten nach Cyberangriffen von erschwerten Vertragsverhandlungen, vorsichtigerem Verhalten von Geschäftspartnern und steigenden Versicherungsprämien, insbesondere bei öffentlich bekannt gewordenen Datenabflüssen oder längeren Betriebsstörungen [27], [40], [185].

## 1.2 NATIONALE BEDROHUNGSLAGE: DEUTSCHLAND IM FOKUS

Deutschland ist einer der am stärksten von Cyberangriffen betroffenen Staaten innerhalb der EU [27], [30], [48], [103], [110], [246]. Etwa 87 Prozent der Unternehmen in Deutschland sind von digitalen oder analogen Angriffen betroffen. 77,5 Prozent der Unternehmen waren in den vergangenen zwölf Monaten Opfer mindestens eines erfolgreichen Cyberangriffs [157]. Das Angriffsgeschehen ist von wiederkehrenden branchen- und größenübergreifenden Mustern geprägt [48], [110], [342]. Dies erhöht insbesondere in ressourcenbegrenzten Organisationen die Anfälligkeit gegenüber skalierten Angriffen [27], [337]. Diese Exponiertheit resultiert aus der hohen wirtschaftlichen Bedeutung Deutschlands, der starken digitalen Vernetzung sowie der zentralen Rolle deutscher Organisationen in europäischen Liefer- und Dienstleistungsketten [27], [48], [246].

Ransomware bleibt in Deutschland eine der folgenschwersten Bedrohungen. Angriffe sind häufig mit Datendiebstahl kombiniert und verursachen erhebliche wirtschaftliche Schäden [27], [185], [233], [313]. Eine Entspannung ist in den kommenden Jahren nicht zu erwarten. Vielmehr dürfte sich die Lage weiter verschärfen [138], [146], [246], [342], [345].

### 1.2.1 Angriffsmuster und Ziele

Die in Deutschland beobachteten Cyberangriffe folgen klaren Strukturen in Bezug auf Einstiegspunkte, Zielgruppen und Angriffszielsetzung. Der überwiegende Teil der Vorfälle ist auf wenige, wiederkehrende Angriffsvektoren zurückzuführen, welche sich unabhängig von Branche oder Organisationsgröße ausnutzen lassen [48], [110], [246], [342]. Dazu zählen Phishing, der Missbrauch bestehender Zugangsdaten sowie der maliziöse Einsatz legitimer Dienste.

#### Häufige Vektoren: E-Mail, legitime Dienste

Phishing ist mit rund 60 Prozent der dominierende Einstiegspunkt in Europa. Deutschland zählt dabei zu den besonders stark betroffenen Staaten [110], [246]. E-Mail bleibt einer der zentralen Angriffswege. Analysen des E-Mail-Verkehrs in deutschen Unternehmen zeigen, dass Phishing-Nachrichten systematisch auf den Diebstahl von Zugangsdaten abzielen. Häufig werden bekannte Marken wie DHL oder Vertrags- und Signaturdienste wie DocuSign imitiert [174], [176].

Besonders verbreitet sind täuschend echte Login-Seiten. Sie werden über Links oder HTML- und PDF-Anhänge ausgeliefert und zielen auf Cloud- und Webmail-Konten [64], [174], [342]. Diese Angriffsformen gewinnen weiter an Bedeutung und werden zunehmend über missbräuchlich genutzte Cloud-Dienste skaliert [58], [175], [180]. Inhalte, Absender und Sprache werden dabei automatisiert variiert, um Filtermechanismen zu umgehen und die Erfolgswahrscheinlichkeit zu erhöhen [174], [177], [178]. Phishing in Deutschland dient häufig als Startpunkt für Kontoübernahmen und nachgelagerte Erpressungsszenarien [174], [246], [342].

Neben E-Mail gewinnen weitere Kommunikationskanäle an Bedeutung. Phishing-Versuche erfolgen zunehmend über Messenger-Dienste und SMS. Aus Sicht von Bürgern werden sie inzwischen häufiger wahrgenommen als klassische Phishing-E-Mails [47], [104], [105].

Parallel dazu werden legitime digitale Dienste verstärkt als Angriffsvektor missbraucht. Cloud-Anwendungen, Datei- und Kollaborationsdienste sowie Freigabe- und Authentifizierungsfunktionen dienen dazu, schädliche Inhalte über vertrauenswürdige Plattformen zu verbreiten oder unbefugte Zugriffe zu etablieren [174], [246], [342].

#### Angriffsautomatisierung auf breiter Front

Die Bedrohungslage in Deutschland ist geprägt von hochgradig automatisierten Angriffen, die gezielt dauerhaft exponierte und schlecht gepflegte Dienste ins Visier nehmen. Besonders gefährdet sind sogenannte Randkomponenten, also Systeme, die als Schnittstelle fungieren und das interne Netzwerk direkt mit dem Internet verbinden – etwa VPN-Zugänge oder Firewalls. Da sie von außen sichtbar sind, dienen sie Angreifern oft als erstes Einfallstor [138], [139], [312], [342].

Ein zentrales Element ist die Wiederverwendung von Angriffs-komponenten – in Deutschland so wie global. Zugangsdaten, Exploits und Schadprogramme werden in arbeitsteiligen Strukturen bereitgestellt und über unterschiedliche Kampagnen hinweg erneut eingesetzt [138], [139], [342]. Dadurch bleiben bekannte Angriffsmuster über längere Zeiträume wirksam und lassen sich schnell auf neue Ziele übertragen [48], [342].

Besonders häufig werden veraltete Web-Anwendungen, vergessene Subdomains oder nicht mehr aktiv betreute Dienste angegriffen. Diese bleiben trotz geringer funktionaler Bedeutung dauerhaft exponiert. Das Angriffsgeschehen wird damit weniger durch neue

Exploits als durch strukturelle Defizite im Lebenszyklus- und Stilllegungsmanagement von IT-Diensten geprägt [11], [265].

Automatisierung beschleunigt zudem die Folgeschritte nach einem erfolgreichen Erstzugriff. Laterale Bewegungen, Datenabfluss oder Erpressung können vorbereitet oder teilautomatisiert durchgeführt werden. Dadurch verkürzt sich die Zeit zwischen Kompromittierung und Schadwirkung [139], [233], [342].

### 1.2.2 Digitale Identitäten und Zugangsinfrastrukturen

Digitale Identitäten zählen zu den wichtigsten Einstiegs-punkten für Cyberangriffe in Deutschland [110], [138], [139]. Digitale Identitäts- und Zugangsinfrastrukturen (Identity and Access Management (IAM)) haben sich in vielen Organisationen zu einer zentralen Steuerungsebene entwickelt. Über Identitätsdienste und Single-Sign-on-Lösungen werden heute Zugriffe auf zahlreiche Fachanwendungen, Cloud-Dienste und Administrationsfunktionen gebündelt. Sicherheitsvorfälle auf dieser Ebene wirken daher nicht punktuell, sondern entfalten häufig eine systemweite Wirkung [139], [246], [342].

Angriffe zielen zunehmend auf die Übernahme zentraler Identitäten, da diese einen unauffälligen und nachhaltigen Zugriff auf Cloud-, On-Premise- und hybride Umgebungen ermöglichen [139], [342]. Zugangsinfrastrukturen werden dadurch nicht nur zu einem technischen, sondern auch zu einem organisatorischen Risikofaktor, insbesondere in komplexen, arbeitsteiligen IT-Landschaften [246].

#### Passwort-Spraying, Credential Stuffing, MFA-Bypass

Angriffe auf digitale Identitäten erfolgen häufig über automatisierte Anmeldeversuche. Sie sind auf Skalierung und geringe Sichtbarkeit ausgelegt. Dabei spielen insbesondere Passwort-Spraying und Credential Stuffing eine zentrale Rolle [48], [139], [339], [342]. Beim Passwort-Spraying werden häufig genutzte Passwörter parallel über viele Konten hinweg getestet. Credential Stuffing basiert auf bereits kompromittierten Zugangsdaten aus früheren Datenlecks, die aufgrund verbreiteter Passwortwiederverwendung erneut eingesetzt werden [139], [342]. Dabei zeigt sich eine deutliche Verteilung nach Plattformtypen: Insbesondere Zugangsdaten für soziale Medien und Gaming-Dienste werden in hohem Maße über spezialisierte Marktplätze und Live-Logs

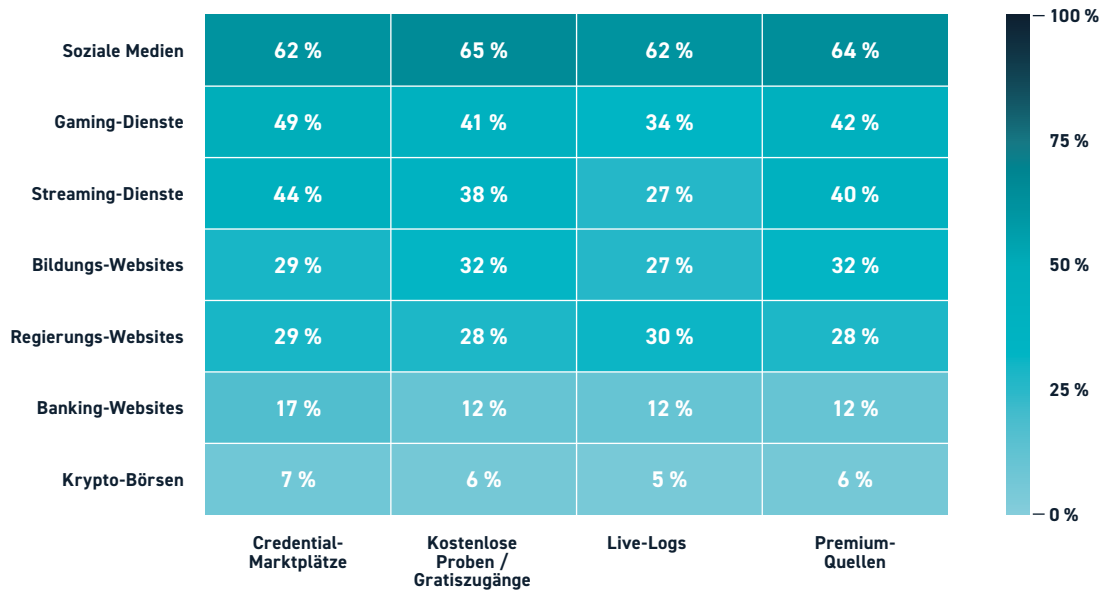


gehandelt (siehe Abbildung 3). Beide Methoden richten sich primär auf E-Mail-Konten, Cloud-Dienste und zentrale Anwendungen. Sie lassen sich mit geringem Aufwand in großem Umfang durchführen [48], [110].

Als Reaktion setzen viele Organisationen auf Multi-Faktor-Authentifizierung (MFA). Angreifer nutzen jedoch gezielt Verfahren, um MFA zu umgehen oder auszunutzen (MFA-Bypass). Zum Einsatz kommen insbesondere Social Engineering, Sitzungsübernahmen oder technische Zwischenschaltungen im Anmeldeprozess [139], [342].

Eine im Umfeld cloudbasierter Arbeitsplattformen beobachtete Methode sind sogenannte Adversary-in-the-Middle-Angriffe (technische Zwischenangriffe auf den Anmeldeprozess). Dabei werden täuschend echte Anmeldeseiten genutzt, um neben Benutzername und Passwort auch Sitzungs- oder Zugriffstokens abzugreifen und bestehende Anmeldungen zu übernehmen [174], [231], [342].

Klassische MFA Verfahren werden zunehmend gezielt umgangen. Der Fokus der Abwehrmaßnahmen verschiebt sich entsprechend [212], [246], [342]. Passwortlose Verfahren wie Passkeys werden insbesondere für privilegierte Konten und zentrale Cloud-Dienste verstärkt diskutiert, da sie strukturelle Abhängigkeiten von menschlichem Fehlverhalten reduzieren können [138], [246], [342].



Quelle: [342]

Abbildung 3: Kompromittierte Website-Zugangsdaten weltweit nach verschiedenen Infostealer-Quellen (n=33.933)

Cloud-Zugänge und Shadow-IT als systemische Risikofaktoren

Cloudbasierte Dienste sind integraler Bestandteil zentraler Geschäfts-, Kommunikations- und Verwaltungsprozesse. In der deutschen Wirtschaft nutzen 90 Prozent der Unternehmen Cloud-Anwendungen. Rund 47 Prozent der IT-Anwendungen werden aus der Cloud betrieben, und 62 Prozent der Unternehmen geben an, ohne Cloud-Lösungen nicht mehr arbeitsfähig zu sein [28].

Mit der Verlagerung von Anwendungen und Daten in die Cloud hat sich zugleich die Zahl digitaler Zugänge und angebundener Identitäten deutlich erhöht [27], [48], [110], [138], [337], [342]. Cloud-Zugänge sind dabei eng mit zentralen Identitäts- und Zugriffsinfrastrukturen verknüpft. Sie erweitern deren Reichweite über Organisationsgrenzen hinweg [246], [342].

Diese Entwicklung erhöht die Komplexität der Zugriffskontrolle erheblich. Da Unternehmen ihre IT-Systeme zunehmend für externe Partner und Dienstleister öffnen, entstehen komplexe Zugriffsstrukturen. Das Risiko: Wenn Berechtigungen nach Projektende nicht entzogen werden oder die Übersicht über diese Gast-Accounts verloren geht, verbleiben ungenutzte Einfallstore, die Angreifer gezielt ausnutzen. Unzureichend verwaltete Berechtigungen, veraltete oder vergessene

Konten sowie fehlende Transparenz über aktive Cloud-Zugriffe tragen regelmäßig zu Sicherheitsvorfällen bei [48], [342].

Ein zusätzlicher Risikofaktor ist die weit verbreitete Nutzung von Shadow-IT. Abteilungen greifen eigenständig auf Anwendungen, Hardware oder Plattformen zurück, um Arbeitsprozesse zu beschleunigen oder kurzfristige Anforderungen zu erfüllen [27], [48], [337].

12 Prozent der deutschen Unternehmen berichten von Problemen durch nicht registrierte IT-Geräte. Etwa 9 Prozent bewerten diese ausdrücklich als mögliches Einfallstor für Cyberangriffe [337]. Shadow-IT wird häufig mit bestehenden dienstlichen Identitäten oder sensiblen Organisationsdaten genutzt, ohne dass Sicherheitskonfigurationen, Berechtigungen oder Protokollierungen zentral gesteuert oder überprüft werden [246], [342].

Shadow-IT verstärkt damit bestehende Risiken im Identitäts- und Zugriffsmanagement. Zugänge entziehen sich der formalen Governance, Sicherheitsrichtlinien werden umgangen, und Kompromittierungen bleiben länger unentdeckt. Gleichzeitig fehlen vielerorts belastbare Kontroll- und Rückbauprozesse. Nur 43 Prozent der Unternehmen suchen regelmäßig nach nicht registrierten oder vergessenen Geräten, während 39 Prozent über keinen definierten Prozess zur Abkopplung alter Geräte und Systeme verfügen [337].

In Verbindung mit zentralisierten Identitätsdiensten können solche unkontrollierten Cloud-Zugriffe die Angriffsfläche erheblich vergrößern und die Nachvollziehbarkeit von Sicherheitsvorfällen deutlich erschweren [48], [246], [342].

Zunehmender Missbrauch legitimer Admin-Zugänge

Administrations- und privilegierte Zugänge – also Konten mit erweiterten Rechten, die tiefgreifende Konfigurationen vornehmen oder auf sensible Gesamtdatenbestände zugreifen können – stellen in modernen IT- und Cloud-Umgebungen einen besonders wirksamen Angriffshebel dar. Ihre Kompromittierung erfolgt häufig über indirekte Wege. Dazu zählen Social-Engineering-Angriffe auf IT-Support- und Helpdesk-Strukturen, die Übernahme schwach abgesicherter Administrationskonten sowie die Eskalation von Rechten nach einem initialen Zugriff [139], [342].

Ein zusätzlicher Risikofaktor liegt in der operativen Nutzung privilegierter Konten im Tagesgeschäft. Aus Effizienz- oder Ressourcenmangel werden Administrationsrechte häufiger und länger eingesetzt als vorgesehen, etwa für Wartung, Support oder Notfallzugriffe. Dadurch steigen Exposition und Missbrauchsrisiken, ohne dass dies unmittelbar erkannt wird [27], [48], [139], [149], [342].

In der Gesamtschau verdichten sich digitale Identitäten, Cloud-Zugänge und privilegierte Konten zu einer zentralen systemischen Angriffsfläche. Automatisierte Angriffe auf Anmeldeprozesse, die Umgehung klassischer Authentifizierungsverfahren, unkontrollierte Cloud-Nutzung und der Missbrauch legitimer Admin-Zugänge verstärken sich gegenseitig.

Mit der weiteren Durchdringung von Cloud- und Plattformdiensten ist davon auszugehen, dass identitätsbasierte Angriffsmuster auch künftig zu den wirkungsvollsten Einstiegspunkten zählen werden. Ohne eine konsistente Steuerung von Identitäten, Berechtigungen und privilegierten Zugängen über Organisations- und Systemgrenzen hinweg steigt das Risiko organisationsweiter Folgeschäden erheblich [138], [246], [342].

1.3 STRUKTURIERTE ANGREIFER – AKTEURE, ZIELE UND MITTEL

Cyberbedrohungen unterscheiden sich aufgrund der Akteurslogiken, mit der sie geplant, kombiniert und strategisch eingesetzt werden [85], [110], [129], [138]. Staatliche Akteure, organisierte Cyberkriminalität sowie hacktivistische und hybride Gruppierungen verfolgen unterschiedliche Ziele und Zeitperspektiven. Sie greifen jedoch häufig auf ähnliche Einstiegspunkte und Infrastrukturen zurück [85], [138], [139], [342].

Cyberrisiken sind nur durch eine differenzierte Betrachtung von Zielen, Mitteln und Organisationsformen der Angreifer belastbar bewertbar [85], [138], [342]. Die folgenden Abschnitte unterscheiden staatliche Akteure (Advanced Persistent Threat, APT) und organisierte Cyberkriminalität. Hacktivistische und hybride Erscheinungsformen werden dabei als Querschnittsphänomene betrachtet [85], [110], [138], [139], [185], [199], [259], [283].

1.3.1 Staatliche Akteure

Staatliche und staatlich unterstützte Akteure bilden eine zentrale Akteursgruppe. Im Unterschied zu primär finanziell motivierten Angreifern verfolgen sie überwiegend langfristige strategische Ziele: Cyberoperationen werden gezielt als Instrument der Außen-, Sicherheits- oder Wirtschaftspolitik eingesetzt. APTs zeichnen sich durch eine hohe operative Persistenz aus. Sie zielen auf einen nachhaltigen Informationsgewinn, politische Einflussnahme oder die Vorbereitung strategischer Handlungsoptionen ab [85], [110], [129], [259]. Trotz vergleichbarer technischer Grundlagen unterscheiden sich APTs deutlich in Zielsetzung, betroffenen Sektoren und Operationsmustern [85], [110], [129], [246]. Es lassen sich drei Zieltypen staatlicher Cyberoperationen unterscheiden: Spionage, Sabotage und Einflussnahme.

Spionage als primäres Ziel

Spionage stellt weiterhin den Schwerpunkt staatlicher Cyberaktivitäten dar. Langfristige Zugriffe werden etabliert, um Regierungsnetze, Forschungseinrichtungen, Telekommunikationsanbieter und technologieintensive Unternehmen auszuspähen. Sichtbare Störungen werden dabei bewusst vermieden [138], [233], [246].

APT-Gruppen mit Bezug zu China werden wiederholt mit systematischer Wirtschafts- und Technologiespionage in Verbindung gebracht. Betroffen sind insbesondere Industrieunternehmen, Halbleiterforschung, Telekommunikation und akademische Einrichtungen [232], [233], [246].

Akteure mit Bezug zu Russland verfolgen eine Doppelstrategie aus Cyberangriffen und Desinformationskampagnen. Diese zielen darauf ab, demokratische Systeme gezielt zu untergraben, politische Instabilität zu schaffen und das Vertrauen in staatliche Institutionen sowie demokratische Prozesse nachhaltig zu erschüttern [21]. Dokumentiert sind Kampagnen gegen staatliche Stellen, diplomatische Vertretungen sowie sicherheitsrelevante Infrastrukturen in Europa und Nordamerika [110], [138], [246].

Im Fall von Iran dienen Cyberoperationen vor allem der regionalen Lageaufklärung sowie der Ausspähung staatlicher und wirtschaftlicher Zielsysteme. Sie stehen häufig im Kontext sicherheitspolitischer Spannungen im Nahen und Mittleren Osten [165], [267].

Nordkoreanische Akteure nutzen vermehrt den gezielten Einsatz von Insidern und extern angeworbenen IT-Fachkräften, die unter falscher Identität in ausländischen Unternehmen tätig werden. Diese Strategie ermöglicht einen direkten Zugriff auf sensible Entwicklungs-, Cloud- und Finanzsysteme, wodurch klassische Abwehrmechanismen gezielt umgangen werden [138], [139], [246]. Ein weiteres operatives Tatfeld sind Cyberangriffe auf Kryptobörsen (z. B. Bybit 2025), um Zugriff auf digitale Vermögenswerte zu erhalten [21].

Sabotage als wirksames Instrument

Sabotage tritt im Vergleich seltener auf, entfaltet jedoch eine hohe politische und symbolische Wirkung. Sie zielt bewusst auf sichtbare Störungen und kurzfristige Effekte. Cyberoperationen werden eingesetzt, um kritische Prozesse temporär zu stören, Verwundbarkeiten offenzulegen oder staatliche Handlungsfähigkeit infrage zu stellen [110], [138], [259].

Insbesondere russische und iranische Akteure werden mit Angriffen auf Energie-, Transport- und Verwaltungsinfrastrukturen in Verbindung gebracht [110], [259], [267]. Diese Aktivitäten zielen auf Abschreckung, Signalwirkung oder Destabilisierung unterhalb der Schwelle militärischer Auseinandersetzungen, bleiben jedoch meist zeitlich begrenzt [85], [138].

Ergänzend rücken strategische digitale Verbindungswege und ausgelagerte IT-Dienstleistungen in den Fokus hybrider Operationen. Vorfälle im Zusammenhang mit Unterseekabeln – unter anderem im Pazifikraum nahe Taiwan – sowie missbräuchlich genutzte IT-Dienstleistungen dienen als Ansatzpunkte, um verdeckten Zugriff auf Systeme zu erlangen und wirtschaftliche oder sicherheitspolitische Ziele zu verfolgen [138], [139].

Einflussnahme- und Informationsoperationen

Einflussnahme- und Informationsoperationen bezeichnen Cyberoperationen, bei denen technische Zugriffe gezielt mit öffentlicher, politischer oder gesellschaftlicher Wirkung verknüpft werden. Im Mittelpunkt steht die kontrollierte Nutzung kompromittierter Informationen und Leaks oder digitale Störaktionen [110], [129], [132], [138].

Akteure mit Bezug zu Russland nutzen kompromittierte Daten und Störaktionen zur Beeinflussung öffentlicher Wahrnehmung und Verstärkung gesellschaftlicher Spannungen [110], [129], [132], [138].

Auch iranische Akteure setzen Datenveröffentlichungen, Drohkampagnen oder symbolische Angriffe ein, um politischen Druck aufzubauen und Narrative zu beeinflussen [267].

Staatliche Akteure unterstützen dabei indirekt hacktivistische Gruppen oder nutzen deren Aktivitäten strategisch aus. Ziel ist es, die eigene Identifikation zu erschweren und Wirkung sowie Reichweite zu verstärken [110], [128], [129].

Hacktivistische Kollektive dienen in diesem Kontext dazu, die öffentliche Sichtbarkeit technischer Cyberoperationen gezielt zu erhöhen. Durch die Kombination aus technischem Zugriff, öffentlicher Kommunikation und indirekter Steuerung lassen sich politische Effekte verstärken, ohne eindeutige staatliche Verantwortung sichtbar zu machen [85], [110], [128], [129].

Regionale Besonderheiten staatlicher APT-Akteure

In der regionalen Betrachtung zeigen sich deutliche Unterschiede in Zieltypen, Wirkmechanismen und strategischer Gewichtung staatlicher Cyberoperationen. Einzelne Akteursprofile nutzen Cyberoperationen nicht ausschließlich zu sicherheitspolitischen Zwecken, sondern auch zur Erfüllung wirtschaftlicher und ressourcenbezogener Interessen [138], [139], [246].

Auch westliche Akteure wie die USA verfügen über ausgeprägte offensive Cyberfähigkeiten, die im Rahmen hybrider Operationen mit informationsstrategischen Elementen kombiniert werden. Im Kontext sicherheitspolitisch relevanter Ereignisse im Energiesektor Venezuelas wurde diskutiert, ob technische Effekte durch vorbereitete narrative Infrastrukturen flankiert wurden, um Wahrnehmung und Deutung der Ereignisse frühzeitig zu beeinflussen [5].

Russland-nahe APTs zeichnen sich durch eine hohe operative Flexibilität aus. Staatliche Stellen, militärische Einheiten und ausgelagerte Akteursstrukturen sind dabei eng verzahnt. Getrennte Gruppen agieren koordiniert und passen ihre Aktivitäten situativ an geopolitische Entwicklungen an [110], [138], [259]. Die Grenzen zwischen staatlichen Operationen und ausgelagerten Strukturen sind häufig fließend [85], [110].

Chinesische APTs werden als besonders langfristig, strategisch und ressourcenintensiv beschrieben. Sie agieren in kontinuierlichen Kampagnen und sind stark arbeitsteilig auf den Aufbau verdeckter, skalierbarer

und nachhaltiger Zugriffsmöglichkeiten ausgerichtet [138], [233], [236], [246]. Diese strategische Ausrichtung manifestiert sich unter anderem in spezialisierten Werkzeugen wie der BRICKSTORM-Malware, die über legitime Administrationsfunktionen unauffällige Persistenz in kritischen Infrastrukturen ermöglicht [69]. Sie zeigt sich auch in langfristig angelegten Kampagnen wie „Salt Typhoon“, mit denen chinesische Akteure seit mindestens 2021 weltweit insbesondere Telekommunikations-, Regierungs- und militärnahe Netzwerke kompromittieren und zur strategischen Vorpositionierung nutzen [204].

Iran-nahe APTs treten im internationalen Vergleich durch hohe Aktivität, Anpassungsfähigkeit und politische Motivation in Erscheinung. Ihre Strukturen gelten als dynamisch und stark von regionalen Konfliktlagen beeinflusst. Staatliche Stellen, Sicherheitsorgane und ideologisch motivierte Gruppen wirken dabei eng zusammen [85], [110], [129], [267]. Im Konfliktumfeld zwischen Israel und Iran stiegen die beobachteten offensiven Cyberaktivitäten iranischer Akteure innerhalb von zwölf Tagen um rund 700 Prozent. Dies unterstreicht die hohe Reaktionsgeschwindigkeit und politische Kopplung dieser Akteure [139].

Nordkoreanische APTs nehmen eine Sonderrolle ein, da sie klassische staatliche Cyberstrukturen mit einer konsequenten finanziellen Ausrichtung kombinieren. Diese Operationen dienen Nordkorea mittlerweile als essenzieller Pfeiler zur Staatsfinanzierung sowie zur Finanzierung staatlicher Programme. Einzigartig ist dabei das Ausmaß, in dem Cyberaktivitäten zur gezielten Umgehung internationaler Sanktionen eingesetzt werden [21], [138], [139], [246].

Für die Verteidigung bedeuten diese regionalen Unterschiede, dass staatliche Cyberoperationen, wirtschaftlich motivierte Angriffe und hacktivistische Kampagnen nicht mit einem einheitlichen Ansatz adressiert werden können. Unterschiedliche Organisationsformen, Zielsetzungen und Wirkmechanismen erfordern differenzierte Gegenmaßnahmen [138], [139], [190], [192], [195], [246], [259].

Für die kommenden Jahre ist eine weitere Verzahnung von Cyberzugriffen, Datenexfiltration und öffentlichkeitswirksamer Nutzung kompromittierter Informationen von staatlichen Akteuren zu erwarten. Dies gilt insbesondere im Vorfeld politischer Entscheidungen, Wahlen oder internationaler Krisen [110], [138], [345].

1.3.2 Organisierte Cyberkriminalität

Organisierte Cyberkriminalität stellt einen hochdynamischen Teil der globalen Bedrohungslandschaft dar. Im Unterschied zu staatlichen APT-Akteuren orientieren sich cyberkriminelle Gruppen primär an wirtschaftlichen Zielen [138], [139], [342], [345]. Ihre Aktivitäten sind heute fest in eine arbeitsteilige Schattenökonomie eingebettet. Zugangsdaten, Schadsoftware, Exploits, Infrastruktur und Geldwäsche-Dienstleistungen werden über spezialisierte Marktplätze gehandelt und flexibel kombiniert [138], [139], [192], [195]. Diese ökonomische Logik prägt sowohl die technische Infrastruktur als auch die Ausgestaltung arbeitsteiliger Angriffsketten.

Kriminelle Infrastruktur

Die zentrale Rolle krimineller Infrastruktur zeigt sich deutlich in aktuellen Strafverfolgungsmaßnahmen. Im November 2025 wurde der Bitcoin-Mixer cryptomixer.io abgeschaltet – ein Dienst zur Anonymisierung von Zahlungsströmen –, über den seit 2016 mehr als 1,3 Milliarden Euro an Kryptowerten aus mutmaßlich kriminellen Quellen abgewickelt worden waren. Ermittlungsbehörden stellten dabei über 25 Millionen Euro in Bitcoin sowie umfangreiche Server- und Logdaten sicher [127].

Parallel dazu stützen sich organisierte cyberkriminelle Strukturen auf sogenannte Bulletproof-Hosting-Dienste. Diese sind resilient gegenüber Abschaltungen, Abuse-Meldungen und Strafverfolgung ausgelegt. Die Anbieter tolerieren oder fördern kriminelle Aktivitäten, verschleiern Betreiberidentitäten und ermöglichen eine schnelle Verlagerung zentraler Infrastruktur bei behördlichem Druck [70].

Aufgrund der modularen und skalierbaren Strukturen weisen organisierte cyberkriminelle Gruppen eine große Zielbreite auf. Angriffe richten sich gegen Unternehmen aller Größen, öffentliche Einrichtungen und zunehmend auch gegen Privatpersonen, sofern wirtschaftliche Erträge zu erwarten sind [139], [312], [342]. Besonders attraktiv sind digital stark abhängige Organisationen, bei denen Betriebsunterbrechungen, Datenverlust oder Reputationsschäden unmittelbare finanzielle Folgen haben [27], [313], [342].

Geschäftsmodelle von Ransomware-Gruppen

Ransomware stellt derzeit das dominierende Geschäftsmodell innerhalb der arbeitsteilig organisierten Schattenökonomie dar [129], [138], [139]. Zentrale Akteure

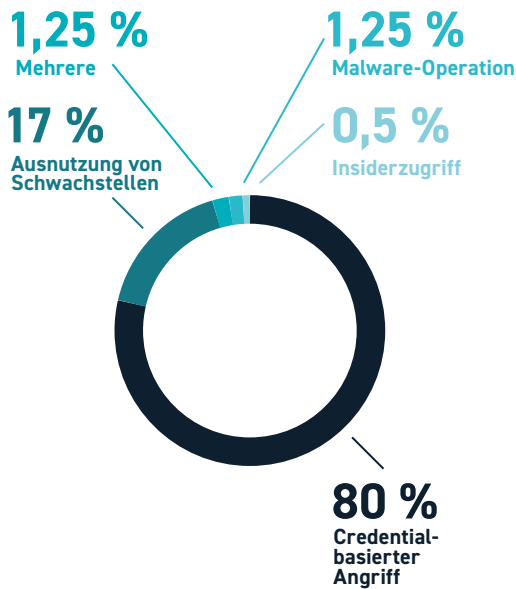
stellen Schadsoftware, Infrastruktur und Zahlungsabwicklung bereit, während angeschlossene Partner die eigentlichen Angriffe durchführen und an den Erlösen beteiligt werden [129], [313]. Dieses Modell senkt die Eintrittshürden und erhöht die Zahl laufender Kampagnen. Kompromittierte Zugangsdaten, Sitzungen oder Fernzugriffe werden in großem Umfang gehandelt und gezielt weiterverwertet [138], [139], [191], [195].

Die Zielauswahl folgt einer klaren wirtschaftlichen Logik: RaaS wird dort eingesetzt, wo Betriebsunterbrechungen oder Datenverluste finanziellen Druck erzeugen [138], [139], [185], [342]. Ziel sind oft Branchen mit hoher Wertschöpfung und geringer Ausfalltoleranz, darunter Technologie, Fertigung, Handel, Dienstleistungen sowie Gesundheits- und Finanzwesen.

Auch Erpressungsmechanismen entwickeln sich weiter. Neben reiner Datenverschlüsselung setzen Ransomware-Gruppen seit mehreren Jahren auf kombinierte Modelle mit Datenabfluss und Veröffentlichungsdrohungen, um den Verhandlungsdruck zu erhöhen [233], [313], [342]. Die Veröffentlichung der Daten dient dabei nicht nur als Druckmittel gegenüber einzelnen Opfern. Sie fungiert zugleich als Marketinginstrument innerhalb der Angreiferökonomie. Die öffentliche Sichtbarkeit erfolgreicher Angriffe erhöht die Glaubwürdigkeit zukünftiger Drohungen und stärkt die Verhandlungsposition der Täter [138], [139].

Zugleich diversifizieren Angreifer ihre Einnahmequellen. Neben Lösegeldzahlungen werden gestohlene Daten zunehmend unabhängig monetarisiert, beispielsweise aus Cloud-, E-Mail- und Kollaborationssystemen [246], [313], [342]. Diese werden durch Weiterverkauf oder Nutzung für Folgeangriffe als eigenständiges Erpressungsinstrument genutzt [138], [139], [342]. Dadurch sinkt die Abhängigkeit von der Zahlungsbereitschaft einzelner Opfer. Selbst Organisationen, die kein Lösegeld zahlen und ihre Systeme selbst wiederherstellen, können durch die Veröffentlichung oder den Verkauf ihrer Daten erheblichen Schaden erleiden. Die Wirksamkeit klassischer Gegenstrategien wird dadurch begrenzt.

Ransomware wird durch flexible, spezialisierte Netzwerke getragen. Diese Entwicklung bildet die Grundlage für eine weitere Arbeitsteilung, etwa durch spezialisierte Zugangsverkäufer, Droh- und Verhandlungsdienste sowie neue Angriffsflächen in Cloud- und Identitätsumgebungen [129], [138], [139], [313].



Quelle: [246]

Abbildung 4: Anteile der von Access Brokern genutzten initialen Zugriffsvektoren

Trotz verstärkter Strafverfolgung bleibt die wirtschaftliche Attraktivität hoch, da sich Strukturen und Marken nach Eingriffen häufig rasch neu formieren [138], [139], [193], [345]. Im Kontext neuer Monetarisierungsstrategien beschleunigt und skaliert der Einsatz von KI bestehende Angriffs- und Erpressungsmechanismen. Sie erhöht Geschwindigkeit, Reichweite und Reproduzierbarkeit bekannter Muster [138], [246], [336], [342]. Mit dem Übergang zu zunehmend agentischen, kampagnenfähig orchestrierten Systemen trägt KI zur weiteren Verdichtung der Angriffsökonomie bei.

Spezialisierung: Von Initial Access Brokern zu Drohkampagnen

Spezialisierte Akteure im Bereich Ransomware sind Initial Access Broker. Sie verkaufen kompromittierte Zugänge zu Unternehmensnetzen und Cloud-Konten sowie entsprechende Fernzugangsinfrastrukturen, etwa VPN-Zugänge [138], [191], [195]. Weltweit wurden 368 aktive Initial-Access-Broker beobachtet, die Zugänge zu mehr als 4.000 kompromittierten Organisationen handelten. In rund 80 Prozent der Fälle ermöglichten gestohlene Zugangsdaten den Erstzugang [246] (siehe Abbildung 4). Die Auslagerung des Initialzugriffs senkt

Kosten und operative Risiken für Ransomware-Gruppen und erhöht zugleich die Skalierbarkeit von Angriffen [138], [191].

Parallel dazu professionalisieren sich die nachgelagerten Erpressungsprozesse. Betreiber von Ransomware-Plattformen stellen standardisierte Infrastrukturen für Kommunikation, Drohkampagnen und Monetarisierung bereit. Dazu zählen Leak-Webseiten, zeitlich gestaffelte Eskalationsmechanismen sowie strukturierte Verhandlungs- und Zahlungsprozesse [129], [195], [345].

In mehr als 50 Prozent der dokumentierten Ransomware-Fälle zahlen betroffene Organisationen weniger als die ursprünglich geforderte Summe. Nur ein Teil überweist den Ausgangsbetrag vollständig [313].

Digitale Zugänge, insbesondere organisationsweit gültige Cloud-Konten, besitzen innerhalb der Ransomware-Ökonomie einen hohen Markt- und Wiederverwertungswert. Ihre Vermarktung erhöht Reichweite und Skalierbarkeit arbeitsteiliger Erpressungsmodelle, ohne dass technische Details im Vordergrund stehen müssen [138], [191], [233], [246], [342].

Für die kommenden Jahre ist insbesondere im Ransomware-Umfeld eine weitere Professionalisierung und Standardisierung arbeitsteiliger Geschäftsmodelle zu erwarten. Diese werden weniger von einzelnen Gruppen als von verfügbaren Rollen, Diensten und Zugängen getragen [138], [139], [189], [342], [345].

1.4. BESONDERS GEFÄHRDETE SEKTOREN UND STRUKTUREN

Cyberangriffe wirken nicht gleichmäßig über alle gesellschaftlichen und wirtschaftlichen Bereiche hinweg, sondern konzentrieren sich auf Strukturen mit hoher digitaler Abhängigkeit und geringer Ausfalltoleranz [110], [138], [185], [246], [259], [342]. Besonders betroffen sind Organisationen, in denen geschäftskritische Prozesse, sensible Daten und privilegierte Zugänge in vernetzten IT-, Cloud- und Plattformumgebungen gebündelt sind. Diese Strukturen werden häufig durch externe Dienstleister und Lieferketten ergänzt, wodurch zusätzliche Abhängigkeiten entstehen [185], [328], [342]. Als besonders exponiert gelten Kritische Infrastrukturen (KRITIS) (Genaueres unter „Aktueller Status der NIS-2-Regulierung“ im Anhang), öffentliche Verwaltungen, mittelständische Unternehmen sowie digitale Dienstleister mit hoher System- und Ökosystemrelevanz [138], [139], [185], [246], [259], [328], [339], [342].

1.4.1 Kritische Infrastrukturen

KRITIS stehen weltweit im Fokus von Cyberangriffen, denn Störungen bei KRITIS entfalten aufgrund ihrer systemischen Funktion unmittelbare Auswirkungen auf Versorgungssicherheit, öffentliche Ordnung und gesellschaftliches Vertrauen [48], [51], [110], [259]. Einen generellen Überblick über durchschnittliche Kosten eines Datenlecks nach Branchen liefert Abbildung 5.

Strukturelle Ursachen der erhöhten Gefährdung kritischer Infrastrukturen

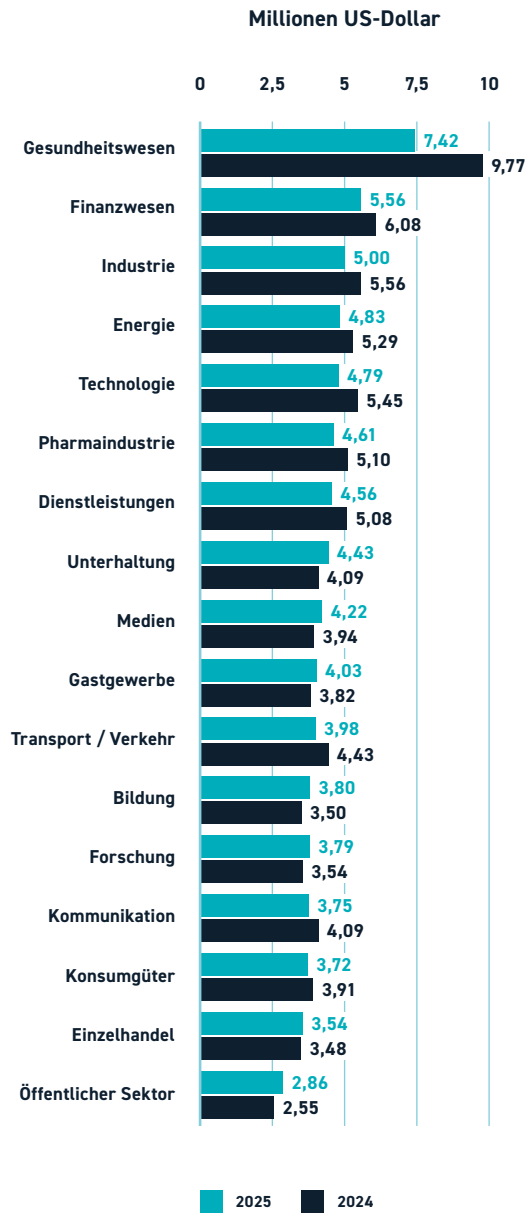
Die besondere Gefährdung von KRITIS resultiert aus einer engen Verzahnung von IT- und OT-Systemen (Operational Technology), historisch gewachsenen Infrastrukturen sowie komplexen Betreiber- und Lieferantenstrukturen [48], [110], [145], [259]. Ein zentraler Risikofaktor sind dabei dauerhaft notwendige externe Zugriffe, insbesondere im Rahmen von Fernwartung und Dienstleistermodellen. Privilegierte Zugänge und geteilte Betriebsmodelle werden dadurch zu zentralen Angriffspfaden [246], [259], [342].

Jeder zweite KRITIS-Betreiber mit OT-Infrastruktur meldet mindestens einen sicherheitsrelevanten Vorfall pro Jahr. In rund 60 Prozent der Fälle sind IT- und OT-Systeme gleichzeitig betroffen [110], [145], [185], [259].

Gesundheitssektor

Der Gesundheitssektor zählt zu den international am stärksten betroffenen KRITIS-Sektoren mit regelmäßig erheblichen wirtschaftlichen und gesellschaftlichen Auswirkungen von Cybervorfällen [48], [185], [313], [342]. Datenpannen verursachten in 2025 durchschnittlich 7,42 Mio. US-Dollar Schaden pro Vorfall und lagen damit deutlich über dem branchenübergreifenden Mittel von 4,44 Mio. US-Dollar [185]. Das Gesundheitswesen wird regelmäßig unter den am häufigsten von Ransomware und schweren Sicherheitsvorfällen betroffenen Branchen geführt [313], [342]. Rund 44 Prozent der global dokumentierten Vorfälle sind mit Ransomware verbunden. Häufige Einstiegspunkte sind kompromittierte Konten und privilegierte Zugänge [313], [342]. Erfolgreiche Angriffe führen regelmäßig zu Ausfällen klinischer Systeme, Terminverschiebungen und Einschränkungen der Patientenversorgung [48], [185].

Strukturelle Faktoren verstärken die Verwundbarkeit zusätzlich. Defizite bei Segmentierung, Zugriffskontrolle und der Absicherung externer Wartungszugänge erschweren Erkennung und Wiederherstellung erheblich [145], [342], [185]. In etwa 30 Prozent der untersuchten Vorfälle waren externe Dienstleister oder ausgelagerte IT-Services involviert. Dies entfaltet im Gesundheitswesen besonders hohe operative Folgewirkungen [342], [185], [337], [328].



Quelle: [185]

Abbildung 5: Durchschnittliche Kosten eines Datenlecks nach Branchen (weltweit)

Energiesektor

Cyberangriffe im Energiesektor sind zwar zahlenmäßig begrenzt, besitzen jedoch ein besonders hohes Schadenspotenzial für Versorgungssicherheit und öffentliche Ordnung [48], [51], [110], [259]. Die durchschnittlichen Kosten pro Sicherheitsvorfall liegen mit rund 4,16 bis 4,89 Mio. US-Dollar über dem globalen Mittel [157], [185].

Fast die Hälfte der Organisationen im Energiesektor in Deutschland und der EU berichten von Betriebsunterbrechungen oder Einschränkungen der Energieversorgung [110], [145]. Langlebige OT-Komponenten, eingeschränkte Update-Fähigkeit und dauerhaft aktive Fernzugänge verstärken bestehende Verwundbarkeiten [145], [259]. Wartungsschnittstellen und unzureichend segmentierte Netze zählen zu den am häufigsten ausgenutzten Zugriffspfaden [110], [145], [259].

Zusätzlich wirken Dienstleister- und Lieferkettenzugänge als Verstärker. Drittparteien spielten in rund 30 Prozent der untersuchten Vorfälle eine Rolle [259], [342].

Bis 2030 ist von steigenden Risiken durch digitale Netzsteuerung, dezentrale Erzeugung und zunehmende Automatisierung von Angriffen auf netznahe Komponenten auszugehen [110], [138], [145], [259].

Öffentliche Verwaltung

Öffentliche Verwaltungen nehmen innerhalb kritischer digitaler Strukturen eine Sonderrolle ein, da sie die digitale Basis staatlicher Funktionsfähigkeit bilden. Unter den betroffenen Organisationen stellen europäische Verwaltungsinstitutionen mit rund 38 Prozent den größten Anteil dokumentierter IT- und OT-naher Vorfälle [110]. Angriffe zielen primär auf die Störung digitaler Prozesse und den Abfluss sensibler Daten. Aus Angreifersicht sind Verwaltungsorganisationen besonders attraktiv, da erfolgreiche Kompromittierungen unmittelbar sichtbare öffentliche Effekte entfalten [48], [110].

OT-nahe Ereignisse betreffen insbesondere gebäudetechnische, verkehrsnah und kommunale Steuerungssysteme. Kommunen sind dabei überdurchschnittlich häufig betroffen. Ransomware-Vorfälle führen regelmäßig zu Ausfällen von Bürgerdiensten und internen Verwaltungsprozessen über Wochen oder Monate hinweg und beeinträchtigen das Vertrauen in staatliche Handlungsfähigkeit unmittelbar [27], [48], [110], [185].

Ein zentraler struktureller Risikofaktor ist der hohe Digitalisierungsgrad bei gleichzeitig begrenzten personellen und finanziellen Ressourcen. Kommunale IT-Landschaften sind häufig historisch gewachsen, heterogen und weisen Defizite bei Standardisierung, Patch-Management, zentraler Sicherheitssteuerung und Fachpersonal auf [48], [337].

Vergleichbare Muster zeigen sich in anderen öffentlichen Einrichtungen mit dezentraler IT-Verantwortung, etwa an öffentlichen Universitäten. Dort führen unzureichend konsolidierte Systemlandschaften zu einer dauerhaft erhöhten Angriffsfläche. Rund 75 Prozent der offen erreichbaren Schwachstellen sowohl an Universitäten als auch in der IT-Landschaft der Bundesländer in Deutschland sind älter als ein Jahr, was auf strukturelle Defizite im Patch- und Schwachstellenmanagement hinweist [10], [11].

Transport und Logistik

Im Transport- und Logistiksektor haben Cyberangriffe regelmäßig sektorübergreifende Folgewirkungen und begünstigen kaskadierende Betriebsunterbrechungen [110], [185], [259], [342]. In Europa entfallen je nach Erhebung zwischen drei und acht Prozent der IT- und OT-nahen Vorfälle auf diesen Sektor [110]. Die Auswirkungen gehen dabei häufig über die unmittelbar betroffenen Organisationen hinaus und entfalten sich entlang nachgelagerter Wertschöpfungsstufen [27], [185], [342].

Ein zentrales Angriffsfeld sind digitalisierte Steuerungs- und Koordinationssysteme. Flotten-, Lager- und Routenmanagementplattformen sind häufig über Cloud-Dienste, externe Schnittstellen und Partnerzugänge angebunden [85], [259], [342]. Unzureichend gesicherte Fernzugänge, kompromittierte Konten und missbrauchte Wartungswerkzeuge zählen zu den häufigsten Angriffsvektoren [145], [259], [342].

Mit der zunehmenden Integration von Betriebstechnologie wächst auch die OT-Exposition des Sektors, insbesondere in verkehrsträgerübergreifenden Steuerungs-, Umschlags- und Infrastruktursystemen [110], [145]. Nahezu die Hälfte der Organisationen mit OT-Anteilen meldet im vergangenen Jahr sicherheitsrelevante Vorfälle [145].

Mit Blick auf die kommenden Jahre ist eine weitere Zunahme der Risiken durch Digitalisierung, Plattformisierung und internationale Abhängigkeiten zu erwarten [185], [259], [342].



1.4.2 Mittelstand und Digitalisierungsdruck

Cyberangriffe stellen für alle Unternehmensgrößen ein wirtschaftliches Risiko dar, wobei sich Wirkung und Bewältigungsfähigkeit deutlich nach Größe unterscheiden. Besonders exponiert ist der Mittelstand. Ihre Rolle in digitalen Liefer- und Dienstleistungsketten sowie begrenzte personelle und finanzielle Ressourcen erhöhen ihre Exposition erheblich [27], [337]. Gleichzeitig stehen kleine und mittlere Unternehmen (KMU) unter systematischem Druck. Digitalisierung und Plattformabhängigkeit nehmen zu, während Bedrohungsintensität und regulatorische Anforderungen schneller wachsen als die verfügbaren Sicherheitskapazitäten.

Cloud-Nutzung und mangelndes Schutzkonzept

Die Verlagerung zentraler Geschäftsprozesse in Cloud- und Software-as-a-Service-(SaaS)-Umgebungen verschiebt das Risikoprofil vieler Unternehmen. Schäden entstehen häufig durch fehlende Governance. Unklare, verteilte Verantwortlichkeiten sowie eine unzureichende Steuerung von Identitäten, Berechtigungen und Drittzugängen stellen zentrale Risikofaktoren dar [185], [246], [337], [342].

MFA wird zunehmend umgangen. Für KMU ist dies besonders kritisch, da zentrale Cloud-Konten organisationsweit wirken. Ein kompromittierter Admin- oder Service-Account kann große Teile der IT- und Datenlandschaft öffnen [139], [174], [246], [342].

Über Identitäts- und Zugriffsrisiken hinaus zeigen sich Defizite in der operativen Steuerung der Cloud-Nutzung. SaaS-Dienste werden häufig außerhalb formaler IT-Prozesse eingeführt und mit bestehenden Identitäten verknüpft. Konsistente Sicherheitskonfigurationen und zentrale Protokollierung fehlen dabei häufig [27], [48], [246], [342]. Hinzu kommt die starke Abhängigkeit von externen Dienstleistern. In rund 30 Prozent der untersuchten Sicherheitsvorfälle erfolgt der Einbruch über Drittparteien oder die Lieferkette, etwa durch kompromittierte Dienstleister oder Software-Partner [342]. Gerade im Mittelstand wachsen externe Zugriffe schneller als Reifegrade bei Zugriffstrennung, MFA-Durchsetzung und Monitoring [246], [337], [342].

Die wirtschaftliche Relevanz dieser Defizite ist hoch. International liegen die durchschnittlichen Kosten pro Sicherheitsvorfall bei 4,44 Mio. US-Dollar (2025) [185], [313]. Stark digitalisierte Organisationen sind besonders anfällig für Betriebsunterbrechungen und auf-

wändige Wiederherstellung. In Deutschland verstärken fehlende Cloud-Governance und schwache Identitätssteuerung unmittelbar Geschäfts- und Lieferkettenrisiken. Diese strukturellen Defizite entfalten ihre Wirkung besonders dort, wo organisationale Kompensationsmechanismen nur eingeschränkt verfügbar sind [27], [185].

Investitions- und Umsetzungsdruck in KMU

Häufig sind Sicherheitsstandards nur teilweise umgesetzt, und strukturierte Risiko- und Notfallprozesse fehlen [27], [147], [337]. Der strukturelle Nachteil wird auch quantitativ sichtbar. Nur 16 Prozent der kleinen Unternehmen erfüllen geltende Cybersicherheitsstandards vollständig, während rund ein Viertel entsprechende Normen gar nicht nutzt [337].

Der Investitionsdruck wird durch die Automatisierung und Skalierung moderner Angriffe weiter erhöht. Automatisierte Angriffsformen erhöhen den Anpassungsdruck insbesondere für ressourcenbegrenzte Organisationen [48], [110], [246], [342]. Gleichzeitig müssen KMU aufgrund immer kürzerer Exploit-Zyklen kontinuierlich in Basismaßnahmen investieren, obwohl Budgets und Personal häufig projekt- statt dauerbetriebsorientiert geplant sind [27], [337].

1.4.3 Lieferketten und IT-Dienstleister als Ziel

Digitale Lieferketten stellen ein zentrales Angriffsfeld dar. Vorgelagerte Dienstleister, Softwareanbieter und technische Abhängigkeiten ermöglichen es Angreifern, mit vergleichsweise geringem Aufwand gleichzeitig auf viele Organisationen zuzugreifen [138], [246], [259], [342].

Diese Verwundbarkeit spiegelt sich in der Wahrnehmung und organisatorischen Maßnahmen wider. 66 Prozent der Organisationen bewerten die Sicherheitsreife ihrer Lieferanten, und 65 Prozent binden die Sicherheitsfunktion in Beschaffungsprozesse ein [346].

Demgegenüber simulieren nur 27 Prozent der Organisationen Cybervorfälle gemeinsam mit Partnern. Lediglich 33 Prozent verfügen über eine vollständige Transparenz ihrer Lieferkettenabhängigkeiten und stimmen ihre Sicherheitsstrategie mit Partnern im Ökosystem ab [346]. Diese Selbsteinschätzungen der Organisationen korrespondieren mit empirischen Befunden. In rund 30 Prozent der untersuchten Sicherheitsvorfälle spielen Drittparteien oder Lieferketten eine Rolle, mit steigender Tendenz [342].

Die besondere Gefährdung resultiert weniger aus einzelnen technischen Schwachstellen als aus strukturellen Abhängigkeiten. Dazu zählen geteilte Identitäts- und Zugriffsmodelle, standardisierte Plattformen, dauerhaft eingerichtete Fernzugänge sowie unklare Verantwortlichkeiten im Sicherheitsmanagement [246], [337], [342].

Kompromittierung über Managed Service Provider

Managed Service Provider (MSP) gelten als besonders wirksamer Angriffshebel. Sie bündeln IT-Betrieb, Fernwartung und Sicherheitsfunktionen für zahlreiche Kunden und benötigen dafür privilegierte, organisationsübergreifende Zugriffsrechte [138], [246], [342]. Angriffe auf MSP zielen darauf ab, über einen einzelnen Einstiegspunkt eine Vielzahl von Kundensystemen zu kompromittieren und Skaleneffekte zu erzielen [138], [259]. Technisch erfolgt dies häufig durch den Missbrauch legitimer MSP-Zugänge, insbesondere über zentralisierte Fernwartungs- und Managementplattformen. Dauerhaft aktive Administrationskonten und zentrale Management-Werkzeuge werden regelmäßig als initiale Zugriffspunkte identifiziert, insbesondere im Zusammenhang mit Ransomware- und Datendiebstahlkampagnen [138], [313], [342]. Vorfälle mit MSP-Beteiligung führen überdurchschnittlich häufig zu längeren Betriebsunterbrechungen und verlängerten Wiederherstellungszeiten. Ursache ist, dass Koordination, Forensik und Wiederanlauf parallel über mehrere betroffene Organisationen hinweg erfolgen müssen [185], [259], [313].

Angriffe über Update-Mechanismen und Remote-Zugänge

Angriffe über Update-Mechanismen und Remote-Zugänge richten sich primär gegen etablierte Vertrauens- und Wartungsketten moderner IT- und Plattformlandschaften. International machen Angriffe auf Lieferketten und Update-Mechanismen zwar einen geringen Anteil aller Vorfälle aus, zählen jedoch zu den schadenträchtigsten Angriffstypen und den Vorfällen mit den längsten Wiederherstellungszeiten [185], [259], [313]. In 2025 lagen Vorfälle mit kompromittierten Update-Prozessen oder zentralen Management-Systemen über dem branchenspezifischen Durchschnittsschaden von 4,44 Mio. US-Dollar pro Vorfall. Sie führten häufig zu mehrwöchigen Wiederherstellungsphasen [185], [313].

Ursache ist, dass nach solchen Angriffen nicht nur einzelne Systeme bereinigt werden müssen. Sämtliche Software-Stände, Update-Pipelines und Vertrauensketten sind neu zu bewerten [185], [259]. Remote-Zugänge verstärken diese Risiken besonders bei zentralen Update- und Management-Infrastrukturen. In Europa gehen je nach Branche 20 bis 40 Prozent der Erstzugriffe auf missbrauchte Fernzugänge, VPN-Konten oder externe Wartungsschnittstellen zurück [48], [110], [342]. Besonders betroffen sind Umgebungen mit dauerhaft aktiven Wartungskonten und fehlender MFA.

Vertrauensmissbrauch über Integrationspartner

Integrationspartner wie Systemhäuser, Software-Integratoren oder Anbieter spezialisierter Fachanwendungen verfügen in vielen Organisationen über dauerhaft eingerichtete Schnittstellen, Service-Accounts und API-Zugänge mit direkter Anbindung an produktive Systeme. Angreifer nutzen dieses implizite Vertrauen gezielt aus, um über bestehende Integrationen in Zielumgebungen einzudringen, ohne klassische Perimeter- oder Zugangssicherungen überwinden zu müssen [138], [246], [259], [342].

Ein dokumentiertes Beispiel ist eine mehrjährige staatlich gesteuerte APT-Kampagne, bei der ein externer Marketing- und Kommunikationsdienstleister wiederholt kompromittiert wurde, um indirekten Zugriff auf angeschlossene Zielorganisationen zu erlangen [162]. Die Angreifer nutzten die bestehende Drittanbieterbeziehung, um personalisierte Phishing-Kampagnen, präparierte Webinhalte und die missbräuchliche Nutzung legitimer Integrationspfade zu kombinieren. Dadurch konnten sie persistente Zugriffe aufbauen, mehrere Angriffskanäle parallel offenhalten und ihre Aktivitäten an Abwehrmaßnahmen anpassen [162].

Ein zentrales Risiko liegt in der technischen Ausgestaltung solcher Integrationen. Service-Konten und API-Tokens besitzen häufig weitreichende Berechtigungen, sind dauerhaft aktiv und unterliegen nur eingeschränkter Überwachung [246], [342]. In Cloud-Umgebungen entfällt ein erheblicher Anteil erfolgreicher Angriffe auf kompromittierte maschinelle Identitäten. Diese umgehen reguläre Benutzerkontrollen und sind operativ kaum von legitimen Zugriffen zu unterscheiden [139], [246], [342].

Die Auswirkungen solcher Vorfälle sind besonders gravierend. Angriffe mit Integrations- oder API-Bezug führen im Median zu längeren Erkennungs- und Wiederherstellungszeiten. Zudem steigt die Wahrscheinlichkeit von Folgeangriffen, da technische Abhängigkeiten, Berechtigungen und Datenflüsse organisationsübergreifend analysiert und bereinigt werden müssen [185], [259], [313].

Mit dem weiteren Ausbau von Plattformökosystemen und API-basierter Integration ist bis 2030 von einer zusätzlichen Verschärfung dieses Risikos auszugehen [138], [259], [328], [342].

1.5. VERTEIDIGUNGS-HERAUSFORDERUNGEN UND STRUKTURELLE LÜCKEN

Trotz steigender Investitionen und wachsender Aufmerksamkeit bleibt die Abwehrfähigkeit vieler Organisationen hinter der Bedrohungsentwicklung zurück. Die Ursachen liegen dabei in strukturellen Defiziten bei Umsetzung, Integration und Steuerung. Verteidigungsmechanismen in vielen Organisationen sind weiterhin stark auf isolierte Schwachstellen ausgerichtet. Angriffe hingegen zielen zunehmend auf dauerhaft wirksame und gut verankerte Angriffsflächen [139], [246], [342].

Erfolgreiche Angriffe entfalten ihre Wirkung insbesondere dort, wo Steuerungs-, Priorisierungs- und Transparenzmechanismen nicht mit der Dynamik moderner Angriffe Schritt halten [139], [185], [233].

Diese strukturellen Lücken betreffen nahezu alle Sektoren. Unternehmen, Verwaltungen und Betreiber kritischer Infrastrukturen berichten übereinstimmend von Defiziten in der Governance, unzureichend abgesicherten Identitäten, Fachkräftemangel sowie einer wachsenden Diskrepanz zwischen technischer Komplexität und organisatorischer Reife [27], [48], [246], [337].

Für die kommenden Jahre wird eine weitere Zuspitzung dieses Missverhältnisses erwartet. Angriffe erfolgen schneller, automatisierter und stärker plattform- und identitätsgetrieben, als defensive Anpassungen typischerweise umgesetzt werden können [138], [259], [342], [345].

1.5.1 Technische Angriffsoberflächen und Schwachstellen

Auf technischer Ebene manifestieren sich die Defizite insbesondere im Umgang mit Schwachstellen, Fehlkonfigurationen und unzureichender Transparenz in komplexen IT- und Cloud-Umgebungen [139], [233], [246], [342]. Dies wird zusätzlich durch KI-gestützte Softwareentwicklung verstärkt. Ein erheblicher Anteil KI-generierten Codes enthält sicherheitsrelevante Schwachstellen, die sich durch Wiederverwendung und Automatisierung vervielfältigen können [336].

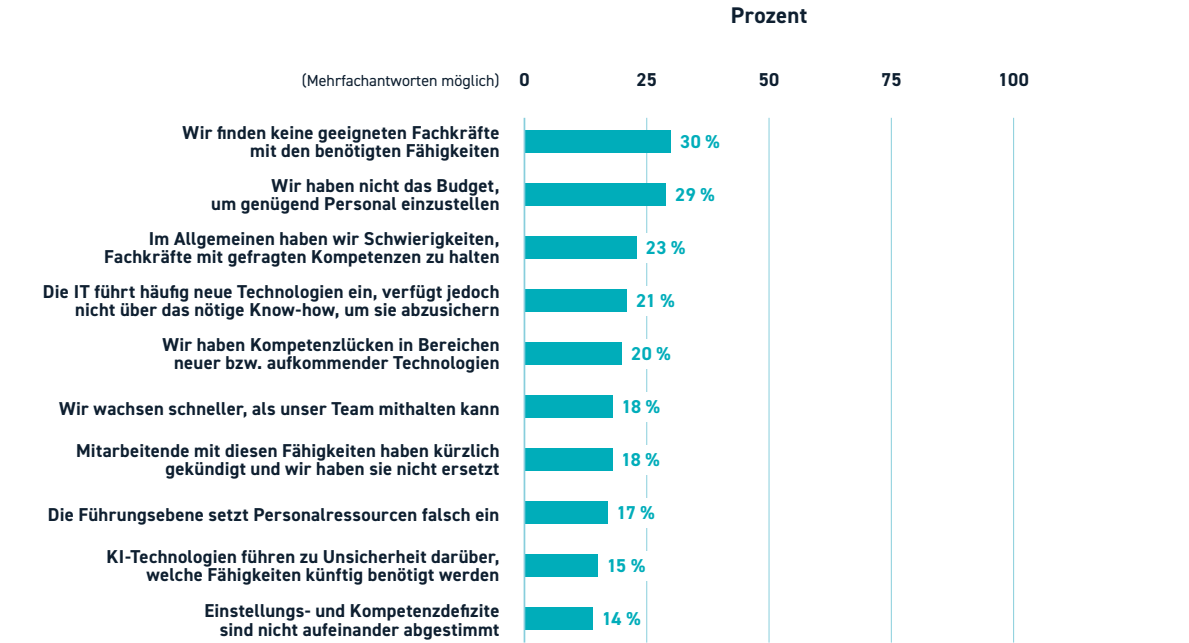
Gleichzeitig basieren 60 bis 80 Prozent erfolgreicher Angriffe auf bekannten Schwachstellen oder Fehlkonfigurationen, für die bereits Gegenmaßnahmen verfügbar waren [48], [139], [342]. Der zentrale Engpass liegt damit in der Priorisierung und zeitnaher Umsetzung unter realen Betriebsbedingungen [73], [139], [185].

Schwachstellenmanagement und Priorisierungslücken

Schwachstellenmanagement scheitert in der Praxis häufig an begrenzter Behandlungskapazität. Organisationen können einen erheblichen Teil der als kritisch eingestuften Schwachstellen nicht innerhalb empfohlener Zeitfenster schließen [139], [342]. Es besteht jedoch kein Erkennungs-, sondern ein Umsetzungsproblem [139], [185]. Für die Behebung kritischer Schwachstellen auf geschäftskritischen Systemen werden häufig mehrere Wochen benötigt, Patch-Zyklen von über 30 Tagen sind keine Ausnahme [111].

Ein Großteil der Organisationen bewertet eine Reduktion von Cybersecurity-Personal als Faktor für eine erhöhte Wahrscheinlichkeit erfolgreicher Angriffe. Diese Einschätzung korrespondiert mit Personalengpässen: 33 Prozent der Organisationen verfügen nicht über ausreichendes Budget zur angemessenen Besetzung ihrer Cybersicherheitsteams [200]. 29 Prozent geben an, sich qualifizierte Fachkräfte nicht leisten zu können (diese und weitere Gründe für Kompetenzbedarf siehe Abbildung 6).

Gleichzeitig berichten 36 Prozent der Organisationen von Budgetkürzungen in ihren Cybersicherheitsabteilungen und 24 Prozent bauten Cybersecurity-Personal ab [200]. Besonders ausgeprägt sind diese Ressourcen- und Strukturmängel in Cloud- und Drittanbieterumgebungen. Dort sind Verantwortlichkeiten fragmentiert, und Patch-Zyklen hängen voneinander ab [246], [342]. Schwachstellenmanagement entwickelt sich in diesem



Quelle: [200]

Abbildung 6: Hauptursachen für Kompetenzbedarf in Cybersecurity-Teams

Kontext von einer operativen zu einer koordinativen Steuerungsaufgabe, bei der Zuständigkeiten, Abhängigkeiten und Eskalationsmechanismen klar geregelt sein müssen.

Hinzu kommt eine systematische Fehlgewichtung in der Priorisierung. Schwachstellen werden häufig nach formalen Schweregraden bewertet, während reale Erreichbarkeit und tatsächliche Ausnutzbarkeit unzureichend berücksichtigt werden [139], [233], [342]. Da sich Angriffe empirisch auf einen kleinen Teil tatsächlich ausnutzbarer Schwachstellen konzentrieren, verstärkt fehlende risikobasierte Priorisierung insbesondere die Wirksamkeit automatisierter Angriffe [139], [185].

Fehlkonfigurationen und Default-Zugangsdaten

Fehlkonfigurationen stellen einen eigenständigen, häufig unterschätzten Risikotreiber dar. Unsichere Voreinstellungen, überprivilegierte Konten oder falsch konfigurierte Cloud- und Netzwerkrisiken sind in 20 bis 30 Prozent der dokumentierten Sicherheitsvorfälle ein wesentlich beitragender Faktor [139], [246], [342]. Anders als klassische Softwarelücken entstehen diese Risiken primär durch operative Entscheidungen, unzureichende Umsetzung von Standards und inkonsistente Konfigurationsänderungen [337], [342].

Besonders relevant sind Zugriffs- und Identitätskonfigurationen. Ein erheblicher Anteil erfolgreicher Cloud-Vorfälle geht auf überprivilegierte Konten, öffentlich

erreichbare Administrationsoberflächen oder unzureichend gesicherte API- und Storage-Ressourcen zurück [139], [246], [342]. In diesen Fällen erhöhen Fehlkonfigurationen die Reichweite und Wirkung kompromittierter Zugänge und verstärken identitätsbasierte Angriffe. Default-Zugangsdaten und schwache Authentifizierungspraktiken tragen weiterhin zu einem Anteil von 20 bis 32 Prozent erfolgreicher Erstzugriffe bei, insbesondere in Netzwerk-, Administrations- und OT-Umgebungen [48], [110], [342]. Fehlkonfigurationsbedingte Vorfälle führen im Median zu längeren Erkennungszeiten und höheren Wiederherstellungskosten als Angriffe über klar identifizierbare Softwarelücken [185], [313].

Sichtbarkeits- und Transparenzdefizite

Unzureichende Sichtbarkeit verstärkt sowohl Schwachstellen- als auch Fehlkonfigurationsrisiken, da sie die Priorisierung erschwert und Reaktionszeiten verlängert [185], [342]. International verfügen 25 bis 40 Prozent der Organisationen über keine vollständige Übersicht ihrer produktiven IT-Assets, Cloud-Ressourcen oder extern erreichbaren Dienste [27], [246], [337]. Eine belastbare risikobasierte Steuerung technischer Sicherheitsmaßnahmen fehlt dadurch häufig.

Besonders ausgeprägt sind Transparenzdefizite in Cloud- und Plattformumgebungen mit dynamischen und kurzlebigen Ressourcen. Deren Zustand verändert sich schneller, als bestehende Erfassungs- und Kontrollmechanismen ihn abbilden können [246], [342].

1.5.2 Digitale Identitäten – Ein unterschätztes Risiko

Digitale Identitäten sind heute einer der wichtigsten und gleichzeitig am schwersten kontrollierbaren Angriffspunkte moderner IT-Landschaften [138], [342], [345]. In vielen Organisationen bilden sie die zentrale Steuerungs- und Zugriffsebene, ohne dass Schutz-, Kontroll- und Notfallmechanismen im gleichen Maße mitgewachsen sind [65], [139], [342]. Identitätsbasierte Risiken lassen sich nur schwer isolieren, da sie zugleich organisatorische, technische und externe Abhängigkeiten betreffen.

40 bis 60 Prozent der untersuchten Sicherheitsvorfälle sind ganz oder teilweise auf den Missbrauch gültiger Zugangsdaten zurückzuführen [139], [246], [342].

Cloud-Nutzung, föderierte Authentifizierungsmodelle und externe Dienstleister verstärken diese Entwicklung zusätzlich. Identitäten sind zunehmend system- und organisationsübergreifend gültig, sodass einzelne Kompromittierungen eine hohe Reichweite entfalten [246], [342].

Identitätsdiebstahl als Zugangsmittel für jede Angriffsstufe

Identitäten ergänzen und verdrängen klassische Exploits zunehmend als zentrales Angriffsinstrument. Sie dienen nicht nur dem Erstzugang, sondern werden über mehrere Angriffsstufen hinweg genutzt. In mehr als der Hälfte der Ransomware- und Datendiebstahlvorfälle kommen kompromittierte Identitäten für laterale Bewegungen, Rechteausweitung und Persistenz zum Einsatz [233], [313], [342].

Diese Mehrfachverwendung erhöht Effizienz und Reichweite der Angriffe. Identitätsbasierte Vorfälle sind im Median mit längeren Verweildauern und höheren Wiederherstellungskosten verbunden als technisch exploitbasierte Angriffe [185], [313]. In stark cloud- und plattformzentrierten Umgebungen fungieren Identitäten zunehmend als durchgängiges Bindeglied entlang der gesamten Angriffskette [138], [246], [342], [345].

Abhängigkeit von wenigen Anmeldediensten

Die zunehmende Konzentration von Authentifizierung auf wenige zentrale Anmeldedienste stellt ein wachsendes systemisches Risiko dar. Viele Organisationen steuern geschäftskritische Prozesse – von Kommunikation

über Kollaboration bis hin zu Administration – über eine kleine Zahl zentraler Identitätsplattformen [139], [246], [342]. Die Kompromittierung einzelner Identitätsdienste oder privilegierter Rollen wirkt dadurch organisationsweit und dienstübergreifend [246], [342].

Entsprechend verursachen Vorfälle in stark zentralisierten Identitätsumgebungen im Median höhere Wiederherstellungskosten und längere Betriebsunterbrechungen [185], [313]. Besonders betroffen sind globale Admin-Rollen, Service-Accounts und unzureichend kontrollierte Drittzugänge [246], [337], [342]. Zusätzlich wird von einem Anstieg zerstörerischer Kampagnen um bis zu 87 Prozent berichtet, bei denen produktive Workloads und Datenbestände gezielt gelöscht oder manipuliert werden [246].

Plattformkonsolidierung, Single Sign-on und föderierte Identitätsmodelle verstärken diese Abhängigkeit weiter. Ohne zusätzliche Absicherung privilegierter Zugänge sowie klare Trenn- und Notfallkonzepte bleibt die Konzentration auf wenige Anmeldedienste ein zentraler Risikofaktor moderner IT-Landschaften [138], [259], [342], [345].

1.5.3 KI als struktureller Beschleuniger

In der Gesamtschau wirkt KI weniger als klarer Vorteil für eine Seite, sondern als Verstärker bestehender struktureller Ungleichgewichte [138], [246], [342]. 94 Prozent der Organisationen sehen KI als einen der dominierenden Treiber der Cybersicherheitslage, wobei bereits 77 Prozent KI zur Unterstützung von Sicherheitsfunktionen einsetzen. Gleichzeitig werden KI-Werkzeuge jedoch nur von 40 Prozent regelmäßig vor dem Einsatz überprüft, während 29 Prozent keinerlei Sicherheitsprüfungen durchführen [346].

Chancen und Risiken durch offene Modelle

Besondere Bedeutung kommt dabei offenen KI-Modellen zu, da sie flexibel, anpassbar und unabhängig von einzelnen Plattformanbietern einsetzbar sind. Daraus ergeben sich Chancen für Innovationsgeschwindigkeit, Transparenz und technologische Souveränität – auch im Sicherheitskontext [138], [259], [342], [345]. Gleichzeitig erhöhen offene Modelle die Zugänglichkeit leistungsfähiger KI für Angreifer, da sie ohne zentrale Nutzungskontrollen angepasst und missbraucht werden können [138], [139], [335]. Zusätzliche Risiken entstehen durch unzureichend abgesicherte KI-Infrastrukturen. Selbst betriebene Modelle, Vektor-Datenbanken und

Inferenzdienste, die sich im Betrieb befinden, eröffnen neue Angriffsflächen, etwa durch offene Schnittstellen, manipulierte Trainingsdaten oder unzureichend kontrollierte Modell-Updates [259], [335].

Offene Modelle verstärken damit die Ambivalenz von KI im Sicherheitskontext. Sie fördern Unabhängigkeit und Innovationsfähigkeit, erhöhen jedoch zugleich die Anforderungen an Governance, Betriebssicherheit und Zugriffskontrolle [138], [259], [342], [345]. Der Einsatz von KI verstärkt bestehende strukturelle Schwächen in Steuerung, Verantwortung und Priorisierung. Insbesondere dort, wo Governance-Strukturen, Verantwortlichkeiten und Entscheidungsprozesse nicht mit der Reichweite moderner IT-, Cloud- und Plattformarchitekturen Schritt halten, fungiert KI als zusätzlicher Beschleuniger von Risiken [138], [259], [342], [345]. Damit verschiebt sich die zentrale Fragestellung von der reinen Wirksamkeit einzelner technischer Maßnahmen hin zur organisatorischen und regulatorischen Einbettung von Cybersicherheit.

1.6 GOVERNANCE, REGULIERUNG UND MANAGEMENT-VERANTWORTUNG

Die zuvor beschriebenen strukturellen Defizite verdeutlichen, dass Cybersicherheit zunehmend durch Fragen der Steuerung, Verantwortungszuordnung und Entscheidungsfähigkeit bestimmt wird. Der Erfolg vieler Cyberangriffe liegt nicht an der Technik, sondern ist die Folge unklarer Zuständigkeiten, fragmentierter Governance und fehlender strategischer Einbindung auf Managementebene [71], [75], [138], [185], [259], [330], [342].

Cybersicherheit als Führungs- und Steuerungsaufgabe

Organisationen mit klar verankerter Governance-Struktur und eindeutiger Managementverantwortung sind signifikant resilienter gegenüber Cyberfällen als Organisationen, in denen Cybersicherheit primär operativ oder technisch verortet ist [185], [259], [337]. Organisationen mit sichtbarer Unterstützung durch die Unternehmensleitung erreichen höhere Sicherheitsreifegrade und können Vorfälle schneller eindämmen. Außerdem weisen Organisationen mit etablierten Compliance- und Governance-Programmen eine geringere Wahrscheinlichkeit schwerer Datenpannen auf (von 78 auf 21 Prozent) [328]. Defizite zeigen sich insbesonde-

re dort, wo Cyberrisiken nicht systematisch in Risikomanagement, Geschäftsstrategie und formale Entscheidungsprozesse eingebunden sind. Priorisierung, Investitionssteuerung und Reaktionsfähigkeit bleiben dadurch eingeschränkt [27], [337], [342]. Fehlende Führungseinbindung wird als Risikofaktor identifiziert [199].

Obwohl Cybersicherheit als relevantes Risiko anerkannt wird, fehlen klar definierte Entscheidungs-, Eskalations- und Berichtslinien. Dies begünstigt reaktive Investitionen, inkonsistente Umsetzung und begrenzte Wirksamkeitskontrolle [27], [185], [337]. Organisationen mit regelmäßiger Berichterstattung zu Cyberrisiken auf Vorstands- oder Behördenleitungsebene weisen demgegenüber kürzere Reaktionszeiten und geringere Folgeschäden auf [185], [259], [313].

Haftbarkeit und Entscheidungsdruck

Vorstände, Geschäftsführungen und Behördenleitungen werden zunehmend für Sicherheitsversäumnisse verantwortlich gemacht, etwa im Rahmen von Aufsichtsverfahren, Haftungsfragen oder politischer Bewertung [27], [283], [337].

Gleichzeitig erfolgen Managemententscheidungen vielfach unter Unsicherheit, da Transparenz über Angriffsflächen, Abhängigkeiten und Wirksamkeit von Maßnahmen begrenzt ist [246], [337], [342]. Governance-Strukturen gewinnen hier an Bedeutung, da sie Entscheidungsfähigkeit auch unter unvollständiger Information ermöglichen sollen [185], [259].

Regulierung als Mindeststandard – nicht als Sicherheitsgarantie

Die Regulatorik in der Cybersicherheit hat sich in den letzten Jahren deutlich verdichtet. Nationale und europäische Rahmenwerke definieren zunehmend verbindliche Mindestanforderungen an Risikomanagement, Meldepflichten und Schutzmaßnahmen [48], [110], [123], [283].

Zwar implementieren stark regulierte Organisationen häufiger formale Sicherheitsprozesse. Erfolgreiche Angriffe treten jedoch auch in diesen Sektoren auf, etwa bei KRITIS-Betreibern, der öffentlichen Verwaltung oder im Finanzsektor [48], [110], [185].

Ursache ist häufig, dass regulatorische Anforderungen formal erfüllt, aber nicht in operative Steuerung übersetzt werden [259], [337]. Beispielsweise werden bei der Umsetzung von NIS-2-Anforderungen (Details zur Richtlinie finden sich im Addendum dieses Berichts) organisatorische und ressourcenbezogene Faktoren häufiger als rein technische Aspekte genannt [111]. Zudem bleibt Regulierung strukturell hinter der Bedrohungsentwicklung zurück. Während Angriffe zunehmend identitäts-, plattform- und lieferkettenbasiert erfolgen, orientieren sich viele Vorgaben weiterhin an klassischen System- und Perimetergrenzen [138], [259], [342].

Regulierung stellt damit eine notwendige, aber allein nicht ausreichende Grundlage wirksamer Cybersicherheitssteuerung dar [259], [342], [345].

### Organisationale Reife, Ressourcen und Umsetzungsrealität

Ein zentrales Governance-Problem liegt in der Diskrepanz zwischen Anforderungen und Umsetzungsfähigkeit [27], [283], [337]. 95 Prozent der Organisationen geben an, aktuell mindestens einen relevanten Skill-Bedarf nicht decken zu können. Bei 59 Prozent bestehen kritische oder signifikante Skill-Lücken. Besonders betroffen sind KI-Skills (41 Prozent), Cloud-Security-Kompetenzen (36 Prozent), Risikobewertung (29 Prozent), Applikationssicherheit (28 Prozent) und GRC-Kompetenzen (27 Prozent) [200].

Sicherheitsreife hängt weniger von der Anzahl eingesetzter Werkzeuge als von klaren Prozessen, Zuständigkeiten und Priorisierungsmechanismen ab [185], [259]. Organisationen mit höherer Reife verfügen über definierte Risikoakzeptanzen, regelmäßige Überprüfungen und geübte Entscheidungsprozesse für Krisensituationen [185], [313]. Fehlende Governance führt demgegenüber häufig zu reaktivem Handeln, verspäteter Kommunikation und ineffizienter Ressourcennutzung [27], [337].

### Von Compliance zu Resilienz

Mit Blick auf die kommenden Jahre zeichnet sich eine weitere Verschiebung von formaler Compliance hin zu operationaler Resilienz ab. Cybersicherheit wird zunehmend als Daueraufgabe verstanden, die kontinuierliche Anpassung, Übung und strategische Steuerung erfordert [138], [259], [342], [345].

Erfolgreiche Organisationen werden Cybersicherheit stärker als integralen Bestandteil von Unternehmens- und Verwaltungshandeln begreifen müssen – vergleichbar mit Finanz-, Personal- oder Produktionsrisiken [27], [185], [259].

Die Bewältigung der Cybersicherheitslage hängt von der Fähigkeit von Organisationen und Entscheidungsträgern ab, Verantwortung zu übernehmen, Prioritäten transparent zu setzen und Cybersicherheitsrisiken als dauerhaftes Führungs- und Steuerungsthema einzuordnen [138], [185], [259], [342], [345].

Cybersicherheit ist keine technische Nebenaufgabe, sondern eine strukturelle Managementfrage. Ihre Wirksamkeit bemisst sich an Resilienz, Entscheidungsfähigkeit und organisatorischer Reife.

## 1.7 AUSBLICK 2026-2035

Die Sicherheitsarchitektur wird in den nächsten Jahren bestimmt durch das Zusammentreffen von systemischen Risiken durch Künstliche Intelligenz, der drohenden Entschlüsselung durch Quantencomputer und einer zunehmend vulnerablen physischen Infrastruktur bestimmt. Während der Klimawandel die Hardware-Basis gefährdet, verschieben autonome Systeme und digitale Zentralbankwährungen die Angriffsziele von reiner Datenspionage hin zu kinetischer Gewalt und staatlicher Destabilisierung [328], [347].

### KI als globales Risiko

Bis 2035 werden „nachteilige Folgen von KI“ einen der vorderen Plätze für globale Gefahren belegen, wobei systemische Schäden weit über einfachen Betrug hinausgehen [347]. KI wird immer stärker von Verteidigern und Angreifern eingesetzt werden. Autonome KI-Agenten werden immer komplexere, mehrstufige Angriffe mit minimaler menschlicher Aufsicht durchführen [336]. Diese Agenten können Entscheidungen treffen, Daten analysieren und Angriffsvektoren in Echtzeit anpassen [336]. Außerdem werden Deepfakes und Social Engineering noch überzeugender und schwerer zu erkennen sein [146]. Die Nutzung von KI-gestützten Tools und „Vibe Coding“ beschleunigt weiter die Softwareentwicklung, führt aber auch zu unsicherem Code, der neue Schwachstellen bedingt [336].

Während Cyberspionage und digitale Kriegsführung dauerhafte Top-Risiken bleiben, fungiert der Klimawandel zunehmend als Risiko-Multiplikator: Extremwetter bedrohen die physische IT-Infrastruktur (Rechenzentren, Seekabel) und erschweren deren Absicherung [347].

### Gefahren für die Verschlüsselung (Q-Day)

Der „Quantum-Day“ (Q-Day) markiert den Zeitpunkt (ca. 2030–2035), an dem Quantencomputer heutige Standard-Verschlüsselungen brechen können [328]. Da diese das Fundament der Internet-Sicherheit bilden, fordern Regierungen den Wechsel auf Post-Quantum-Kryptographie bis spätestens 2035; für kritische Systeme gilt bereits 2030 als Zielmarke [246]. Akut ist zudem die Strategie „Harvest Now, Decrypt Later“: Angreifer entwenden bereits heute verschlüsselte Daten, um sie künftig nachträglich zu dechiffrieren. Damit ist die Quanten-Sicherheit schon heute entscheidend für Daten, die langfristig geheim bleiben müssen [246], [328], [339].

### Expansion der Angriffsflächen durch technologische Transformation

Die technologische Transformation schafft bis 2030 kritische Gefahrenfelder, die bisher kaum im Fokus stehen. Ein Schwerpunkt liegt auf der Vulnerabilität physischer Infrastrukturen sowie der Schnittstelle zur Robotik: Cyberangriffe auf Satellitendienste oder Unterseekabel – ein Thema, das bereits im Schwarz Digits Cybersecurity Report 2025 vertieft wurde – bleiben eine zentrale Bedrohung für die globale Wirtschaft [347].

In Kombination mit der Infiltration autonomer, humanoider Systeme können solche Angriffe künftig unmittelbar materielle Schäden oder physische Gewalt auslösen. Da diese Systeme in Millisekunden agieren, markieren sie den Übergang von digitaler Spionage hin zu kinetischen Bedrohungsszenarien und moderner Kriegsführung (siehe auch Kapitel 3 dieses Cybersecurity Reports) [347].

Parallel dazu entstehen neue systemische Risiken im Finanzsektor. Die Einführung digitaler Zentralbankwährungen schafft hochkomplexe Architekturen, die neue Angriffsflächen für die Destabilisierung ganzer Volkswirtschaften bieten [347].

Diese qualitativen neuen Gefahren treffen auf eine quantitativ explodierende IT-Landschaft, wie das Beispiel der deutschen Bundesländer zeigt: Bis 2035 wird sich die Zahl der IT-Services auf voraussichtlich 400.000 vervierfachen. Auch veraltete Systeme und ein „Patch-Rückstand“ stellen massive Risiken dar. Angesichts einer drohenden Verzehnfachung kritischer Schwachstellen wird eine automatisierte Abwehr in diesen hochdynamischen Umgebungen künftig alternativlos, um die staatliche Handlungsfähigkeit zu sichern [10].



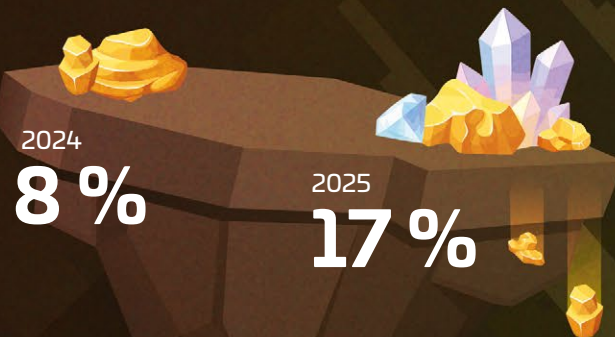
# KAPITEL 2



# WIRTSCHAFTSBAROMETER DEUTSCHLAND

## CYBERSICHERHEIT UND DIGITALE SOUVERÄNITÄT

Anteil für IT-Sicherheit am IT-Gesamtbudget



Hohe Akzeptanz für offensive Gegenmaßnahmen

**79 %**

der befragten Unternehmen befürworten staatliche „Hackbacks“ gegen ausländische Angreifer

Unzureichende Risiko-Prävention

Nur **36 %** der Unternehmen führen Penetrationstests durch

Sind Regeln für den Umgang mit generativer KI vorhanden?

in **26 %** aller Unternehmen

in **73 %** der großen Unternehmen

Nur jedes **8. Unternehmen**

plant Investitionen in die Verringerung von Abhängigkeiten (13 %)



CISO etabliert?

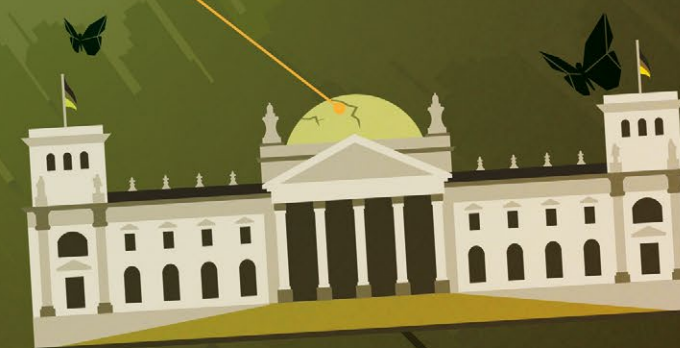
NEIN **57 %**

Ja: nur 43 %

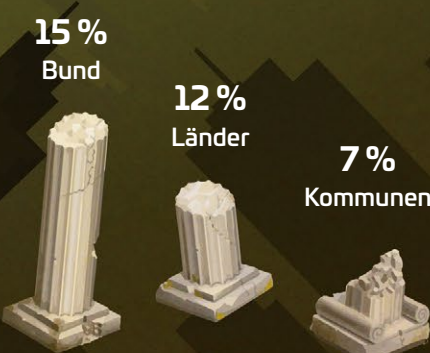
Risikofaktor Lieferkette



**67 %** fühlen sich vom Staat **nicht** ausreichend beim Schutz vor Cyberangriffen unterstützt



Gut aufgestellt gegen Cyberbedrohungen?



Machen Europäische Datenräume die EU digital souverän?

JA: **50 %**

**59 %** Zustimmung in der Finanzbranche  
European Financial Data Space

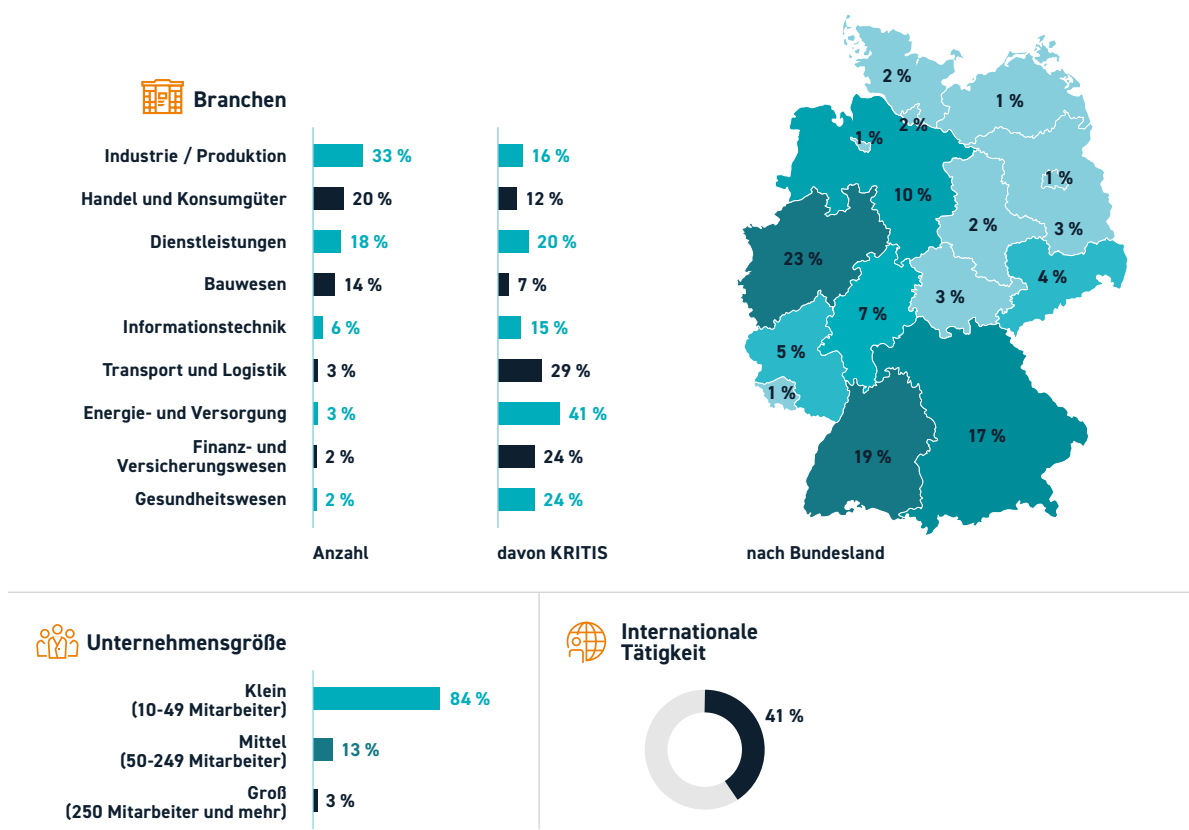
**68 %** Zustimmung im Gesundheitswesen  
European Health Data Space



## 2 WIRTSCHAFTSBAROMETER DEUTSCHLAND – CYBERSICHERHEIT UND DIGITALE SOUVERÄNITÄT

Die deutsche Wirtschaft agiert heute in einem Spannungsfeld, das von einer dynamischen Bedrohungslage sowie einem stetig steigenden regulatorischen Druck geprägt ist. Gleichzeitig wächst das Bedürfnis nach digitaler Souveränität, um technologische Abhängigkeiten in globalen Lieferketten nachhaltig zu reduzieren und digitale Resilienz aufzubauen. In diesem Umfeld ist Cybersicherheit nicht länger nur eine operative IT-Aufgabe, sondern eine strategische Kernvoraussetzung, die über die unternehmerische Handlungsfähigkeit und den dauerhaften Markterfolg deutscher Unternehmen entscheidet.

Der vorliegende Bericht nimmt gezielt die Perspektive der Unternehmen in Deutschland in den Blick, um eine verlässliche Datenbasis zur tatsächlichen Widerstandsfähigkeit der Wirtschaft im Jahr 2026 zu schaffen.



Mögliche Abweichungen in den Summen sind rundungsbedingt.  
Dies gilt für alle Zahlen im Text und in den Abbildungen in diesem Kapitel.

Quelle: Eigene Erhebung

Abbildung 7: Übersicht der Stichprobe nach Branchen, Bundesländern, Unternehmensgröße und Internationalität (in %)

|                               | (C)ISO |                   |                   |
|-------------------------------|--------|-------------------|-------------------|
|                               | Gesamt | Ja                | Nein              |
| N                             | 1001   | 466               | 535               |
| Sehr gut vorbereitet          | 17 %   | 22 % <sup>1</sup> | 14 %              |
| Gut vorbereitet               | 48 %   | 51 %              | 46 %              |
| Durchschnittlich vorbereitet  | 28 %   | 22 %              | 31 % <sup>1</sup> |
| Nicht ausreichend vorbereitet | 4 %    | 3 %               | 6 % <sup>1</sup>  |
| Keine Angabe                  | 3 %    | 2 %               | 4 %               |

<sup>1</sup> Die Ergebnisse sind statistisch signifikant bei einem Signifikanzniveau von  $\alpha = 0,01$

Quelle: Eigene Erhebung

Tabelle 1: Zusammenhang (C)ISO und Selbsteinschätzung zur Vorbereitung auf Bedrohungen

2.1 STUDIENDESIGN

Die vorliegende Studie basiert auf einer repräsentativen Befragung zur Cybersicherheit und digitalen Souveränität in Deutschland, die im vierten Quartal 2025 durchgeführt wurde.

Die Befragung umfasst sowohl strategische als auch organisatorische und operative Aspekte der Cybersicherheit. Sie zeigt auf, wie Unternehmen sich ausrichten, welche Strukturen und Verantwortlichkeiten etabliert sind und wie mit aktuellen Rahmenbedingungen umgegangen wird. Die vorliegende Untersuchung setzt dabei die Befragung aus dem vierten Quartal 2024 [299] fort und kontrastiert die aktuellen Ergebnisse an ausgewählten Stellen mit den entsprechenden Vorjahreswerten.

Die Datenerhebung erfolgte mittels computergestützter telefonischer Interviews (CATI) mit 1.001 Unternehmen am Standort Deutschland. Befragt wurden Experten in verantwortlichen IT-Funktionen, die über Einblicke in die Sicherheitsstrukturen ihrer Organisation verfügen. Durch eine repräsentative Gewichtung bietet die Stichprobe ein belastbares Abbild der deutschen Unternehmenslandschaft (siehe Abbildung 7).

2.2 BEDROHUNGSWAHRNEHMUNG

Die Wahrnehmung von Cyberbedrohungen und der eigenen Verwundbarkeit prägt maßgeblich, wie Unternehmen ihre Cybersicherheitsstrategien ausrichten und priorisieren. Einschätzungen zur eigenen Vorbereitung, zur realen Schadensdimension sowie zu neuen technologischen Risiken geben Aufschluss darüber, wie ernst Cybersecurity als unternehmerisches Risiko genommen wird und wo mögliche Diskrepanzen zwischen Selbstbild und Gefährdung bestehen.

Größere Unternehmen fühlen sich besser auf Cybersicherheitsbedrohungen vorbereitet

Die Mehrheit der befragten Unternehmen in Deutschland schätzt ihre Vorbereitung auf Cybersicherheitsbedrohungen als gut bis sehr gut ein. Insgesamt geben 65 Prozent der Befragten an, (sehr) gut vorbereitet zu sein. Dieses Bild zeigt sich über alle Unternehmensgrößen hinweg, unterscheidet sich jedoch in der Intensität der Einschätzung. Große Unternehmen bewerten ihren Vorbereitungsgrad signifikant häufiger als sehr gut als kleine und mittlere Unternehmen: Während sich 28 Prozent der großen Unternehmen sehr gut vorbereitet sehen, liegt dieser Anteil bei kleinen Unternehmen bei 16 Prozent und bei mittleren bei 18 Prozent.

Ein weiterer Unterschied zeigt sich in Abhängigkeit von der Organisationsstruktur: Unternehmen mit einer dedizierten (Chief) Information Security Officer ((C)ISO)-Funktion schätzen sich signifikant häufiger als sehr gut vorbereitet ein, als Unternehmen ohne solche Rolle (siehe Tabelle 1).

Über die Zeit hinweg erweist sich diese Selbsteinschätzung stabil. Auch im Jahr 2024 [299] gaben im Durchschnitt 66 Prozent der Unternehmen an, gut bis sehr gut auf Cyberbedrohungen vorbereitet zu sein.

Im Vergleich zu anderen deutschen Studien [337], in der sich 91 Prozent der Unternehmen als gut geschützt einschätzen, fällt die Selbsteinschätzung in der vorliegenden Befragung moderater aus. Gleichzeitig besteht weiterhin ein Kontrast zwischen der wahrgenommenen Vorbereitung und der steigenden Zahl von Cyberangriffen.

Hinsichtlich interner Bedrohungen, wie etwa Datenabfluss durch Unachtsamkeit oder bewusste Innentäter, stufen 56 Prozent der Unternehmen ihre Absicherung als mindestens gut ein, wobei große Unternehmen ihre Resilienz mit 26 Prozent besonders häufig als sehr gut bewerten. Dies steht im Kontext globaler Studien, wonach 77 Prozent der Organisationen in den letzten 18 Monaten mindestens einen datenschutzrelevanten Vorfall durch Insider verzeichneten [147].

20 Prozent der Unternehmen wurden bereits Opfer eines Cyberangriffs

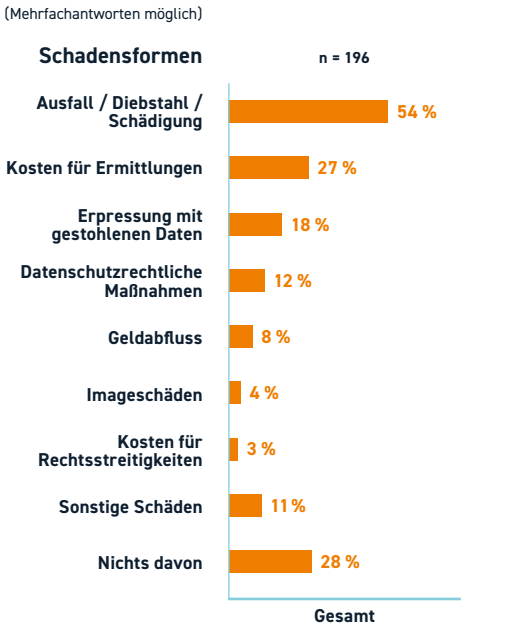
Nur wenige Unternehmen berichten von eigenen Angriffserfahrungen. Insgesamt geben 20 Prozent an, bereits Opfer eines Cyberangriffs gewesen zu sein, während 80 Prozent dies vereinen. Große Unternehmen sind deutlich häufiger betroffen: Hier berichten 33 Prozent von grundsätzlich mindestens einem Angriff, während 64 Prozent keinen Vorfall angeben. Ein Vergleich mit Ergebnissen aus der Datenklostudie 2025 [134] zeigt, dass der dort ausgewiesene Anteil betroffener Unternehmen (33 Prozent) dem Niveau entspricht, das in der vorliegenden Befragung bei großen Unternehmen beobachtet wurde. Dies ist vor dem Hintergrund der Stichprobenzusammensetzung zu sehen: In der Datenklostudie 2025 entfallen rund zwei Drittel der Befragten auf Unternehmen mit einem Jahresumsatz von mindestens 25 Millionen Euro. Entsprechend spiegelt der dort ausgewiesene Betroffenheitsanteil vor allem die Situation größerer Unternehmen wider [134].

Bei der zeitlichen Einordnung der Cyberangriffe unter betroffenen Unternehmen zeigen sich signifikante Unterschiede nach Unternehmensgröße. Große Unternehmen berichten deutlich häufiger von jüngeren Vorfällen: 41 Prozent geben an, in den Jahren 2023 oder 2024 Opfer eines Cyberangriffs gewesen zu sein. Kleine und mittlere Unternehmen verorten Angriffe hingegen signifikant häufiger in der weiter zurückliegenden Vergan-

genheit und nennen überwiegend das Jahr 2022 oder früher (jeweils 65 Prozent). Nur insgesamt 20 Prozent der Befragten geben an, im Jahr 2025 Opfer geworden zu sein.

Ausfall, Diebstahl, Schädigung als häufigste Schadensformen

Die Folgen von Cyberangriffen äußern sich in unterschiedlichen Schadensformen (siehe Abbildung 8). Am häufigsten werden Ausfälle, Diebstahl und Schädigungen genannt. Zudem berichten 27 Prozent der betroffenen Unternehmen von Kosten für Ermittlungen. Diese fallen deutlich häufiger bei Unternehmen ohne (C)ISO an als bei Unternehmen mit einer entsprechenden Funktion. Bei großen Unternehmen treten darüber hinaus Imageschäden wesentlich häufiger auf, hier geben 21 Prozent entsprechende Reputationsverluste an. Branchenbezogen zeigen sich ebenfalls Unterschiede. In der Finanz- und Versicherungsbranche sowie im Gesundheitswesen wird wesentlich häufiger von Erpressung mit gestohlenen Daten berichtet als in anderen Branchen.



Quelle: Eigene Erhebung

Abbildung 8: Folgen von Cyberangriffen



202 Milliarden Euro Schaden durch Cyberangriffe: Ein realistisches Szenario für drei Viertel der Unternehmen

Vor diesem Hintergrund wurden die Unternehmen gefragt, wie realistisch sie die von der Wirtschaftsschutzstudie 2025 von Bitkom [27] ausgewiesenen wirtschaftlichen Schäden durch Cyberangriffe in Deutschland in Höhe von 202 Milliarden Euro einschätzen. Drei Viertel der Befragten halten diese Angabe für realistisch. Im Durchschnitt stimmen 76 Prozent dieser Größenordnung zu, während 11 Prozent sie für nicht realistisch halten. Kleine und mittlere Unternehmen geben dabei signifikant häufiger an, keine Einschätzung abgeben zu können oder zu wollen. Große Unternehmen bewerten die Schadenssumme deutlich häufiger als realistisch (86 Prozent). Unter den Unternehmen, die die Angabe der Bitkom-Studie als nicht realistisch bewerten, überwiegt die Einschätzung, dass die tatsächlichen Schäden eher zu niedrig angesetzt sind.

KI erst teilweise im Fokus der Risikowahrnehmung trotz neuer Angriffsvektoren

Neben klassischen Angriffsszenarien rückt der Einsatz von Künstlicher Intelligenz (KI) zunehmend in den Fokus der Risikowahrnehmung. Dennoch stuft mehr als die Hälfte der Unternehmen das Cybersicherheitsrisiko durch die Nutzung von KI als nicht oder überhaupt nicht vorhanden ein (54 Prozent). Bei kleinen Unternehmen liegt dieser Anteil bei 55 Prozent, bei großen Unternehmen noch bei 32 Prozent. Mittlere und große Unternehmen bewerten das Risiko deutlich häufiger als sehr hoch (siehe Abbildung 9).

Als zentrale neue Angriffsvektoren im Zusammenhang mit dem Einsatz von KI und Large Language Models (LLM) nennen die Unternehmen vor allem Schatten-KI und unkontrollierten Datenabfluss durch Mitarbeitende (38 Prozent). Weitere Risiken sehen sie in der KI-gestützten Perfektionierung von Social-Media-Angriffen (24 Prozent) sowie in Angriffen auf KI-Systeme und deren Ergebnisse, etwa durch Prompt Injection (11 Prozent). Unternehmen der kritischen Infrastruktur (KRITIS) weisen wesentlich häufiger (48 Prozent) auf das Gefahrenpotenzial von Schatten-KI und unkontrolliertem Datenabfluss hin als andere Unternehmen. In der Finanz- und Versicherungsbranche wird wiederum signifikant häufiger als in anderen Branchen das Risiko durch Social Engineering hervorgehoben.

2.3 IT-SECURITY-BUDGETS

Mit zunehmender Unternehmensgröße steigen sowohl die gesamten IT-Budgets als auch die Anteile für IT-Security. Gleichzeitig arbeitet ein Großteil der befragten Unternehmen mit vergleichsweise begrenzten IT-Budgets. Insgesamt verfügen 70 Prozent über ein jährliches IT-Budget von unter 100.000 Euro. Bei mittleren Unternehmen liegt dieser Anteil noch bei 50 Prozent, erst bei großen Unternehmen verschiebt sich das Bild deutlich: Hier geben 27 Prozent an, über ein IT-Budget von mindestens einer Million Euro zu verfügen. KRITIS-Unternehmen heben sich ebenfalls ab. Bei rund 60 Prozent von ihnen übersteigt das IT-Budget 100.000 Euro.

Anteil für IT-Sicherheit im IT-Budget von 2024 auf 2025 stark gestiegen

Der Anteil des IT-Budgets, der für IT-Security aufgewendet wird, liegt im Durchschnitt bei 17 Prozent und variiert nach Unternehmensgröße. Während kleine Unternehmen im Mittel ebenfalls rund 17 Prozent einsetzen, steigt der Anteil bei großen Unternehmen auf bis zu 22 Prozent. Im Zeitverlauf zeigt sich dabei eine deutliche Verschiebung: Zwar ist das IT-Budget insgesamt gestiegen, zugleich hat sich die anteilige Mittelverfügbarkeit für IT-Security von acht Prozent im Jahr 2024 auf 17 Prozent im Jahr 2025 mehr als verdoppelt.

Damit liegt der ausgewiesene Anteil auf einem ähnlichen Niveau wie in der Bitkom-Studie [27], die für Unternehmen mit einem Jahresumsatz von mindestens einer Million Euro einen durchschnittlichen IT-Security-Anteil von 18 Prozent ausweist. Vor dem Hintergrund der breiteren Unternehmensbasis der vorliegenden Befragung erscheint das Ergebnis konsistent.

Ein Blick auf die absoluten Cybersicherheitsbudgets der vorliegenden Befragung – ohne Personalkosten, aber inklusive Technologie und externer Dienstleister – verdeutlicht die Unterschiede zwischen den Unternehmensgrößen. Insgesamt liegen 85 Prozent der Unternehmen mit ihrem jährlichen Cybersicherheitsbudget unter 100.000 Euro. Bei großen Unternehmen reduziert sich dieser Anteil deutlich auf 41 Prozent.

Ein Vergleich mit internationalen Daten der Agentur der Europäischen Union für Cybersicherheit (European Network and Information Security Agency (ENISA)) ordnet diese Ergebnisse ein: In der EU-weiten Erhebung, die alle 27 Mitgliedstaaten und sämtliche NIS-2-Sektoren umfasst, entfallen im Median rund neun Prozent der IT-Budgets auf Cybersicherheit. Das mittlere Investitionsvolumen liegt dabei bei etwa 1,5 Millionen Euro [111].

Cybersicherheitsbudgets steigen – in Deutschland und international

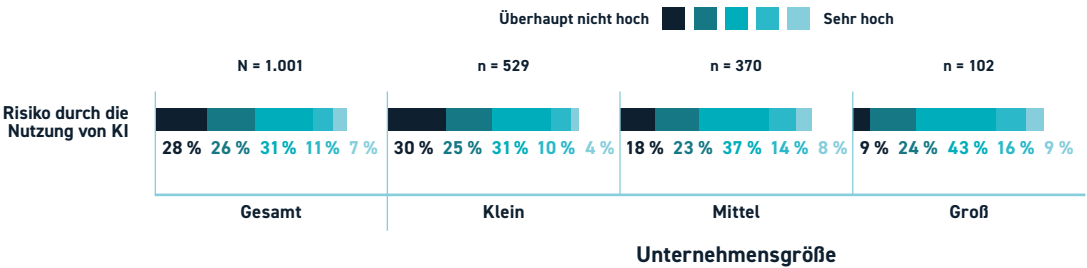
In den vergangenen zwölf Monaten haben 36 Prozent der Unternehmen ihr Cybersicherheitsbudget erhöht. Besonders ausgeprägt ist diese Entwicklung bei großen Unternehmen: Mehr als die Hälfte von ihnen (53 Prozent) gibt an, ihr Budget erhöht zu haben. Bei kleinen Unternehmen blieb das Budget hingegen überwiegend unverändert, hier berichten 65 Prozent, keine Anpassungen vorgenommen zu haben.

Im weltweiten Vergleich geben rund 50 Prozent der Unternehmen an, ihr Cybersicherheitsbudget erhöht zu haben, ein Drittel meldet unveränderte Budgets. Gleichzeitig zeigt sich im Zeitverlauf eine Abschwächung der Dynamik, denn in den Jahren vor 2025 wurden Budgeterhöhungen häufiger genannt. Der Anteil unveränderter oder reduzierter Budgets hat zugenommen, was auf eine aktuell zurückhaltende Budgetplanung im Bereich Cybersicherheit hindeutet [35]. Dieses Bild wird durch Daten der ENISA für den europäischen Raum bestätigt, welche für das aktuelle Jahr ein zum Vorjahr stabiles Investitionsniveau ausweisen [111].

Ein wesentlicher Faktor für Budgeterhöhungen ist die Reaktion auf die verschärfte Bedrohungslage, wobei vor allem die Zunahme von Phishing-Angriffen und Vorfällen im direkten Umfeld, wie gehackten Partnerfirmen oder Branchenkollegen, als Katalysatoren wirken. In Sektoren wie der Industrie wird Cybersicherheit durch die NIS-2-Richtlinie zum strategischen Schwerpunkt, während im Gesundheitswesen und im Energiesektor vor allem die persönliche Haftung der Geschäftsführung und die Vermeidung lebensbedrohlicher Systemausfälle durch Ransomware im Fokus stehen. Im Handel hingegen treiben oft mediale Sensibilisierung, der Schutz der Kundenreputation und unfreiwillige Kostensteigerungen bei Software-Lizenzen die Ausgaben nach oben, ergänzt durch notwendige Modernisierungszyklen und die Anforderungen von Cyberversicherungen.

Dem gegenüber stehen gezielte Budgetreduzierungen, die laut der befragten Unternehmen häufig auf den Wegfall von Einmalkosten nach abgeschlossenen Projekten oder auf Effizienzgewinne durch Cloud-Migrationen zurückzuführen sind. Dennoch gibt es kritische Sparmaßnahmen, die durch allgemeinen wirtschaftlichen Druck, Personalabbau oder eine gefährliche Fehleinschätzung des tatsächlichen Risikos begründet werden.

Diese Befunde decken sich mit dem breiteren europäischen Trend: Europaweit geben 70 Prozent der Unternehmen an, dass regulatorische Compliance-Anforderungen wie NIS-2, der Digital Operational Resilience Act (DORA) oder der Cyber Resilience Act (CRA) der primäre Grund für ihre Investitionen in Cybersicherheit sind [111]. Damit wird deutlich, dass die gesetzliche Rahmensezung der zentrale Impulsgeber für die finanzielle Priorisierung von Sicherheitsmaßnahmen im Jahr 2026 ist.



Quelle: Eigene Erhebung

Abbildung 9: Einschätzung Risiko durch KI-Nutzung steigt mit Unternehmensgröße

2.4 PERSONELLE IT-STRUKTUR UND COMPLIANCE-ROLLEN

Die personelle Verankerung von IT-Sicherheit und Compliance entscheidet maßgeblich darüber, ob Cyberresilienz als bloße regulatorische Pflichtaufgabe oder als gelebte Strategie verstanden wird. Die vorliegenden Daten offenbaren hierbei eine deutliche Diskrepanz zwischen der stabilen Besetzung rechtlich geforderter Datenschutzrollen und einer oft lückenhaften Institutionalisierung dedizierter Sicherheitsverantwortlicher wie des CISO.

Zahl der IT-Arbeitsplätze in Unternehmen steigt, IT-Sicherheit weiterhin nur mit einzelnen Stellen besetzt.

Knapp 69 Prozent der Unternehmen verfügen über maximal zehn IT-Arbeitsplätze, weitere 15 Prozent über bis zu 25. Erst bei großen Unternehmen zeigt sich eine deutlich andere Struktur: Hier geben 20 Prozent an, mehr als 100 IT-Arbeitsplätze zu besitzen. Besonders deutlich fällt der Unterschied bei Unternehmen der kritischen Infrastruktur aus: Sie verfügen signifikant häufiger über größere IT-Abteilungen. Rund 32 Prozent der KRITIS-Unternehmen beschäftigen 26 oder mehr IT-Mitarbeitende, gegenüber 14 Prozent bei nicht kritischen Unternehmen.

Im Jahresvergleich ist die Zahl der IT-Arbeitsplätze insgesamt gestiegen. Während im Jahr 2024 noch 91 Prozent der Unternehmen maximal zehn IT-Arbeitsplätze angaben, hat sich dieser Anteil reduziert. Zugleich ist der Anteil der Unternehmen mit mehr als zehn IT-Arbeitsplätzen gewachsen [299].

Deutlich geringer fällt die personelle Ausstattung im Bereich IT-Security aus. Nahezu alle Unternehmen (94 Prozent) verfügen über maximal zehn Arbeitsplätze, die sich ausschließlich oder überwiegend mit IT-Security befassen. Dieses Bild ist über die Zeit hinweg stabil: Bereits im Jahr 2024 gaben 97 Prozent der Unternehmen an, höchstens zehn entsprechende Stellen zu haben [299].

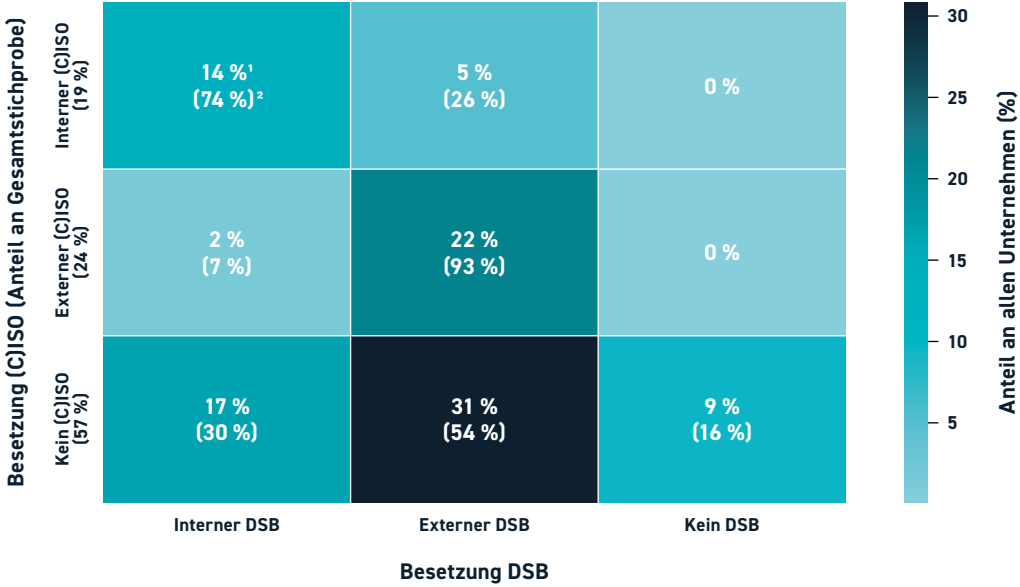
Datenschutzbeauftragte im Durchschnitt zu einem Drittel intern besetzt, häufiger in der IT- sowie Finanz- und Versicherungsbranche

Ein differenziertes Bild zeigt sich bei der formalen Besetzung von Compliance-Rollen, insbesondere beim Datenschutz. Mit insgesamt 91 Prozent verfügt die große Mehrheit der Unternehmen über eine entsprechende Beauftragtenfunktion. Dabei dominiert mit 58 Prozent das externe Modell, während rund ein Drittel (33 Prozent) auf interne Lösungen setzt. Lediglich neun Prozent der Unternehmen geben an, die Rolle derzeit nicht besetzt zu haben.

Diese Struktur ist maßgeblich durch die gesetzlichen Vorgaben des Bundesdatenschutzgesetzes geprägt: Gemäß § 38 Abs. 1 Satz 1 besteht eine Benennungspflicht, sobald in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Während große Unternehmen etwas häufiger interne Datenschutzbeauftragte (DSB) benennen und nur selten ganz auf diese Rolle verzichten, greifen kleine und mittlere Unternehmen überwiegend auf externe Lösungen zurück. Branchenbezogen zeigen sich jedoch deutliche Schwerpunkte. Im Finanz- und Versicherungswesen sowie in der Informationstechnik werden Datenschutzbeauftragte häufiger intern besetzt. In den Branchen Industrie/Produktion sowie Handel und Konsumgüter dominiert hingegen klar das externe Modell.

57 Prozent der Unternehmen haben keine Rolle des (C)ISO etabliert

Im Vergleich dazu ist die Rolle des (C)ISO deutlich seltener etabliert. Insgesamt verfügen 19 Prozent der Unternehmen über einen internen und 24 Prozent über einen externen (C)ISO, 57 Prozent haben keinen (C)ISO. Die Unterschiede nach Unternehmensgröße sind ausgeprägt. Während bei kleinen Unternehmen rund 60 Prozent keinen (C)ISO haben, sinkt dieser Anteil bei mittleren Unternehmen auf knapp 49 Prozent und bei großen Unternehmen auf 34 Prozent. Entsprechend steigt bei großen Unternehmen der Anteil interner (C)ISOs deutlich an. International tätige Unternehmen haben signifikant häufiger einen (C)ISO als rein national agierende Organisationen.



1 Die erste Zahl gibt den Anteil an der Gesamtstichprobe an (Summe aller Felder = 100 %).  
2 Die Prozentangabe in Klammern gibt den Anteil innerhalb der jeweiligen (C)ISO-Gruppe an (entspricht den Werten im Text).

Quelle: Eigene Erhebung

Abbildung 10: Besetzungsstrategien (C)ISO und Datenschutzbeauftragter

Interne Besetzung von (C)ISO und DSB korrelieren, interne DSBs nehmen ab

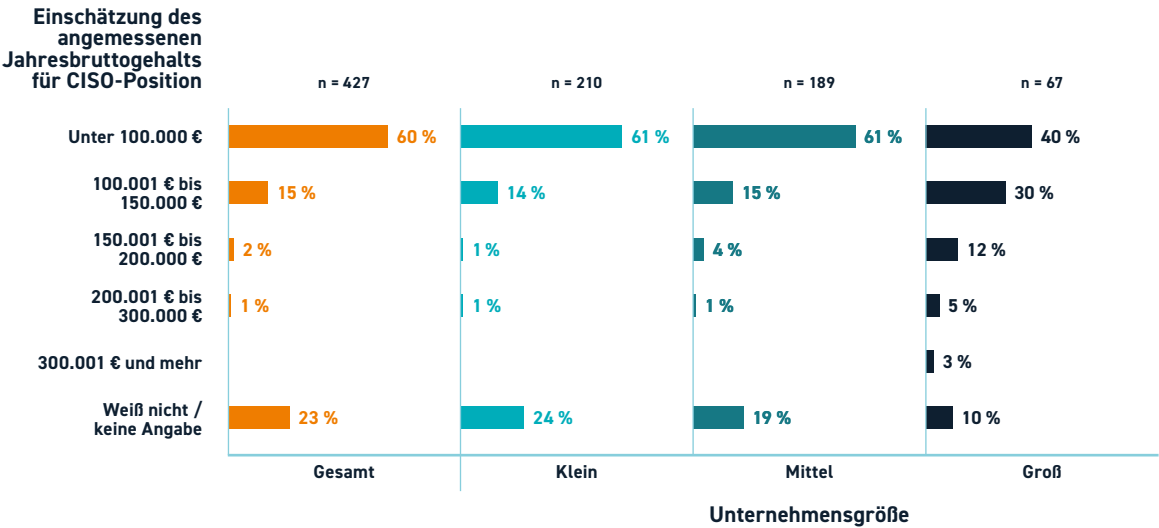
Die Analyse der personellen Sicherheitsstrukturen in den befragten Unternehmen verdeutlicht ein Compliance-getriebenes Organisationsprinzip. Während Datenschutzbeauftragte in der überwiegenden Mehrheit der Unternehmen vorhanden sind, bleibt die Rolle des (C)ISO deutlich häufiger unbesetzt. Datenschutz scheint damit primär als rechtlich verpflichtende Funktion verstanden zu werden, deren Besetzung unmittelbar aus regulatorischen Anforderungen resultiert. Die Verantwortung für Informationssicherheit wird demgegenüber seltener als eigenständige strategische Rolle institutionalisiert.

Die Wahl der jeweiligen Besetzungsstrategien folgt dabei erkennbaren Mustern. Unternehmen mit einem internen (C)ISO verfügen in rund 74 Prozent der Fälle auch über einen internen DSB. Umgekehrt zeigt sich bei Unternehmen mit einem externen DSB, dass in über 70 Prozent der Fälle kein (C)ISO vorhanden ist, was die häufigste Kombination darstellt. Ein weiteres signifikantes Ergebnis der Auswertungen ist, dass Unternehmen mit einem vorhandenen (C)ISO (unabhängig davon, ob intern oder extern besetzt) wesentlich häufiger (65 Prozent) einen externen DSB beauftragen als Unternehmen ohne (C)ISO (54 Prozent). Fehlt ein DSB vollständig, ist

nahezu immer auch kein (C)ISO vorhanden (siehe Abbildung 10). Vor diesem Hintergrund fällt auf, dass die Präsenz interner DSB rückläufig ist. Während im Jahr 2024 noch 38 Prozent der Unternehmen einen internen DSB hatten [299], liegt dieser Anteil inzwischen deutlich niedriger.

60 Prozent schätzen ein Jahresbruttogehalt für CISOs unter 100.000 Euro als angemessen ein

Die Einschätzung des Marktwerts der CISO-Rolle unterstreicht tiefgreifende strukturelle Unterschiede in der Wahrnehmung von Informationssicherheit. Rund 60 Prozent der befragten Unternehmen halten ein Jahresbruttogehalt von unter 100.000 Euro für angemessen, weitere 15 Prozent sehen die Vergütung in einer Spanne von 100.000 und 150.000 Euro als gerechtfertigt an. Diese Bewertung liegt deutlich unter den in Deutschland beobachtbaren Marktwerten, die über alle Erfahrungsstufen hinweg einen Median von rund 198.000 Euro ausweisen (siehe Abbildung 11).



Quelle: Eigene Erhebung

Abbildung 11: Einschätzung des angemessenen Jahresbruttogehalts für CISO-Position

Vor diesem Hintergrund ist festzustellen, dass die Gewinnung qualifizierter Experten für viele Betriebe zur unlösbaren Aufgabe wird. Internationale Vergleiche verschärfen diese Diskrepanz zusätzlich. In den USA beispielsweise liegen die Median-Gehälter für CISOs zwischen 385.000 [293] und 392.000 US-Dollar [184]. Parallel dazu berichten europäische Studien von erheblichen Schwierigkeiten bei der Besetzung von Cybersicherheitspositionen. Rund drei Viertel der Organisationen geben an, offene Positionen nur schwer besetzen zu können [111].

## 2.5 RISIKOMANAGEMENT UND OPERATIVE PRÄVENTION

Die operative Absicherung der IT-Infrastruktur in deutschen Unternehmen zeigt ein ambivalentes Bild zwischen fortschrittlicher Überwachung und erheblichen Lücken in der präventiven Risikoanalyse.

### Risikoanalysen und Penetrationstests sind für viele der Unternehmen noch Neuland

Ein zentraler Baustein, die ganzheitliche Analyse von Risiken und Schutzbedarfen, ist längst nicht flächendeckend implementiert. Im Schnitt geben 40 Prozent der Unternehmen an, noch nie eine solche Analyse vorgenommen zu haben, wobei diese Lücke bei kleinen Unternehmen mit 43 Prozent besonders ausgeprägt ist. Während bei mittleren und großen Unternehmen der Zeitpunkt der letzten Durchführung weniger weit zurückliegt, zeigt sich bei kleineren Akteuren eine geringere Planungstiefe: Während 40 Prozent der mittleren und 46 Prozent der großen Unternehmen eine Analyse für das Jahr 2026 anvisieren, verfolgen 67 Prozent der

kleinen Unternehmen bisher noch keinerlei Planung für eine solche Maßnahme.

Ähnlich verhält es sich bei Penetrationstests, die insgesamt nur von 36 Prozent der Unternehmen durchgeführt werden. Während mittlere und große Betriebe diese Tests deutlich häufiger und regelmäßiger einsetzen, verzichten 61 Prozent der kleinen Unternehmen vollständig darauf (versus 56 Prozent im Gesamtschnitt). Sofern Tests stattfinden, erfolgt dies bei 40 Prozent einmal jährlich, während 27 Prozent nach Bedarf agieren. Im Vergleich zum Vorjahr zeigt sich hier eine leichte Verschiebung: Während 2024 noch 62 Prozent angaben, keine Penetrationstests durchzuführen [299], stieg 2025 der Anteil derer, die anlassbezogen prüfen (von 15 Prozent im Vorjahr auf nun höhere Werte). Aktuell geben 58 Prozent der testenden Unternehmen an, die letzte Prüfung im Befragungsjahr 2025 absolviert zu haben.

### 69 Prozent der Unternehmen setzen auf externe Dienstleister zur Systemüberwachung

Trotz der Defizite in der Risikoanalyse setzen rund zwei Drittel der Unternehmen in Deutschland (69 Prozent) auf externe Dienstleister zur Systemüberwachung (Security Operations Center (SOC) oder Managed Security Services (MSS)). Die Informationstechnik-Branche bildet eine Ausnahme: 55 Prozent der IT-Unternehmen verzichten auf externe Überwachung und managen diese Aufgaben signifikant häufiger intern.

Zur Abwehr interner Bedrohungen setzen deutsche Unternehmen primär auf die Überwachung von Zugriffsrechten (76 Prozent) und Sensibilisierungsschulungen (70 Prozent). Bei großen und mittleren Betrieben stehen

Schulungen mit Werten von bis zu 95 Prozent an erster Stelle. Regelmäßige Audits (42 Prozent) und Mitarbeiterüberprüfungen (2 Prozent) folgen mit deutlichem Abstand, wobei letztere im Vergleich zu 2024 (51 Prozent) abgenommen haben [299]. Ergänzt werden diese Maßnahmen durch Firewalls, Backups und Zwei-Faktor-Authentifizierung sowie reaktive SOC-Strukturen.

Eine deutliche Divergenz zeigt sich beim regulatorischen Umgang mit generativer KI. Während 73 Prozent der großen Unternehmen bereits eine hohe Regelungsdichte aufweisen, verfügen aktuell nur 23 Prozent der kleinen Unternehmen über entsprechende Richtlinien (Insgesamt 26 Prozent der befragten Unternehmen). Auch im Bereich der kritischen Infrastruktur besteht eine Regelungslücke: Bisher haben lediglich 60 Prozent dieser Betriebe verbindliche Vorgaben für den Einsatz generativer KI-Anwendungen implementiert.

## 2.6 RISIKOFAKTOR LIEFERKETTE

Die Absicherung der Lieferkette stellt deutsche Unternehmen vor erhebliche Herausforderungen, wobei insbesondere die Abhängigkeit von externen Partnern und internationalen Dienstleistern kritisch bewertet wird.

### Mehr als zwei Drittel verzichten auf regelmäßige Bewertungen der Cybersicherheit ihrer Lieferanten

Bereits 51 Prozent der Unternehmen berichten, dass einer oder mehrere ihrer Lieferanten Opfer eines Cyberangriffs wurden, wobei dieser Anteil bei großen Unternehmen mit 65 Prozent deutlich höher liegt. Trotz dieser Vorfälle findet eine proaktive Überprüfung von Sicherheitslücken bei Partnern kaum statt: 66 Prozent der Befragten führen keinerlei Überprüfungen durch. Lediglich bei den großen Unternehmen zeigt sich eine aktivere Kontrolle, dort stellten 27 Prozent im vergangenen Jahr ein bis vier Sicherheitslücken bei ihren Lieferanten fest.

Die Reaktion auf Vorfälle bei Lieferanten umfasst ein breites Spektrum, das von der sofortigen Kommunikationssperre und dem Kappen aller Verbindungen über kooperative Problemlösungen bis hin zur Aktivierung interner Notfallprotokolle reicht. Zudem werden technische Absicherungsmaßnahmen der eigenen Systeme sowie Sensibilisierungsschulungen für die eigene Belegschaft eingesetzt. Dennoch verzichten 75 Prozent der Unternehmen auf regelmäßige Audits oder Assess-

ments zur Bewertung der Cybersicherheit ihrer Lieferanten. Größere Unternehmen führen solche Prüfungen eher durch, und zwar am ehesten ein Mal pro Jahr oder häufiger (19 Prozent). Zu verorten sind diese Prüfprozesse primär im Bereich der KRITIS-Unternehmen, die zu 51 Prozent Audits durchführen, zumeist jährlich oder häufiger (24 Prozent).

### Lieferkettenunterbrechungen werden selbst aus den USA als mögliches Risiko betrachtet, Wechselfähigkeiten sind nur teilweise gegeben

Hinsichtlich kritischer digitaler Services aus den USA wird das Risiko einer Lieferkettenunterbrechung differenziert bewertet. Während der Gesamtschnitt das Risiko zu 27 Prozent als niedrig, zu 30 Prozent als mittel und zu 20 Prozent als hoch einstuft, fällt die Einschätzung bei großen Unternehmen deutlich kritischer aus: Hier wird das Risiko zu 39 Prozent als mittel und zu 28 Prozent als hoch bewertet. Bei kleineren Akteuren herrscht Unsicherheit: Kleine und mittlere Unternehmen können das Risiko signifikant häufiger nicht einschätzen (25 Prozent beziehungsweise 22 Prozent).

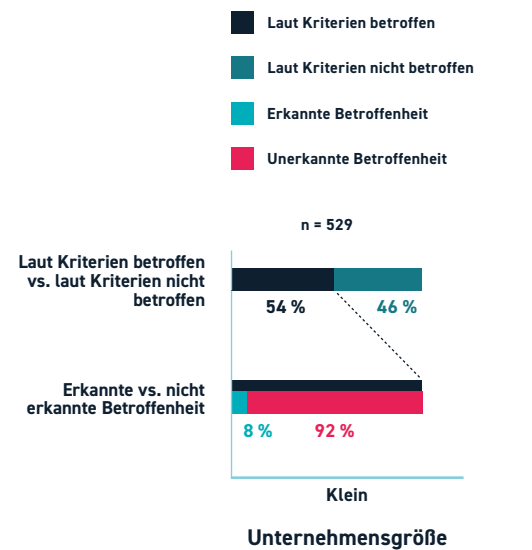
Sollte ein zentraler Nicht-EU-Cloud-Anbieter den Service einstellen, prognostizieren 57 Prozent der Unternehmen eine Wiederherstellungszeit ihrer geschäftskritischen Prozesse von weniger als einer Woche. Hierbei fällt jedoch ein Anteil von 19 Prozent der kleinen Unternehmen auf, die dazu keine Angaben machen können. Auch beim notwendigen Know-how für einen Providerwechsel im Notfall zeigen sich Lücken: Während im Schnitt 49 Prozent über ausreichendes Wissen verfügen – ein Wert, der bei großen Unternehmen auf 60 Prozent steigt – geben 33 Prozent an, kein entsprechendes Fachwissen zu besitzen. Selbst bei den großen Einheiten antworten 17 Prozent lediglich mit „teilweise“.

2.7 NIS-2-REGULATORIK UND VERANTWORTLICHKEIT

Die Einführung der NIS-2-Richtlinie offenbart eine tiefgreifende Diskrepanz zwischen der objektiven Rechtslage und der subjektiven Wahrnehmung im Mittelstand. Während ein erheblicher Teil der Unternehmen die eigene Betroffenheit aufgrund komplexer Schwellenwerte unterschätzt, wächst gleichzeitig der Druck auf die Führungsebene, regulatorische Versäumnisse durch persönliche Haftung abzusichern.

NIS-2: Knowledge Gap bei KMUs – besonders kleinere Unternehmen sollten Einschätzung überprüfen

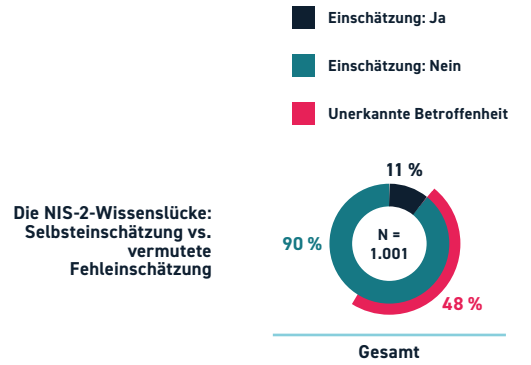
In der direkten Befragung zur Betroffenheit durch die NIS-2-Richtlinie zeigt sich eine deutliche Abhängigkeit von der Unternehmensgröße. Während bei den kleinen Unternehmen 93 Prozent angeben, nicht unter die Richtlinie zu fallen, zeichnet sich bei größeren Organisationen ein anderes Bild ab: Bei den mittleren Unternehmen bejahen 22 Prozent eine Zugehörigkeit (78 Prozent verneinen diese), und bei den großen Unternehmen liegt der Anteil derer, die sich als betroffen identifizieren, bei 43 Prozent.



Quelle: Eigene Erhebung

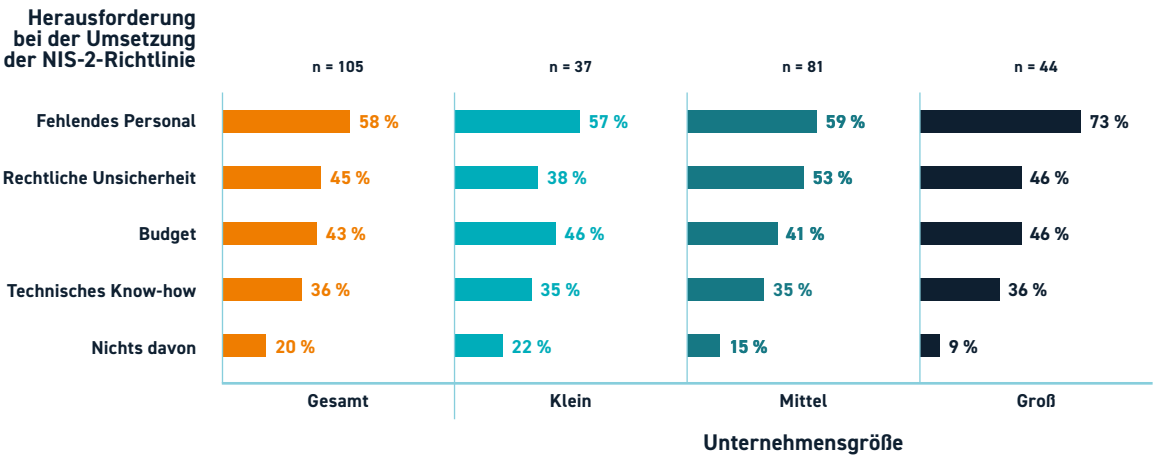
Abbildung 12: NIS 2 Knowledge Gap bei kleinen Unternehmen

Die Analyse der Gesamtdaten lässt jedoch vermuten, dass die tatsächliche Reichweite der Regulierung deutlich unterschätzt wird. Gleicht man die Angaben der Unternehmen zu Sektor, Mitarbeiterzahl und Umsatz mit den formalen Kriterien der Richtlinie zum Stand Ende 2025 ab [49], legen die Merkmale weiterer 478 Organisationen eine potenzielle NIS-2-Pflicht nahe. Da durch die gewählte Erhebungsmethode keine Rückschlüsse auf die tatsächlichen Unternehmen möglich sind und die endgültige Einstufung eine detaillierte juristische Prüfung erfordert, dienen diese Zahlen lediglich als Indizien für eine mögliche Fehleinschätzung: Ein erheblicher Anteil der potenziell betroffenen Organisationen scheint seine regulatorische Rolle zum Befragungszeitpunkt noch nicht erkannt zu haben. Diese Vermutung einer weitreichenden Fehleinschätzung wird insbesondere durch die Anwendung der „Size-Cap-Rule“ gestützt. Insbesondere die Umsatzschwelle scheint bei kleinen Unternehmen mit 10 bis 49 Mitarbeitenden zu Irrtümern zu führen: Viele dieser Akteure schließen offenbar aufgrund ihrer geringen Personalstärke eine Betroffenheit aus, obwohl sie die maßgebliche Umsatzgrenze von 10 Millionen Euro überschreiten. Innerhalb dieser Gruppe der umsatzstarken Kleinunternehmen lässt sich auf Basis der formalen Kriterien bei 92 Prozent eine Fehleinschätzung konstatieren (siehe Abbildung 12). Insgesamt deutet die Datenlage darauf hin, dass 48 Prozent aller befragten Unternehmen eine unerkannte Betroffenheit aufweisen könnten (siehe Abbildung 13). Diese Befunde weisen auf eine Wissenslücke im KMU-Bereich hin. Während Großunternehmen ihre Betroffenheit tendenziell eher erkennen, scheinen mittlere Unternehmen und umsatzstarke kleine Betriebe die NIS-2-Regularien teilweise noch nicht auf das eigene Profil zu projizieren.



Quelle: Eigene Erhebung

Abbildung 13: NIS 2 Knowledge Gap



Quelle: Eigene Erhebung

Abbildung 14: Größte Herausforderungen bei der Umsetzung der NIS-2-Richtlinie

Fehlendes Personal, rechtliche Unsicherheit und begrenzte Budgets als Haupthindernisse für NIS-2 Umsetzung

Jene Unternehmen, die sich als betroffen von NIS-2-Richtlinie einstufen, berichten von erheblichen operativen Hindernissen. Als größte Herausforderungen bei der Umsetzung der NIS-2-Richtlinie nennen sie fehlendes Personal (58 Prozent), rechtliche Unsicherheit (45 Prozent) und begrenzte Budgets (43 Prozent) (siehe Abbildung 14). Der Informationsstand ist dabei selbst in den kritischen Sektoren defizitär. Während sich zwar 49 Prozent der KRITIS-Unternehmen als (sehr) gut informiert bezeichnen, geben 54 Prozent der kleineren KRITIS-Betriebe sowie 41 Prozent der großen Organisationen an, sich wenig bis gar nicht über die konkreten Anforderungen informiert zu fühlen. Diese Wahrnehmung korreliert mit einer kritischen Distanz zu den staatlichen Institutionen: 62 Prozent der Befragten geben an, sich von den zuständigen Behörden im Prozess der NIS-2-Einführung unzureichend unterstützt zu fühlen.

Vor diesem Hintergrund findet die Debatte um die persönliche Verantwortung breite Unterstützung: 48 Prozent der Befragten befürworten eine persönliche Haftbarkeit von Geschäftsführern und Aufsichtsräten bei mangelnden Schutzvorkehrungen vor Cyberangriffen, wobei diese Forderung in großen Unternehmen (70 Prozent) und innerhalb der KRITIS-Sektoren (60 Prozent) eine noch deutlich stärkere Zustimmung erfährt. Diese Einschätzung deckt sich mit der aktuellen regulatorischen Entwicklung durch die NIS-2-Richtlinie. Wie der Start des neuen BSI-Meldeportals verdeutlicht, rückt die Organhaftung für rund 30.000 Unternehmen nun ins Zentrum der Compliance. Dass insbesondere große Unternehmen und KRITIS-Betreiber die Haft-

barkeit befürworten, lässt sich auf die drakonischen Sanktionen von bis zu 2 Prozent des weltweiten Jahresumsatzes zurückführen. In diesen Sektoren wird die persönliche Haftung der Geschäftsführung zunehmend als unverzichtbarer Hebel begriffen, um IT-Sicherheit auf die gleiche strategische Stufe wie Kartellrecht oder Datenschutz zu heben [102].

2.8 DIGITALE SOUVERÄNITÄT UND LIEFERKETTEN-RESILIENZ

Digitale Souveränität hat sich spätestens seit 2025 zu einem greifbaren Umsetzungs-Thema entwickelt. Während Initiativen wie GAIA-X, die European Data Spaces oder das Sovereign Cloud Framework (siehe Kapitel 4) auf politischer Ebene das Ziel digitaler Souveränität verfolgen, stehen Unternehmen vor der praktischen Herausforderung, ihre Handlungsfähigkeit in einer volatilen und vernetzten Welt zu sichern. Digitale Souveränität ist hierbei kein Selbstzweck, sondern der Grundstein für Resilienz. Die Fähigkeit, kritische Systeme auch bei geopolitischen Spannungen oder Lieferkettenausfällen aufrechtzuerhalten, hängt direkt davon ab, wie stark Unternehmen in Abhängigkeiten (Vendor-Lock-in) gefangen sind oder sie managen können. Die vorliegenden Ergebnisse zeigen, wie deutsche IT-Entscheider zwischen strategischem Anspruch und operativer Realität navigieren.



2.8.1 Strategische und personelle Verankerung

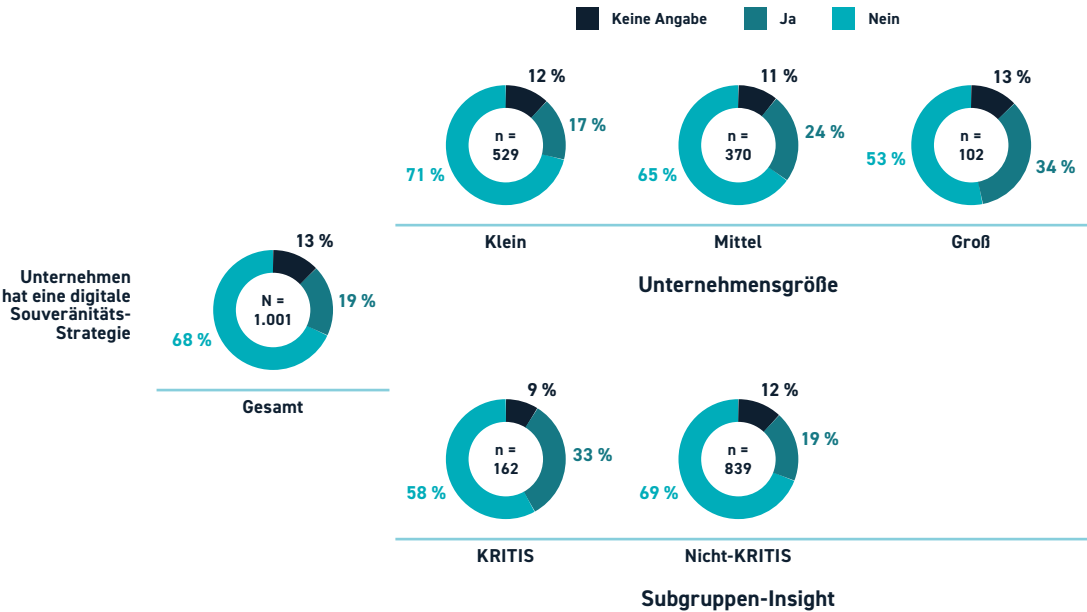
Jedes fünfte Unternehmen verfolgt eine digitale Souveränitäts-Strategie – wobei das Thema eher für mittlere und große Unternehmen relevant ist

Obwohl digitale Souveränität als geopolitisches und wirtschaftliches Schlagwort allgegenwärtig ist, zeigt die Realität in deutschen Unternehmen noch ein anderes Bild. Das Thema scheint vielfach noch ein Randphänomen zu sein: Lediglich 19 Prozent der befragten Unternehmen geben an, über eine definierte Strategie für die digitale Souveränität zu verfügen (siehe Abbildung 15). Dem gegenüber steht eine deutliche Mehrheit von 68 Prozent, die bislang ohne ein solches strategisches Leitbild agiert. Diese Zahlen decken sich mit einer Studie aus dem Mai 2025, welche „tech readiness“ bei nur 18 Prozent der deutschen und 22 Prozent der französischen Unternehmen als C-Level Priorität identifiziert [18]. Diese Zahlen legen nahe, dass digitale Souveränität oft noch eher als abstraktes politisches Ziel, denn als konkrete Corporate Strategy begriffen wird.

Ein Blick auf die Unternehmensgrößen und Branchen offenbart jedoch, dass das Thema in der deutschen Wirtschaft durchaus ankommt. Bei Großunternehmen mit über 250 Mitarbeitenden ist die strategische Verankerung mit 34 Prozent fast doppelt so hoch wie im Durchschnitt. Noch deutlicher wird die Relevanz in stark regulierten Sektoren: Die Finanz- und Versicherungswirtschaft nimmt hier eine klare Vorreiterrolle ein. Mit 48 Prozent hat fast die Hälfte der Unternehmen in diesem Sektor eine Souveränitäts-Strategie implementiert – ein Wert, der die wachsende Bedeutung des Themas im Kontext sensibler Finanzdaten unterstreicht. Auch KRITIS-Betreiber liegen mit 33 Prozent signifikant über dem Niveau anderer Unternehmensgruppen.

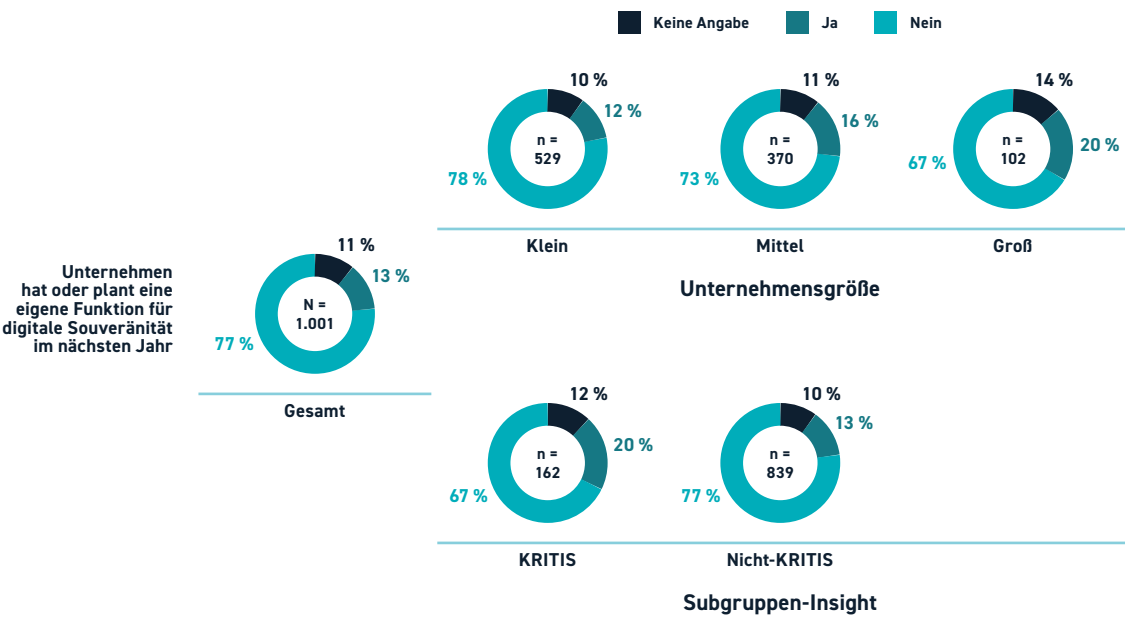
13 Prozent der Unternehmen haben oder planen eine Funktion für digitale Souveränität, bei großen Unternehmen ist der Anteil mit 20 Prozent höher

Hinsichtlich der personellen Verankerung wählen Unternehmen unterschiedliche organisatorische Pfade. Dass aktuell nur 13 Prozent aller Unternehmen eine dedizierte Funktion für digitale Souveränität geschaffen haben oder planen (siehe Abbildung 16), ist nicht zwangsläufig als Mangel an Umsetzungskraft zu deuten. Vielmehr legt dieser Befund nahe, dass digitale Souveränität in der Breite der Wirtschaft überwiegend



Quelle: Eigene Erhebung

Abbildung 15: Vorhandensein einer digitalen Souveränitätsstrategie



Quelle: Eigene Erhebung

Abbildung 16: Planung einer Funktion für digitale Souveränität im Unternehmen

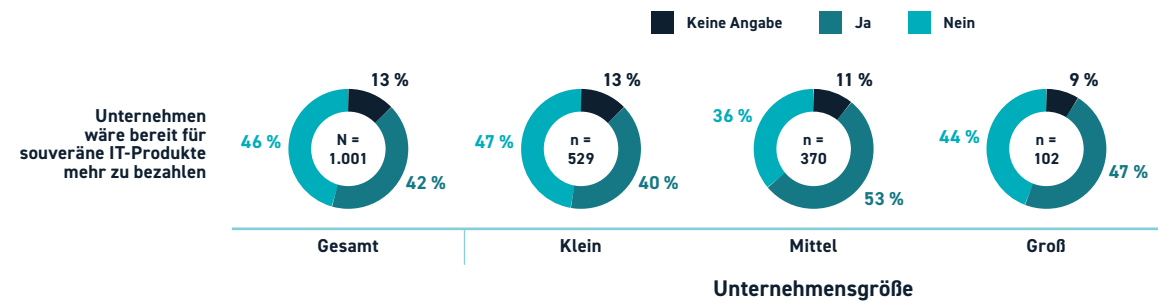
als Querschnittsaufgabe verstanden werden könnte, die in bestehenden Verantwortungsbereichen – etwa beim CIO oder CISO – integriert ist, anstatt isoliert in einer neuen Stabsstelle behandelt zu werden. Dennoch zeigt sich bei steigender Unternehmensgröße und Komplexität eine Tendenz zur Spezialisierung. Bei Großunternehmen liegt der Anteil dedizierter Funktionen mit 20 Prozent signifikant höher. Auch stark regulierte oder technologieintensive Branchen wie das Finanz- und Versicherungswesen (17 Prozent), die IT-Branche (18 Prozent) sowie KRITIS-Betreiber (20 Prozent) setzen häufiger auf spezialisierte Rollen. Dies deutet darauf hin, dass ab einem gewissen Grad an regulatorischer Dichte oder internationaler Verflechtung (16 Prozent bei international aktiven Firmen) die Schaffung expliziter Verantwortlichkeiten als notwendiger Schritt erachtet wird, um die strategischen Anforderungen operativ zu bewältigen.

2.8.2 Zahlungsbereitschaft und Souveränitäts-Premium

42 Prozent der Unternehmen geben an, dass sie bereit wären, für souveräne IT-Produkte mehr zu bezahlen

Ein relevanter Teil der Befragten ist nach eigenen Angaben bereit, für souveräne IT-Lösungen höhere Kosten in Kauf zu nehmen (42 Prozent) (siehe Abbildung 17). Das Handelsblatt Research Institut und StackIT finden 2025 noch höhere Werte von 70 Prozent beziehungsweise 80 Prozent (öffentlicher beziehungsweise privater Sektor) Zustimmung zur Bereitschaft, einen Aufpreis für digitale Souveränität zu zahlen [314], während andere vor der Höhe der ökonomischen Kosten für digitale Souveränität warnen [226]. Dabei ist zu berücksichtigen, dass es sich um eine deklarative Selbstausskunft handelt, die nicht zwangsläufig das tatsächliche Kaufverhalten widerspiegelt. Dennoch deutet das Ergebnis darauf hin, dass Unabhängigkeit von einem Teil der Unternehmen als werthaltig wahrgenommen wird.

Diese Bereitschaft, für ein Souveränitäts-Premium zu zahlen, variiert deutlich zwischen den Branchen. Die höchsten Zustimmungswerte finden sich im Gesundheitswesen (56 Prozent), gefolgt von der IT-Branche (53 Prozent) und dem Finanz- und Versicherungswesen



Quelle: Eigene Erhebung

Abbildung 17: Zahlungsbereitschaft für souveräne IT-Produkte

(52 Prozent). In diesen Sektoren wird der Mehrwert souveräner Lösungen und die Vermeidung von Abhängigkeiten offenbar höher gewichtet als die initialen Mehrkosten. Dem gegenüber steht die Energie- und Versorgungsbranche mit einer Zustimmung von 30 Prozent.

International agierende Unternehmen weisen eine höhere Zahlungsbereitschaft (49 Prozent) auf als rein national tätige Firmen (41 Prozent). Dies lässt sich vor dem Hintergrund globaler Compliance-Anforderungen interpretieren: Unternehmen, die in verschiedenen Jurisdiktionen operieren, investieren offenbar eher in Lösungen, die Datensicherheit und Rechtskonformität grenzüberschreitend gewährleisten sollen. Eine ähnliche Tendenz zeigt sich bei der Betrachtung der IT-Sicherheitsstrukturen: In Unternehmen mit einem etablierten (C)ISO liegt die Bereitschaft für ein Preis-Premium bei 53 Prozent, was eine Korrelation zwischen vorhandener Sicherheits-Expertise und der Wertschätzung digitaler Souveränität nahelegt.

#### Investitionen in technologische Unabhängigkeit bleiben vorerst ein Thema für Großunternehmen und KRITIS-Betreiber

Obwohl die Reduktion von Abhängigkeiten (Vendor-Lock-in) in der fachpolitischen Debatte hohe Priorität genießt, schlägt sich dies in den konkreten Budgetplanungen der meisten deutschen Unternehmen noch nicht nieder. Während eine Studie aus 2025 ein Anteil von 58 Prozent der Unternehmen angibt, Investitionen in die Verringerung von Abhängigkeiten von nicht europäischen Technologieanbietern zu planen [18], führen in der vorliegenden Umfrage lediglich 13 Prozent der Befragten an, gezielte Ausgaben oder Investitionen zu planen, um ihre Abhängigkeit von bestimmten Anbietern zu verringern. Dem gegenüber steht eine deutliche

Mehrheit von 83 Prozent, die aktuell keine finanziellen Mittel für diesen Zweck vorsieht. Diese Diskrepanz deutet darauf hin, dass die technologische Diversifizierung oft noch an hohen Wechselkosten oder fehlenden Marktalternativen scheitert. Diese Werte spiegeln auch eine Diskrepanz zur oben geführten Bereitschaft wider, für ein Souveränitäts-Premium zu zahlen, welche sich weitestgehend nicht in geplanten Investitionen niederschlagen scheint.

Ein differenzierter Blick auf die Unternehmensstrukturen zeigt jedoch, dass die Relevanz des Themas mit der Größe und Komplexität der Organisation zunimmt. Bei Großunternehmen ist die Investitionsbereitschaft mit 28 Prozent mehr als doppelt so hoch wie im Gesamtdurchschnitt, und auch mittlere Betriebe liegen mit 18 Prozent sichtbar über dem Niveau kleinerer Einheiten. Besonders deutlich wird der Investitionsdruck in Bereichen mit erhöhten Sicherheits- und Compliance-Anforderungen: Mit 22 Prozent investieren KRITIS-Betreiber signifikant häufiger in die Verringerung von Abhängigkeiten als Nicht-KRITIS-Unternehmen (14 Prozent). Weltweit agierende Firmen planen zu 19 Prozent entsprechende Investitionen (gegenüber 12 Prozent bei rein national tätigen Unternehmen). Unternehmen, in denen die Rolle eines (C)ISO etabliert ist, weisen mit 18 Prozent eine höhere Aktivität auf als Unternehmen ohne diese Funktion (12 Prozent). Dies legt nahe, dass technologische Unabhängigkeit zunehmend als integraler Bestandteil einer professionellen Cyberresilienz begriffen wird.

### 2.8.3 Strategien für den Umgang mit Abhängigkeiten

#### Multi-Vendor-Strategien finden immer mehr Verbreitung

Das Bewusstsein für die Risiken durch Abhängigkeiten, besonders von Vendor-Lock-ins, ist in der deutschen Wirtschaft fest etabliert. In einem Gutachten des Leibniz-Zentrum für Europäische Wirtschaftsforschung (ZEW) geben 58 Prozent der Unternehmen in der Informationswirtschaft Lock-in-Effekte als zentralen Grund für bestehende Abhängigkeit an [358]. Insbesondere Großunternehmen überlassen dieses Thema nicht mehr dem Zufall: Während über alle Befragten hinweg noch gut ein Viertel angibt, keine speziellen Maßnahmen gegen Lock-in-Effekte zu ergreifen, sinkt dieser Wert bei Unternehmen mit mehr als 250 Mitarbeitenden auf 8 Prozent. Das Management von Abhängigkeiten ist im Enterprise-Segment somit zur Standardaufgabe avanciert. Als am stärksten genutzte Instrumente haben sich dabei die regelmäßige Evaluierung von Alternativen (54 Prozent) und die konsequente Nutzung offener Standards (47 Prozent) durchgesetzt, gefolgt von expliziten Multi-Vendor-Strategien (23 Prozent). Wenn auch auf niedrigerem Niveau hinter anderen Maßnahmen, wächst die Adoption von Multi-Vendor-Strategien merklich im Vergleich zum Vorjahr (2024: 10 Prozent) [299]. Außerdem setzen Unternehmen laut eigenen Angaben unter anderem auf eigene Softwareentwicklung, eigene Rechenzentren und On-Premise-Betrieb.

#### Open-Source-Lösungen, offene Schnittstellen und Sicherheitszertifikate als Prioritäten zum Management geopolitischer Risiken

Bei der Software-Beschaffung zeigen sich Unterschiede in den Prioritäten unter Maßnahmen zur Mitigierung geopolitischer Risiken. Zwei Kriterien dominieren das Feld: 36 Prozent der Entscheider fordern nachweisbare Sicherheitszertifikate über die gesamte Lieferkette hinweg. Nahezu gleichauf liegt mit 39 Prozent eine Präferenz für Open-Source (OS)-Lösungen. Erwähnung finden außerdem die exklusive Nutzung europäischer Cloud-Lösungen, Präferenz für Vendor-Firmensitze in der EU sowie die Datenlokalisierung in der EU.

Der Blick auf die Branchen offenbart hierbei unterschiedliche Ansätze zur Erreichung von digitaler Souveränität. Das Gesundheitswesen setzt am stärksten auf nachweisbare Sicherheitszertifikate (60 Prozent) und im Branchenvergleich überdurchschnittlich stark

auf OS (48 Prozent). Im Finanzsektor hingegen steht die Compliance im Vordergrund: Hier priorisieren 59 Prozent der Entscheider die explizite juristische Kontrolle über ihre Daten.

Dieser Wunsch nach rechtlicher Absicherung korreliert stark mit dem Grad der Internationalisierung. International tätige Unternehmen pochen signifikant häufiger auf die juristische Datenkontrolle (38 Prozent) als rein nationale Akteure (27 Prozent). Dies ist als klare Abwehrhaltung gegenüber extraterritorialen Zugriffsmöglichkeiten, etwa durch den US Cloud Act, zu werten. Gleichzeitig setzen internationale Firmen stärker auf OS-Lösungen (47 Prozent). Diese Kombination aus rechtlicher Abschottung und technologischer Offenheit scheint die moderne Formel für globale digitale Resilienz zu sein.

### 2.8.4 Wahrnehmung europäischer Initiativen

#### Nur 28 Prozent der Befragten stimmen der Aussage zu, dass GAIA-X Europa digital souverän machen wird

Die Wahrnehmung zentraler EU-Initiativen zur Stärkung der digitalen Souveränität fällt zwischen deutschen IT-Entscheidern unterschiedlich aus. Das einstige politische Vorzeigeprojekt GAIA-X, gestartet mit der Vision einer europäischen Dateninfrastruktur, scheint in der breiten Masse der Unternehmen an Zugkraft verloren zu haben. Nur 28 Prozent der Befragten stimmen der Aussage zu, dass GAIA-X Europa digital souverän machen wird. Ein fast identisch großer Anteil lehnt dies ab, während die größte Gruppe (43 Prozent) unsicher ist oder keine Angabe macht. Für ein Projekt dieser finanziellen und politischen Tragweite deutet dieser hohe Anteil an Unentschlossenen auf ein erhebliches Kommunikations- oder Relevanzdefizit hin.

#### Das größte Potenzial europäischer Initiativen für digitale Souveränität wird in European Data Spaces gesehen

Ein wesentlich positiveres Bild zeichnet sich bei den Common European Data Spaces ab. Hier stimmt knapp die Hälfte der Entscheidungsträger (50 Prozent) zu, dass diese einen echten Beitrag zur europäischen Souveränität leisten werden. Im Gegensatz zu GAIA-X scheinen die sektorspezifischen Datenräume greifbaren Nutzen zu versprechen. Besonders deutlich wird dies

in betroffenen und schon eingebundenen Industrien: Im Gesundheitswesen (European Health Data Space) sehen 68 Prozent und in der Finanzbranche (European Financial Data Space) 59 Prozent die Data Spaces als Souveränitäts-Treiber. Die gemeinsame Vision des Datenaustauschs innerhalb einer Branche wirkt hier offenbar als starker Katalysator für Akzeptanz.

**Etwa ein Drittel der IT-Verantwortlichen (29 Prozent) äußert bereits heute Besorgnis über die Verfügbarkeit ausreichender Rechenzentrumskapazitäten**

Ergänzend zur Software- und Datenebene rückt zunehmend die physische Infrastruktur in den Fokus. Etwa ein Drittel der IT-Verantwortlichen (29 Prozent) äußert bereits heute Besorgnis über die Verfügbarkeit ausreichender Rechenzentrumskapazitäten, insbesondere im Hinblick auf kommende KI-Workloads. Diese Sorge ist bei mittleren und größeren Unternehmen mit circa 35 Prozent stärker ausgeprägt als bei kleineren Firmen. Die Dringlichkeit dieser Kapazitätsfrage unterstreicht auch das Zentrum für KI-Risiken und -Auswirkungen (KIRA Center), das vor einem Verlust der technologischen Souveränität warnt, sofern Deutschland nicht umgehend eine ambitionierte Ausbaustrategie für eigene KI-Infrastrukturen verfolgt [150].

**2.9 POLITISCHE MASSNAHMEN**

Wie lässt sich digitale Souveränität in einem global vernetzten Markt praktisch umsetzen? Für BSI-Präsidentin Claudia Plattner hängt der Erfolg entscheidend von der „engen Kooperation von Staat, Wirtschaft, Wissenschaft und Gesellschaft“ ab [276]. Die vorliegenden Umfrageergebnisse spiegeln jedoch eine ambivalente Realität wider: Von der Skepsis gegenüber EU-Regeln bis hin zur Forderung nach aktiver Cyberabwehr wird deutlich, dass IT-Entscheider derzeit die verlässlichen Rahmenbedingungen vermissen, die für diese gemeinschaftliche Strategie notwendig wären.

**Ambivalente Haltung zu EU-Regulierung**

Die Frage, ob aktuelle EU-Regulierungen die digitale Souveränität Deutschlands und der Europäischen Union tatsächlich stärken, spaltet die befragten Unternehmen. Mit einer Zustimmungsrate von 41 Prozent bewertet weniger als die Hälfte der Entscheider den derzeitigen regulatorischen Rahmen als positiv für

die Souveränität. Dies deutet darauf hin, dass die regulatorischen Eingriffe vielfach nicht als Enabler, sondern möglicherweise als bürokratische Hürde oder als wirkungslos wahrgenommen werden. Dabei zeigt sich eine Korrelation zur Unternehmensgröße: Bei Großunternehmen steigt die Zustimmung auf 50 Prozent. Ein deutlicher Ausreißer ist auch hier die Finanz- und Versicherungsbranche, die mit 59 Prozent Zustimmung eine signifikant positivere Sicht auf die EU-Vorgaben hat. Der internationale Tätigkeitsradius eines Unternehmens hat keinen messbaren Einfluss auf diese Einschätzung.

**2.9.1 Politische Massnahmen für digitale Souveränität und Cybersicherheit**

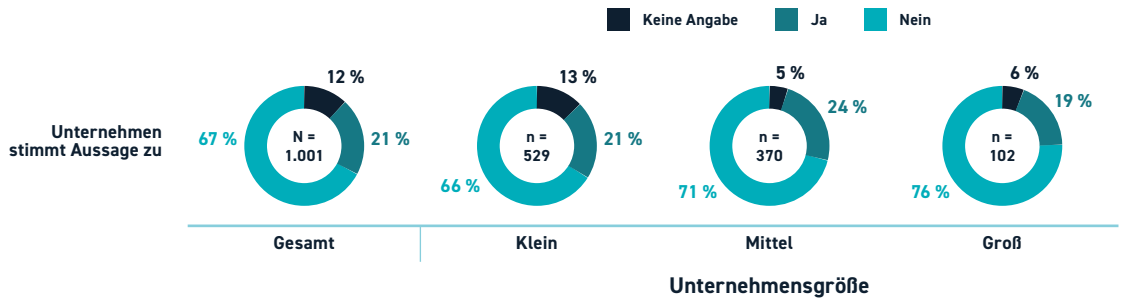
**Die große Mehrheit wünscht sich politische Maßnahmen zur Stärkung der digitalen Souveränität**

Hinsichtlich der Frage, welche politischen Maßnahmen geeignet wären, die digitale Souveränität in Europa zu stärken, favorisieren die IT-Entscheider vor allem fördernde Rahmenbedingungen und den Aufbau von Kapazitäten. Dass Maßnahmen grundsätzlich als notwendig erachtet werden, ist Konsens: Lediglich 6 Prozent der Befragten geben an, dass keine speziellen Maßnahmen erforderlich seien.

An der Spitze der Prioritätenliste steht dabei nicht die Technologie, sondern der Faktor Mensch: 66 Prozent der Befragten sehen in Förderprogrammen zum Aufbau digitaler Fachkompetenzen einen wirksamen Hebel. Dicht darauf folgen infrastrukturelle und technische Grundlagen, die Alternativen zu bestehenden Abhängigkeiten bieten sollen: Die Schaffung vertrauenswürdiger Dateninfrastrukturen (63 Prozent) sowie die Bereitstellung souveräner Standard-IT-Lösungen (60 Prozent) werden als zentrale Bausteine identifiziert.

Auch finanzielle Anreize finden breite Zustimmung als Instrument der Souveränitätsstärkung: 59 Prozent befürworten Investitionsanreize oder Subventionen, 53 Prozent sehen die gezielte Finanzierung von Open-Source-Technologien als zielführend an. Spezifischere Instrumente wie ein „European Sovereign Tech Fund“ (34 Prozent) finden im Durchschnitt weniger Anklang, werden jedoch in der finanzorientierten Versicherungs- und Bankenbranche deutlich relevanter eingeschätzt (59 Prozent). Auffällig ist zudem ein Größeneffekt: Je größer das Unternehmen, desto stärker werden die genannten politischen Maßnahmen als wirkungsvoll für

„Aktuelle Maßnahmen von Politik und Verwaltung unterstützen uns ausreichend dabei, das Unternehmen vor Cyberangriffen zu schützen.“



Quelle: Eigene Erhebung

Abbildung 18: Einschätzung aktueller politischer Maßnahmen gegen Cyberangriffe

die Stärkung der Souveränität bewertet. Darüber hinaus wünschen sich Unternehmen vereinzelt finanzielle Förderung, bessere Aufklärung und zentrale Informationsstellen, Bürokratieabbau, Stärkung der staatlichen Abwehr und Strafverfolgung sowie die Bereitstellung und Sicherung von Infrastruktur.

**2.9.2 Vertrauensdefizit bei Cyberresilienz und staatlicher Aufstellung**

**Lediglich 21 Prozent der Unternehmen empfinden die Unterstützung von Politik und Verwaltung beim Schutz vor Cyberangriffen als ausreichend**

Ein kritisches Bild zeichnet sich bei der Bewertung der aktuellen Sicherheitsarchitektur ab. Auf die Frage, ob die derzeitigen Maßnahmen von Politik und Verwaltung die Unternehmen ausreichend beim Schutz vor Cyberangriffen unterstützen, stimmen nur 21 Prozent zu (siehe Abbildung 18). Eine deutliche Mehrheit von 67 Prozent verneint dies. Das Gefühl, vom Staat im Cyberraum nicht hinreichend geschützt zu werden, dominiert branchenübergreifend. Lediglich im Finanzsektor ist das Vertrauen mit 38 Prozent etwas höher ausgeprägt, während Sektoren wie Transport und Logistik (16 Prozent) eine besonders geringe Unterstützungswahrnehmung aufweisen.

**Die Aufstellung von Bund, Ländern und Kommunen gegen Cyberangriffe wird mehrheitlich als mittel oder schwach wahrgenommen**

Dieses Misstrauen korrespondiert mit der Einschätzung der eigenen Widerstandsfähigkeit des Staates. Die Befragten trauen der öffentlichen Verwaltung kaum zu, selbst gegen Cyberangriffe gewappnet zu sein. Der Bund schneidet hierbei noch vergleichsweise am besten ab, wird aber nur von 15 Prozent als gut aufgestellt bewertet (siehe Tabelle 2). Bei den Bundesländern sinkt dieser Wert auf 12 Prozent. Besonders alarmierend ist die Wahrnehmung der kommunalen Ebene: Nur 7 Prozent attestieren den Kommunen eine gute Aufstellung, während gut die Hälfte der Befragten (51 Prozent) die Cyberresilienz der Kommunen explizit als schwach einstuft. Dies spiegelt eine tiefe Skepsis gegenüber der digitalen Handlungsfähigkeit des Staates auf der Verwaltungsebene wider.

|              | Bund | Länder | Kommunen |
|--------------|------|--------|----------|
| Schwach      | 28 % | 32 %   | 51 %     |
| Mittel       | 42 % | 40 %   | 28 %     |
| Gut          | 15 % | 12 %   | 7 %      |
| Keine Angabe | 16 % | 16 %   | 14 %     |

Quelle: Eigene Erhebung

Tabelle 2: Aufstellung von Bund, Ländern und Kommunen gegen Cyberangriffe

### Hohe Zustimmung zur aktiven Cyberabwehr

Während die deutsche Sicherheitspolitik beim Thema „Hackback“ traditionell zur Zurückhaltung mahnt, offenbaren IT-Entscheidungsträger eine deutlich offensivere Haltung: 79 Prozent der Befragten befürworten staatliche offensive Cybermaßnahmen gegen ausländische Angreifer (siehe Abbildung 19). Noch auffälliger ist die Einschätzung auf privatwirtschaftlicher Ebene, wo solche Befugnisse mit 59 Prozent eine Mehrheit sogar selbst Unternehmen zugesteht. Diese Zahlen sind im deutschen Kontext als unerwartet einzustufen, da sie in deutlichem Kontrast zur geltenden Rechtslage und der völkerrechtlichen Debatte stehen. Offensive Maßnahmen, die von der gezielten Störung krimineller Infrastrukturen wie beim Fall „Emotet“ bis hin zu aktiven Vergeltungsschlägen reichen, unterliegen hierzulande strengen Hürden. Sie gelten als Ultima Ratio und erfordern eine zweifelsfreie Zuordnung des Angreifers, was technisch häufig kaum lückenlos möglich ist.

Die hohe Akzeptanz für solche Operationen ignoriert zudem Eskalationsrisiken und die Gefahr von Kollateralschäden an ziviler Infrastruktur, die mit aktiver Cyberverteidigung einhergehen. Während das Bundeskriminalamt oder das Militär für solche Eingriffe klare Mandate benötigen und der Verfassungsschutz zwar zur Aufklärung, aber kaum zur aktiven Störung befugt ist, scheint die Praxis eine deutlich robustere Gangart einzufordern. Dass mehr als die Hälfte der Befragten sogar Unternehmen offensive Rechte einräumen möchte, deutet auf eine wachsende Frustration über rein de-

fensive Schutzmaßnahmen hin. Letztlich offenbart der Befund eine Kluft zwischen dem Wunsch nach digitaler Wehrhaftigkeit und den verfassungsrechtlichen Bedenken gegen eine „digitale Selbstjustiz“, die das Risiko unkontrollierbarer Konfliktspiralen birgt.

### 2.10 FAZIT

Die Ergebnisse der Studie zeigen eine deutsche Wirtschaft im Umbruch. Einerseits reagieren die Unternehmen mit einer massiven Steigerung der IT-Sicherheitsbudgets, deren Anteil am IT-Gesamtbudget sich von 8 Prozent im Jahr 2024 auf 17 Prozent im Jahr 2025 mehr als verdoppelt hat. Diese Entwicklung wird maßgeblich durch die verschärfte Bedrohungslage sowie neue gesetzliche Vorgaben wie die NIS-2-Richtlinie vorangetrieben, wobei insbesondere in hochregulierten Sektoren die gesetzlich verankerte persönliche Haftung der Geschäftsführung dazu führt, dass IT-Sicherheit zur „Chefsache“ priorisiert wird.

Andererseits offenbaren die Daten eine strukturelle Implementierungslücke: Während der Datenschutz als rechtlich verpflichtende Rolle etabliert ist, bleibt die strategische Verantwortung für die Informationssicherheit häufig unbesetzt oder wird an externe Partner ausgelagert. Solange die Gehaltsvorstellungen für die Rolle eines CISO nicht mit dem tatsächlichen Marktwert und der wachsenden regulatorischen Verantwortung korrespondieren, bleibt eine personelle Lücke in der

deutschen Sicherheitsarchitektur bestehen, welche die Transformation von rein formaler Compliance hin zu langfristiger Resilienz erschwert.

Dabei zählt sich die Institutionalisierung der (C)ISO-Rolle messbar aus: Organisationen mit dedizierter Sicherheitsleitung schätzen ihren Vorbereitungsgrad signifikant höher ein und reduzieren Folgekosten bei Vorfällen. Über den reaktiven Schutz hinaus fungiert der (C)ISO als Treiber für digitale Souveränität: In diesen Unternehmen liegen die Bereitschaft, ein Premium für souveräne Produkte zu zahlen (53 Prozent), und die Aktivität zur Reduktion technologischer Abhängigkeiten (18 Prozent) deutlich über dem Durchschnitt.

Besonders KRITIS-Betreiber bilden hier mit einer überdurchschnittlichen personellen und finanziellen Grundausstattung das Fundament einer Resilienz-Architektur, um komplexe Governance-Aufgaben wie Lieferketten-Audits oder KI-Regulierung zu adressieren. Trotz dieser Strukturen bleibt eine Informationslücke bestehen, da sich insbesondere kleinere KRITIS-Einheiten unzureichend über konkrete Anforderungen der NIS-2-Richtlinie informiert fühlen. Jedoch befürworten Unternehmen dieser Sektoren die persönliche Haftung der Geschäftsführung, was den Wunsch unterstreicht, Cybersicherheit als unverzichtbaren Hebel auf die strategische Ebene der Unternehmensführung zu heben.

Die operative Absicherung der IT-Infrastruktur zeichnet ein ambivalentes Bild zwischen fortschrittlicher Überwachung und erheblichen Defiziten in der Prävention. Während externe Sicherheitsdienstleister (SOC/MSS) zum Standard gehören, mangelt es an systematischen Risikoanalysen und Penetrationstests, die insgesamt nur von 36 Prozent der Unternehmen durchgeführt werden.

Besonders im Mittelstand hemmen Ressourcenmangel und regulatorische Komplexität die Prävention. Die dort vermutete Wissenslücke bezüglich der NIS-2-Betroffenheit ist Symptom einer tiefergehenden Herausforderung. Die hohe Akzeptanz für offensive staatliche Maßnahmen wie Hackbacks (79 Prozent) bei gleichzeitigem Defizit an elementaren Eigenmaßnahmen verdeutlicht eine wachsende Frustration im Markt.

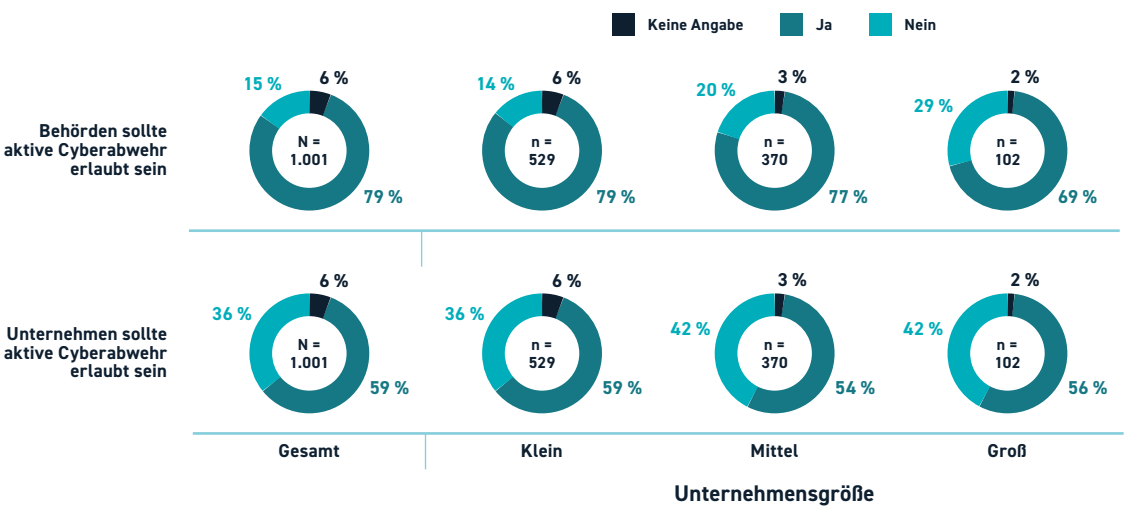
Branchenspezifisch zeigt sich eine Heterogenität, die sich entlang des regulatorischen Drucks formiert. Während hochregulierte Sektoren durch eine überdurchschnittliche strategische Verankerung und eine hohe Akzeptanz für Souveränitäts-Investitionen eine Vorreiterrolle einnehmen, weisen weniger regulierte Bereiche wie das Bauwesen merkbare personelle Defizite auf.

Auch in der Wahl der Resilienz-Instrumente unterscheiden sich die Branchen deutlich: Während das Gesundheitswesen und die IT-Branche ihre Unabhängigkeit verstärkt über technologische Offenheit durch Open-Source-Lösungen und Zertifikate sichern, fokussieren KRITIS-Unternehmen ihre Maßnahmen unter anderem auf die Überprüfung der Lieferketten. Ein kritisches Gefälle zeigt sich schließlich im Systemvertrauen: Sektoren mit komplexen Logistikketten konstatieren eine Diskrepanz zwischen ihrer Bedrohungslage und der wahrgenommenen Unterstützung durch die öffentliche Hand, während das Vertrauen in staatliche Schutzmaßnahmen im Finanzsektor vergleichsweise am höchsten ausgeprägt ist.

Abschließend wird digitale Souveränität zwar als Grundstein für unternehmerische Handlungsfähigkeit begriffen, doch klafft eine Lücke zwischen Anspruch und Umsetzung: Lediglich 13 Prozent der Befragten planen aktuell gezielte Investitionen zur Reduktion von Abhängigkeiten. Immerhin gewinnt das Management von Lock-in-Effekten durch Multi-Vendor-Strategien an Bedeutung und hat sich im Vergleich zum Vorjahr mehr als verdoppelt. Währenddessen zeichnet sich auf der physischen Ebene ein neues Nadelöhr ab: Ein Drittel der IT-Verantwortlichen beunruhigt die Verfügbarkeit ausreichender Rechenzentrumskapazitäten, was die technologische Souveränität im Hinblick auf kommende KI-Workloads ernsthaft gefährden könnte.

Zusammenfassend lässt sich konstatieren, dass für nachhaltige Cybersicherheits-Governance nicht nur ein höheres Budget, sondern auch eine gezielte Schließung der Informations- und Fachkräftelücke erforderlich ist. Regulatorische Anforderungen müssen von einer rein bürokratischen Last in eine gelebte Sicherheitskultur transformiert werden.

Ein wesentlicher Aspekt für die künftige Risikobewertung bleibt jedoch die Grundhaltung innerhalb der Unternehmenslandschaft: Die Durchführung der Studie wurde dadurch erschwert, dass viele kleine Unternehmen ein deutlich geringeres Interesse an einer Teilnahme zeigten. Diese Betriebe gaben häufig an, Cybersicherheit nicht als Teil ihres eigenen Aufgabenbereichs zu definieren. Solange diese Wahrnehmung besteht, bleibt die operative Resilienz der Breite der deutschen Wirtschaft gefährdet, da technische Aufrüstung allein fehlendes Risikobewusstsein und unbesetzte Verantwortlichkeiten nicht kompensieren kann.



Quelle: Eigene Erhebung

Abbildung 19: Zustimmung zu aktiver Cyberabwehr



# KAPITEL 3



# ROBOTIK IM KONFLIKT VOM HELFER ZUM TERMINATOR

## CPU / GEHIRN

Wetware, Spiking Neural Networks und Photonik

## SENSORIK

Neuromorphe und ereignisbasierte Sensoren, Edge Analytics

## KÖRPER

Speziallegierungen, Soft Robotics, Quasi-Direktantriebsmotoren

## ENERGIEVERSORGUNG

Festkörperbatterien und Harvesting

## 12 KILLS / SEKUNDE

mit einem Standard Sturmgewehr

## BIOHYBRIDE WAFFENSYSTEME

## HAUT UND MUSKELN

Selbstheilende Vitrimere, Polymere, künstliche Muskeln

## 100x SCHNELLERE REAKTION ALS DER MENSCH

**EIN ROBOTER DARE KEINEM MENSCHEN SCHADEN ODER DURCH UNTÄTIGKEIT EINEN SCHADEN AN MENSCHEN ZULASSEN.**

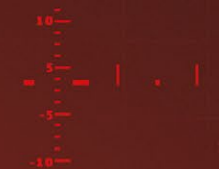
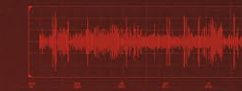
ASIMOV'S ERSTES ROBOTERGESETZ

## GÜNSTIGER ALS EIN SOLDAT

Roboter-Stückpreis sinkt bis 2035 auf ca. **25.000 USD**

DAS WORT „**ROBOTER**“ FEIERTE 1920 PREMIERE IN **KAREL ČAPEK**'S THEATERSTÜCK **R.U.R.** DER BEGRIFF LEITET SICH VOM TSCHECHISCHEN **ROBOTA** AB, WAS ÜBERSETZT „**FRONARBEIT**“ BEDEUTET. DER URSPRÜNGLICHE NAMENSENTWURF WAR ÜBRIGENS „**LABORI**“.

## TARGET: HUMAN BEING - CONFIRMED -



## AEROSOL LEVEL

$10^5/m^3$   
10-RNA-PROBEN ANALYSIERT

## VITALZEICHEN



## MOBILTELEFON

## HR 120 BPM

## SMARTWATCH

## AKUSTISCHE ORTUNG

auf +/- 50 cm genau

## ABSATZ VON INDUSTRIEROBOTERN (Stand 2024)



## ROBOTERDICHTEN IN DER INDUSTRIE

Anzahl Roboter pro 10.000 Mitarbeiter (Stand 2023)



Globaler Durchschnitt: 162

**1,4 MIO. HUMANOIDE EINHEITEN BIS 2035**

**SOLDATEN GEBEN IHREN ROBOTER-KAMERADEN OFT NAMEN, BEFÖRDERN SIE UND VERLEIHEN IHNEN Sogar VERWUNDETEN-ABZEICHEN.**



### 3 ROBOTIK IM KONFLIKT – VOM HELFER ZUM TERMINATOR

Vor einigen Jahren rief das Thema „Roboter“ bei vielen wohl zunächst Bilder des Terminators, von kybernetischen Killern oder Agenten à la Matrix hervor. All diesen Maschinen ist gemein, dass sie die Menschheit ausradieren oder unterjochen wollen, statt ihr zu dienen, wie es ihre Schöpfer im Sinne der Asimov'schen Robotergesetze ursprünglich avisiert hatten [9]. Während die Vorstellung einer feindseligen Technik für lange Zeit pure Fiktion und fern jeder Realität war, ist spätestens seit dem disruptiven Erfolg von ChatGPT allgemein sichtbar und insbesondere erlebbar, wie schnell sich Technologie mittlerweile fortentwickelt und welche immer neuen Möglichkeiten – und damit auch Gefahren – dies eröffnet.

#### Exponentielle Entwicklung

Im Bereich der Robotik erscheinen Meldungen über neu erzielte Fortschritte und Fähigkeiten in immer kürzeren Abständen und eine ganze Reihe konkurrierender Produkte sollen bereits in den nächsten ein bis zwei Jahren auf den Massenmarkt kommen. Gerade humanoide Roboter entwickeln sich in den letzten Jahren mit atemberaubender Geschwindigkeit weiter und werden beispielsweise bereits umfassend in industriellen Fertigungsanlagen getestet. So wurde Ende 2025 für das Modell Figure 02 eine elfmonatige Erprobung im BMW-Werk Spartanburg abgeschlossen. In 10-Stunden Schichten an fünf Tagen pro Woche hatten die Roboter an der Produktion von über 30.000 X3-Fahrzeugen mitgewirkt [136]; die dabei gewonnenen Daten fließen unmittelbar in das Nachfolgemodell Figure 03 ein. Für das laufende Jahr stehen zahlreiche neue Modelle in den Startlöchern, welche nicht nur immer bessere Fähigkeiten haben sollen, sondern durch besonders günstige Einsteigermodelle wie den Unitree G1/R1 auch zu einer schnelleren Verbreitung führen sollen.

Was diese dann tatsächlich können werden, wird immer wieder heftig diskutiert. Schließlich wurde ja schon der eine oder andere Hersteller beim Tricksen erwischt, etwa Tesla, als der Roboter Optimus beim Wäschefalten ferngesteuert wurde. Bei Videos gilt es in Zeiten von generativer KI daher natürlich, genau hinzuschauen und

nicht alles zu glauben. Trotzdem sind die Fortschritte in vielen Bereichen enorm: Blickt man ein wenig genauer auf die Science-Fiction Blockbuster der 80er und 90er Jahre und vergleicht die dortigen „Zukunftsentwicklungen“ mit dem heutigen Stand der Forschung in Laboren, bei Start-Ups und in Universitäten, zeigt sich schnell, dass an vielen von einst unmöglich erachteten Fähigkeiten intensiv gearbeitet wird und schon einiges in experimentellen Umgebungen funktioniert, wenn auch mit stellenweise noch erheblichen Einschränkungen. So haben es Wissenschaftler 2025 beispielsweise geschafft, „innere Sprache“ zu dekodieren und darzustellen [216], ein Schritt Richtung Gedankenlesen wie in „Minority Report“.

Verschiedene Entwicklungen der vergangenen Monate stimmen jedoch nachdenklich, wo wir schon heute stehen. Im Dezember 2025 hat China beispielsweise damit begonnen, humanoide Roboter der Walker S2-Serie an Grenzübergängen in der Stadt Fangchenggang an der Grenze zu Vietnam zu stationieren. Die Roboter sollen dort Patrouillen und Kontrollgänge durchführen, beim Transport von Ausrüstung helfen und bei der Lenkung des Personenflusses an Checkpoints unterstützen [327]. Durch die Fähigkeit des Walker S2, selbständig seine Batterien zu wechseln, ist nahezu ein 24/7-Einsatz möglich – wie er sich im Einsatz bewährt, wird sich zeigen.

#### Future is Now

Auch die Vorstellung und Demonstration des T800, der ganz bewusst nach dem Killerroboter-Vorbild T-800 der Firma Cyberdyne Systems im Film Terminator von James Cameron benannt wurde, zeigt, was technisch bereits machbar ist und wo die Reise hingeht. Dieser humanoide Roboter ist zwar für den allgemeinen Einsatz konzipiert, aber auch speziell zum Kämpfen ausgelegt [109]. Eine Aluminiumlegierung aus der Luftfahrt sowie Magnesiumelemente verleihen ihm besondere Stabilität, während starke Elektromotoren mit 450 nm Drehmoment genug Kraft für schnelle Bewegungen, anspruchsvolle Kampfmanöver und das Heben schwerer Lasten generieren. Durch ein aktives Kühlsystem kann der T800 auch ohne Pausen agieren.



### 3.1 ROBOTIK IN KONFLIKTEN

Gerade in bewaffneten Konflikten ist die Nutzung von Robotertechnologien nichts Neues. Schon im Ersten und Zweiten Weltkrieg wurden mit Sprengstoff beladene, kleine fernsteuerbare Kettenfahrzeuge eingesetzt, um in den feindlichen Schützengräben ohne Gefährdung der eigenen Soldaten Wirkung zu erzielen (z. B. Torpille Terrestre ab 1915, Goliath ab 1942) [99].

An den Frontlinien in der Ukraine übernimmt heutzutage beispielsweise der Ratel S entsprechende Aufgaben. Dieser ist ein ferngesteuerter 4-Rad-Roboter, welcher unter anderem Panzerabwehrminen transportieren kann und zur Bekämpfung von Fahrzeugen und Bunkern eingesetzt wird, ohne eigene Soldaten in der Todeszone zu gefährden – das selbe Prinzip wie bereits beim Einsatz einfacherer Plattformen in den beiden Weltkriegen. Zunehmende Bedeutung haben auch Roboterplattformen wie das Unex-System, welches für den Munitionstransport an die Front sowie den Abtransport Verwundeter von der Front eingesetzt wird [208].

Insbesondere gehört auch die Luft mittlerweile fast ganz den Drohnen. Das Portfolio an der Front hat sich von den vorherrschenden, taktischen First Person View (FPV) Kamikaze-Drohnen um Hexacopter mit schwereren Wirkladungen sowie verschiedenen Aufklärungssystemen und auch strategischen Langstreckendrohnen hoher Reichweite erweitert. Auch im Wasser haben Systeme wie die Magura V5 die Mächtigkeit unbemannter Kleinsysteme demonstriert und durch das Versenken mehrerer russischer Einheiten die Schwarzmeerflotte in die Defensive gezwungen und faktisch wirkungslos gemacht. Kleine, günstige und sich schnell weiterentwickelnde Systeme beherrschen derzeit die Dimensionen Land, See und Luft.

#### Innovation versus staatliche Beschaffung

Die Nutzung und schnelle Weiterentwicklung von Technologie ist somit zentral. Mit Blick auf das veraltete militärische Material zu Beginn der russischen Invasion musste die Ukraine allerdings zunächst Wege finden, langsame Beschaffungswege zu überkommen und die Möglichkeiten schneller industrieller Innovationszyklen zu aktivieren – kein seltenes Problem, liegen die Beschaffungszeiten für militärische Systeme in westlichen Ländern häufig bei zehn Jahren und mehr. Gerade in Deutschland sind Vertragszyklen sogar bis zu 60 Prozent länger als im globalen Schnitt [227].

Um schnell Waffen an die Front zu liefern, bildeten sich in der Ukraine zunächst freiwillige Unterstützerguppen, welche Spenden sammelten, mittels 3D-Druck Drohnenteile hergestellt und diese direkt an die Front geschickt haben. Signal- und Telegram-Kanäle wurden wiederum genutzt, um die Erfahrungen der Truppen unmittelbar in die Weiterentwicklungen einfließen zu lassen. Da freiwillige Spenden jedoch weder garantiert noch skalierbar sind und somit keine verlässliche Planung ermöglichen, schaffte das ukrainische Ministerium für Digitalisierung mittels Entbürokratisierung, geänderten Regeln und der Schaffung finanzieller Anreize die Basis für einen schnellen Aufwuchs: Indem zum Beispiel von Herstellern durchgeführte Tests akzeptiert wurden und keine staatlichen Versuchsdurchläufe oder die im Westen üblichen Zertifizierungen mehr erforderlich waren, konnte die Zeitspanne zur Einführung eines Systems von zwei Jahren auf wenige Wochen reduziert werden. Quantität, niedrige Kosten und Geschwindigkeit waren überlebenswichtiger als Qualität und Prozessstreue.

#### Gamifizierung des Kriegs: Punkte fürs Töten

Weiter beschleunigt werden konnte dies durch den Innovationscluster „Brave1“, welcher zentraler Anlaufpunkt für Firmen und Unterstützer ist. Zur Minimierung von Lieferzeiten und optimaler Ausrichtung am Bedarf der Truppe hat der Cluster unter anderem eine Webseite mit einem Marktplatz eingerichtet, welcher Start-Ups und Hersteller innovativer Lösungen direkt mit den Soldaten an der Front verbindet. Ohne Bürokratie, langwierige Vertragsschlüsse und zeitaufwändige Entwicklung von Produkten, welche bei Auslieferung bereits überholt sind, können Hersteller ihre Lösungen direkt den ukrainischen Streitkräften anbieten, welche diese im Online-Marktplatz wiederum direkt erwerben können [43].

Bezahlt werden kann ganz klassisch, beispielsweise aus verfügbarem Budget oder Spenden, oder auf Basis eines Belohnungssystems mittels „ePoints“. Letztere werden für die per Videoaufnahmen nachgewiesene erfolgreiche Vernichtung von russischem Personal und Material vergeben. Die Punkte können auf dem Brave1-Marktplatz direkt für die Beschaffung neuer Drohnen eingesetzt werden, welche dann in nur wenigen Tagen an die Truppen geliefert werden. Durch die „Gamifizierung“ des Tötens können somit erfolgreiche Einheiten auf Basis ihrer Punkte schnell neue Ausrüstung beschaffen – und dadurch umso besser wirken: Die russischen Verluste hatten sich in den ersten zehn Monaten

nach Einführung des Systems verdoppelt, Tendenz kontinuierlich steigend: Im Dezember waren es über 33.000 Soldaten [8].

Während sich diese schnell anpassende Digitalisierung des Schlachtfeldes direkt in den Zahlen gefallener und verwundeter Soldaten und von zerstörtem Material reflektiert, sind die derzeit eingesetzten Systeme, wie in den Weltkriegen oder beim wäschefaltenden Optimus, typischerweise noch immer ferngesteuert und autonome Funktionen sehr eingeschränkt. Im Ukrainekrieg werden schätzungsweise weniger als ein Prozent der als „autonom“ vermarkteten Technologien wirklich entsprechend eingesetzt [13].

Einzelne Systeme wie das TFL-1 von The Fourth Law, welches eine autonome Übernahme der Flugsteuerung und den Endanflug aufs Ziel auch bei Störung oder Abbruch des Funksignals auf optischer Basis ermöglicht und einfach in gängige Plattformen integriert werden kann, stechen aber hervor. Da ein Modul für lediglich knapp 50 Euro (oder mittels ePoints) auf Brave1 erhältlich ist und die Trefferquoten an der Front dadurch bereits deutlich gesteigert werden konnten, werden Weiterentwicklungen und neue, sophistiziertere Module nicht lange auf sich warten lassen.

#### Vorteil durch Geschwindigkeit

Wie technologisch fortgeschritten heutige Roboter teilweise schon sind, zeigt aber ein Blick auf den Krieg in Israel und Gaza, der auch als „erster Roboterkrieg“ bezeichnet wird [203].

Um die komplexe Situation zu beherrschen und möglichst schnell agieren zu können, wurde zum einen im Vorbereitungsbereich ein hoher Grad an Automatisierung zur Identifizierung von Zielen und gegnerischen Schlüsselfiguren genutzt. Allerdings können sich dadurch auch gefährliche Routinen und eine sinkende Qualität der menschlichen Überwachung und Kontrolle einschleichen. So hat beispielsweise das von den israelischen Verteidigungsstreitkräften (Israel Defense Forces, IDF) im Gazakrieg zur Identifizierung von Zielen genutzte KI-System „Lavender“ gemäß Berichten zu einer äußerst schnellen, jedoch ungenauen Kontrolle der maschinengenerierten Vorschläge und somit erheblichen Kollateralschäden geführt [341].

Entscheidender Wendepunkt in der Nutzung von militärischer Robotik war deren Einsatz nicht nur als Aufklärungssystem, sondern zur Durchführung aktiver Kampf- und Pionieraufgaben in dicht besiedelten, urba-

nen Räumen mit dem Ziel, eigene Verluste zu minimieren. Die IDF haben hierfür unter anderem den Caterpillar D9 genutzt, welcher mit schwerer Panzerung für die Auslösung von Sprengfallen, Räumung von Minenfeldern und Trümmerbarrieren auch in engen Gassen eingesetzt wird. Das semi-autonome Bodenfahrzeug Jaguar geht noch einen Schritt weiter und wird insbesondere für die Grenzsicherung und zum Perimeterschutz eingesetzt: Ausgestattet mit einem 7,62-mm-Maschinengewehr und hochauflösender Sensorik kann es autonom navigieren, Hindernissen ausweichen und Patrouillenwege abfahren. Eine selbstständige Zielbekämpfung ist derzeit noch nicht vorgesehen – die Sensoren können ein Ziel automatisch erkennen und verfolgen (sogenannter „Lock-On“), der Feuerbefehl muss allerdings durch einen Menschen nach Begutachtung des Videobildes in der Einsatzzentrale erfolgen (Human-in-the-Loop).

#### Human-in-the-Loop oder autonom: wenige Zeilen Code

Der Schritt von der Feuerfreigabe durch einen Operateur zu einem vollautonom agierenden System sind hier aber nur wenige Zeilen Code. Es ist keine technische Frage mehr, entsprechende Roboter zu bauen – es ist eine rein ethische und doktrinaire, solche Funktionalität zu aktivieren und zu nutzen.

Mit Blick auf weitere Entwicklungen ist es daher nur eine Frage der Zeit, bis auch vollautonome, bewaffnete Roboter zum Einsatz kommen. Die Vorteile sind für viele Militärs weltweit attraktiv. Die 72. Heeresgruppe der Volksbefreiungsarmee Chinas (People's Liberation Army, PLA) hat in einer Anlandeübung beispielsweise bereits die Integration von sogenannten „Robot Wolves“ geübt, welche unter anderem als bewaffnete Begleitsysteme für die Infanterie Gassen durch Strandhindernisse geschaffen und gegnerisches Feuer abgefangen haben [202]. Die fortgeschrittene Koordination der Übung lässt darauf schließen, dass China auch doktrinär die Integration von Manned/Unmanned Teaming (MUM-T) zügig vorantreibt.

Die humanoiden Roboter in Fangchenggang sind entsprechend nicht nur als Machbarkeitsstudie und Ende der Entwicklung zu verstehen. Im Gegenteil, sie zeigen vielmehr, wie schnell sich der Bereich humanoider Roboter, insbesondere unter der Einwirkung von KI, Werkstoffkunde, Bioinformatik und Chemie weiterentwickelt. Dual-Use wird zum Standard.

Wird ein Terminator-Szenario damit immer wahrscheinlicher? Ein kompletter Überblick – von Kopf bis Fuß des humanoiden Roboters – mit Erörterung des jeweiligen Entwicklungsstandes und erwartbarer Fortschritte soll diese Frage beantworten.

### 3.2 TERMINATOR – STAND DER TECHNIK UND MÖGLICHKEITEN

Die zahlreichen Produktdemonstrationen humanoider Roboter stellen die schon heute verfügbaren Fähigkeiten dar. Ein genauerer Blick auf den Stand der Wissenschaft zeigt aber, dass sich alle für den Terminator erforderlichen Elemente rasant weiterentwickeln.

#### 3.2.1 Das Gehirn

Der tatsächliche Grad der Autonomie ist sicherlich noch einer der schwierigsten und umstrittensten Punkte aktueller Roboter. Auch wenn einige Unternehmen die Fakten mit Blick auf die Aktienkurse gern mal etwas flexibler auslegen und die eine oder andere Tech-Demonstration eine ferngesteuerte Kontrolle hatte, gibt es gerade auf dem Gebiet der Datenverarbeitung oder des „Gehirns“ des Roboters rasante Entwicklungen. Die kognitive Architektur [301], welche derzeit noch ein stark limitierender Faktor für die tatsächliche Autonomie von Robotern ist, macht immense Fortschritte und Fernsteuerungen werden schon bald der Vergangenheit angehören. Und dies nicht nur in relativ einfachen Fabrikumgebungen, sondern auch unter komplexen Umweltbedingungen.

Möglich wird dies weniger durch die Weiterentwicklung *klassischer Prozessoren*, als vielmehr einer Reihe neuer Technologien. *Photonik* kann gerade im Bereich der KI-Beschleuniger neue Leistungsklassen erreichen, der wirkliche Leistungsschub kommt aber durch *Spiking Neural Networks*, *neuromorphe Sensoren* und *Edge Analytics* sowie den Möglichkeiten durch *Wetware*.

#### Möglichkeiten und Limitierungen klassischer Prozessoren

Über Jahrzehnte erfolgreiche Konzepte klassischer Digitalrechner wurden zwar immer weiter optimiert, stoßen heutzutage durch deutlich höhere Datenmengen und Rechenanforderungen aber zunehmend an ihre Grenzen, sowohl bezüglich Geschwindigkeiten, als auch

energetisch. Da die Berechnungen von KI-Modellen in hohem Maße auf einigen bestimmten mathematischen Operationen beruhen, konnten für diesen Bereich zunächst nochmal deutliche Leistungssteigerungen erzielt werden, da genau diese Funktionen in KI-Chips in Hardware gegossen werden. Architekturen wie beispielsweise NVIDIAs Blackwell nutzen daneben noch weitere Möglichkeiten, indem beispielsweise die Reduzierung der Genauigkeit von Berechnungen reduziert wird, ohne dass dies Auswirkungen auf das Ergebnis hat. Dies generiert höhere Geschwindigkeiten und bessere Effizienz: Die Nutzung eines speziell für physische KI und Robotik entwickelten NVIDIA Jetson Thor, mit maximal 2070 TeraFLOPS (TFLOPS) ermöglicht beispielsweise im T800 ein verzögerungsfreies Verarbeiten komplexer Bewegungsabläufe und visueller Daten.

Entscheidend ist jedoch, dass die gesamte Datenerfassung und -verarbeitung künftig nicht mehr konzentriert in einer zentralen Recheneinheit erfolgen wird, welche sämtliche Datenströme kontinuierlich verarbeitet. Aktuell ist dies noch ein Hauptgrund für den wenig effizienten Energiehaushalt von Robotern: So muss für die visuelle Wahrnehmung ein konstanter Bilderstrom verarbeitet und per KI-Algorithmen ausgewertet werden. Mittels spezialisierter Prozessoren wie des Jetson Thor ist dies zwar auch heute schon in Echtzeit problemlos möglich – verbraucht aber unnötig viel Energie: Denn auch die Feststellung, dass *nichts* passiert, belastet die Batterie. Zwar ist der Jetson Thor mit einer Leistungsaufnahme von 130 Watt relativ sparsam, die Einsatzdauer eines autarken Roboters wird dadurch aber trotzdem spürbar beeinflusst, auch wenn die Aktuatoren und somit der Bewegungsapparat des Roboters die Hauptverbraucher sind. Mit einer Reduzierung der Leistungsaufnahme des Prozessors wäre bei aktuellen Modellen aber durchaus eine Laufzeitsteigerung von knapp 25 Prozent beziehungsweise einer Stunde möglich.

#### Spezialisierte Photonikprozessoren

KI-Berechnungen können aber auch sehr schnell und effizient mittels Photonik durchgeführt werden. Statt Elektronen kommen dabei Lichtstrahlen zum Einsatz. Ein weiterer Vorteil dabei ist, dass sie kaum Kühlung benötigen. Ein 16-Kanal-Prozessor mit einer Leistung von 1,28 Billionen Operationen pro Sekunde wurde bereits im letzten Jahr vorgestellt [351] und auch entsprechende kommerzielle Prozessoren sind schon verfügbar. In den nächsten Jahren ist mit einer weiteren deutlichen Leistungssteigerung und Miniaturisierung zu rechnen. Der derzeitige Flaschenhals der Technologie ist die Notwendigkeit, elektronisch vorliegende Da-

ten für die Berechnung zunächst in Licht umzuwandeln und das Ergebnis wieder zurückzuwandeln. Dies geht nicht nur zulasten der Gesamtgeschwindigkeit, sondern benötigt insbesondere auch relativ viel Energie [166], womit die Effizienz der eigentlichen Berechnung wieder zunichtegemacht wird. Derzeit lohnt sich der Einsatz von Photonik energetisch erst bei großen Matrizen und hohen Taktraten über 10 GHz, ansonsten sind digitale ASICs noch im Vorteil. Der Einsatz ist daher insbesondere auch in Bereichen interessant, in denen die Daten ohnehin als Licht vorliegen, wie beispielsweise in Glasfasernetzen.

#### Neuromorphe Sensoren und Edge Analytics

Aufgrund der bisherigen Limitierungen werden künftige Systeme genau wie beim natürlichen, menschlichen Vorbild massiv dezentral arbeiten. Edge Computing, was beispielsweise im Bereich von Mobilfunknetzen schon zunehmend Verbreitung findet, ist hier ein Stichwort. Vergleichbar dem menschlichen Reflexsystem werden Aktionen, soweit möglich, lokal und nicht im „Gehirn“ verarbeitet. Vielmehr werden Detektion und Reaktion direkt in den jeweiligen Roboterteilen durchgeführt und es wird nur eine Information über den Vorgang an das Roboterhirn übersandt (sogenanntes Edge Analytics). Neben einer Reduzierung des Rechenaufwands in der zentralen Recheneinheit ermöglicht dies insbesondere auch sehr viel schnellere Reaktionszeiten im Millisekundenbereich – essenziell für die Überlegenheit des Terminators.

Um Edge Analytics wirkungsvoll umzusetzen, werden unter anderem neuromorphe Sensoren zum Einsatz kommen. Diese versuchen, die Wahrnehmungs- und visuellen Verarbeitungseigenschaften lebender Organismen nachzuahmen. Indem nur die für die Nachbearbeitung relevanten Informationen extrahiert werden, reduziert sich der erforderliche Rechenaufwand erheblich [112]. Dass der künftige Terminator entsprechende, weit fortgeschrittene Sensorik an Bord hat, steht außer Frage: Start-Ups bieten schon heute entsprechende Module an, welche Reaktionszeiten unter 100 Mikrosekunden bei minimaler Stromaufnahme haben [281]. In den nächsten Jahren ist mit der zunehmenden Integration von Neuromorphic Processing Units (NPU) in Ergänzung zu den heutigen CPUs und GPUs zu rechnen. Gerade im IoT sowie Mobilfunkbereich sind die Möglichkeiten von „Always-On“ Sensoren mit minimaler Energieaufnahme enorm, was die Kommerzialisierung und schnelle Verbreitung massiv beschleunigen wird.

#### Spiking Neural Networks

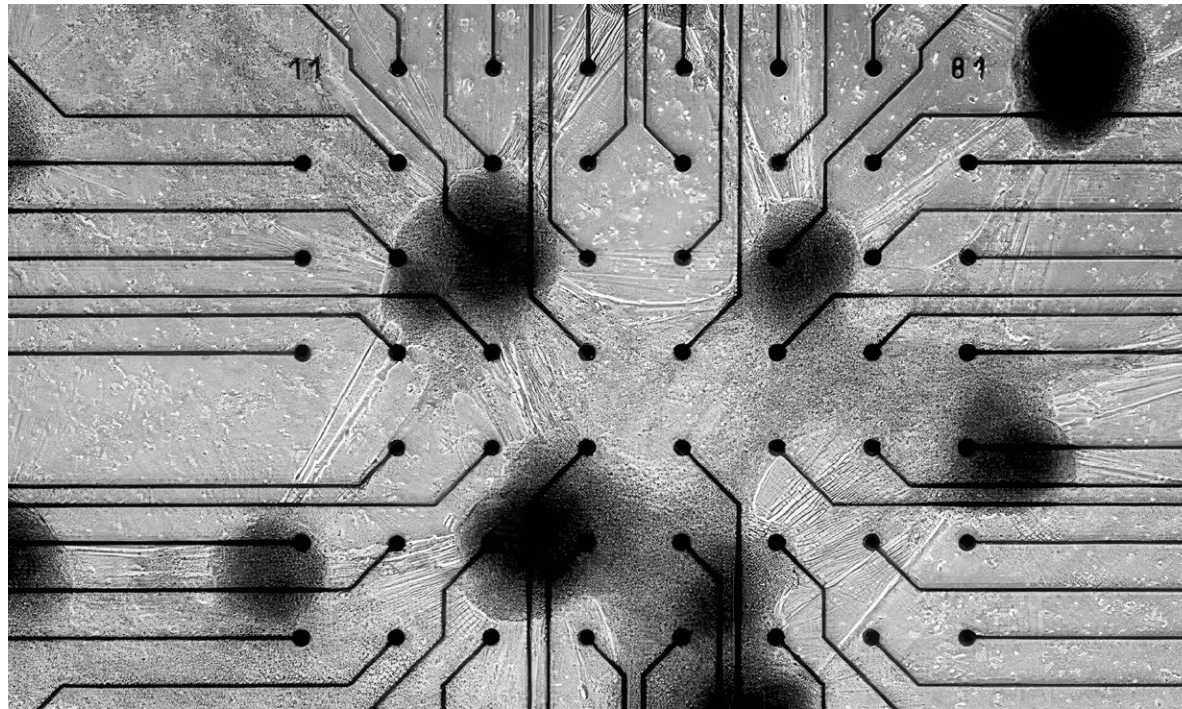
Neben einer geeigneten Verteilung von Rechenaufgaben ist mit neuromorphem Computing aber noch viel mehr mit Hinblick auf das zentrale Gehirn des Roboters möglich. Logische Verarbeitung und Datenspeicherung werden hierbei in künstlichen Neuronen und Synapsen vereint. Dies ermöglicht eine signifikante Verbesserung der Energieeffizienz, wodurch auch ressourcenintensive KI-Aufgaben mit geringer Latenz direkt auf batteriebetriebenen Endgeräten ausgeführt werden können [154], zum Beispiel durch die Nutzung von Spiking Neural Networks (SNN). Im Gegensatz zu klassischen künstlichen neuronalen Netzen (Artificial Neural Network, ANN), die auf Signalen mit kontinuierlichen Werten basieren, arbeiten SNNs energiebasiert. Ein künstliches Neuron „feuert“ (sendet einen Spike) nur dann, wenn der Schwellenwert eines oder mehrerer bestimmter Eingangssignale überschritten wird. Dies führt zu einem deutlich reduzierten Energieverbrauch, denn bei statischen Sensordaten (Ruhestadium) wird nahezu kein Strom benötigt. Auch komplexe Operationen, wie die Unterscheidung zwischen einem Zivilisten und einem Kombattanten, können sehr viel effizienter und schneller durchgeführt werden.

Daneben sind neuartige Memristoren auf dem Weg. Statt der üblichen Verarbeitung digitaler Signale kann die Nutzung analoger Signale den Energiebedarf um bis zu 99 Prozent senken. Die Technologie ermöglicht weiterhin auch Selbstheilungseffekte. Damit könnte das analoge Rechnen ein Comeback feiern, nachdem entsprechende Systeme in den 60er und 70er Jahren fast vollständig durch die günstigeren und genaueren Digitalrechner verdrängt wurden. Zwar ist die Genauigkeit der Analogtechnik seither nicht sehr viel besser geworden, aber für KI-Berechnungen muss diese eben nicht sehr hoch sein. Somit kann diese Technologie nicht nur ein Revival erleben, sie kann sogar ein Kernstück der Datenverarbeitung im Terminator werden – obwohl sie noch älter ist als der Originalfilm.

#### Assimiliert: Wetware Computing

Aber nicht nur neuromorphes Computing schaut sich die Lösungen der biologischen Evolution ab, auch die Möglichkeiten und Effizienz des menschlichen Gehirns selbst sind seit vielen Jahrzehnten intensiver Forschungsgegenstand. Unter „Wetware Computing“ versteht man innovative Ansätze, mittels lebender biologischer Gewebe Rechenaufgaben auszuführen. Die Menge vielversprechender Anwendungsfälle ist aber sehr viel breiter: Brain-on-a-Chip ist nur eine Möglich-





Quelle: [187]

**Abbildung 20: Menschliche Neuronen auf Siliziumchip. Cortical Labs.**

keit von Organ-on-a-Chip (siehe Abbildung 20) [223]. Derzeit münden die Fortschritte der letzten Jahre in die ersten Prototypen, welche zum Beispiel im Labor gezüchtete menschliche Gehirnzellen mit Siliziumchips verschmelzen.

Dadurch können Informationen auf ähnliche Weise wie im menschlichen Gehirn in Echtzeit verarbeitet werden, bei einem sehr viel geringeren Energieverbrauch als bei anderen Architekturen wie GPUs und KI-Beschleunigern, oder auch den komplexen Systemanforderungen von Quantenrechnern. Bei bestimmten, wenn auch nicht allen, Aufgaben wird durch die Nutzung von Wetware ein bis zu  $10^6$ -fach geringerer Energieverbrauch im Vergleich zu digitalen Prozessoren erwartet [137].

Für die „geistigen“ Fähigkeiten des Roboters kann dies einen gewaltigen Schritt nach vorne bedeuten. Bei einem Experiment in 2022 lernten Neuronen innerhalb weniger Minuten, den Klassiker „Pong“ zu spielen [91]. Diese grundlegende Demonstration hat bereits erste kommerzielle Systeme, noch fokussiert auf den Forschungsbereich, hervorgebracht. Biologischen Netzwerke können Algorithmen des Deep Reinforcement Learning in Bezug auf die Lerneffizienz übertreffen [187]. Für den Terminator bedeutet dies in Zukunft, dass mittels Wetware Computing energieeffiziente Informationsverarbeitung in Echtzeit möglich wird und der Roboter auch in neuen und unbekannten Umgebungen schnell lernen sowie sich zurechtfinden und anpassen kann.

Von besonderer Bedeutung ist in diesem Kontext auch, dass im Gegensatz zur klassischen IT die Datenverarbeitung in solchen Systemen *nicht* deterministisch ist. Dies bedeutet, dass derselbe Input und scheinbar identische Startbedingungen eben *nicht* zu exakt demselben Output führen müssen. Während dies für Digitalrechner inakzeptabel wäre, ist es eine Kerneigenschaft lebender neuronaler Netze, mit den dadurch verbundenen Vorteilen wie Generalisierbarkeit, Robustheit und explorativem Verhalten. Die Kehrseite ist, dass gerade in den Bereichen Spezifikation, Test und Betrieb ein höherer Aufwand betrieben werden muss und „Safety Engineering“ eine noch bedeutendere Rolle erhält. Insbesondere, wenn man verhindern will, dass die Systeme ein ungewolltes Eigenleben entwickeln.

Für den künftigen Terminator ist davon auszugehen, dass ganz im Sinne des Edge Analytics Ansatzes eine Kombination verschiedener Technologien zum Einsatz kommen wird, welche die jeweiligen Vorteile ausschöpfen und durch geeignete Auswahl und Integration limitierende Faktoren minimieren.

### 3.2.2 Die Energieversorgung

Neben dem Ziel einer deutlichen Leistungssteigerung steht insbesondere auch die Energieeffizienz im Zentrum der Forschung. Die Energieversorgung ist derzeit eine der größten Limitierungen humanoider Roboter. Grundsätzlich kann die Energie lokal im System *gespeichert* oder *generiert*, oder per *Drahtlostechnologie* übertragen werden.

Für die lokale Speicherung und Erzeugung bieten sich nicht nur *Batterien* an, sondern auch neue Möglichkeiten durch *Bio-Elektrochemische Systeme (BES)*, *Radionuklidbatterien* und *Betavoltaik* sowie mittels des *Energy-Harvestings* – der Energiegewinnung direkt aus der Umgebung. Aber auch die *Nahfeldübertragung* beispielsweise mittels Induktion oder Fernfeldübertragung mittels *Funkwellen* oder *Laserstrahlen* können neue Wege der Energieversorgung sein.

### Entwicklung der Batterietechnologie

Bei Speicherung mittels *Batterien* sind typischerweise nur wenige Stunden Einsatz möglich – dies kann für Aufgaben in Fabriken, Geschäften oder auch im privaten Bereich, wo sich Arbeits- und Ladezyklen abwechseln können, völlig ausreichend sein. Auch demonstrieren Modelle wie der Walker S2 bereits die Fähigkeit, die eigenen Batterien autonom in unter drei Minuten zu wechseln, was einen nahezu unterbrechungsfreien Einsatz bei entsprechender Infrastruktur ermöglicht. Ein Kampfroboter wäre mit derart kurzen Laufzeiten oder dem Bedarf für „Betankungsstationen“ aber nicht praxistauglich.

Blickt man auf die Entwicklungen im Bereich der E-Mobilität, zeigen sich jedoch einige Fortschritte bei den Batteriekapazitäten. Lithium-Ionen-Akkus haben eine Energiedichte auf Systemebene von bis zu 250 Wh/kg [100], welche durch Nutzung von anderem Kathoden- und Anodenmaterial deutlich erhöht werden kann [242]. Bei den in Einführung befindlichen und auch im T800 genutzten Festkörperbatterien steigt dieser Wert auf bis zu 500 Wh/kg an. Diese haben auch den Vorteil, dass sie nicht entflammbar sind – ein wichtiger Aspekt, insbesondere für einen Kampfroboter.

Einen noch größeren Schritt könnten Lithium-Luft ( $\text{Li-O}_2$ ) Batterien machen. Deren theoretische Energiedichte ist mit bis zu 11 kWh/kg bis zu 30-mal höher als die von derzeitigen Lithium-Ionen-Akkus, die technische Serienumsetzung steht aber vor vielen Herausforderungen [307] und dürfte noch über ein Jahrzehnt dauern.

### Lokale Energieerzeugung

Für die lokale Energieerzeugung im Roboter könnten grundsätzlich auch *BES* genutzt werden, welche biologische Abfälle direkt in elektrische Energie umwandeln [360]. Auch *Radionuklidbatterien*, welche die beim Zerfall von Alpha-Strahlern entstehende Hitze ausnutzen

und *Betavoltaik*, bei der die kinetische Energie von Beta-Teilchen in elektrische Energie umgewandelt wird, wären denkbar. Allerdings wird die Anwendbarkeit solcher Systeme sehr eingeschränkt bleiben: BES haben eine sehr geringe Leistungsdichte, die Technologie ist eher für die Selbstversorgung von Kläranlagen geeignet.

Natürliche Strahler wiederum haben eine jahrzehntelange Haltbarkeit und eine bis millionenfach höhere Energiedichte als Lithium-Ionen-Akkus, geben diese Energie aber nur sehr langsam über einen Zeitraum von Jahrzehnten ab. Eine Radiovoltaik-Batterie mit 100 mW [343] könnte aber beispielsweise die Erhaltungsladung eines schlafenden, vorpositionierten Systems unterstützen („Loitering Weapon“).

Dieselben Einschränkungen gelten auch für die Verfahren des *Energy-Harvestings*, also des Nutzbarmachens von Energie, welche in der Umgebung inhärent vorliegt. Aufgrund der geringen Leistung wird auch dies im Bereich von spezieller Sensorik verortet bleiben [305].

Neben der lokalen Speicherung und Erzeugung von Energie kann diese auch über *Drahtlostechnologien* bereitgestellt werden, welche wiederum in *Nah-* und *Fernfeldverfahren* unterteilt werden können.

### Drahtlostechnologien im Nahfeld

Im *Nahfeld* haben sich Verfahren zum kontaktlosen Laden schon seit längerer Zeit in den Alltag integriert, beispielsweise das induktive Laden von Smartphones oder Zahnbürsten. Auch im Bereich von Industrierobotern kommen entsprechende Systeme – mit deutlich höherer Leistung – zunehmend zum Einsatz. Über Spulen im Boden kann Energieübertragung im zweistelligen kW-Bereich bei Wirkungsgraden bis über 90 Prozent erfolgen. Die entsprechenden Anwendungen erfordern jedoch physikalische Parameter wie Luftspalte zwischen Boden und Fahrzeug von einigen Milli- bis wenigen Zentimetern [186].

Mit Blick auf nachhaltige Transportsysteme sind auch Teststrecken für dynamisches Drahtlosladen von E-Fahrzeugen in Erprobung, welche beispielsweise mit Leistungen bis über 200 kW Lkws mit Geschwindigkeiten von 100 km/h erfolgreich laden können [243].

Aber auch im Falle, dass beispielsweise wichtige Haupttransitverbindungen oder Straßennetze im urbanen Bereich entsprechend ausgestattet sein werden, wird sich der Terminator kaum auf einer vielbefahrenen Straße aufladen, um im nächsten Moment von einem 60-Tonner



überfahren zu werden. Nahfeldtechnologien können jedoch trotzdem nützlich werden. Im Bereich von Drohnen wurde demonstriert, wie sich diese an Hochspannungsleitungen hängen können, um die Akkus aufzuladen [171]. Somit können Inspektionsdrohnen auch lange Hochspannungstrassen autark abfliegen, ohne auf den Wechsel von Akkus angewiesen zu sein. Auf ähnliche Weise könnte sich ein Roboter über längere Distanzen fortbewegen, indem er sich an entlegenen Stellen lädt und im Falle einer Entdeckung entsprechende Protokolle aktiviert.

In künftigen Kommunikationsnetzen wie 6G wird weiterhin mittels *Power Beaming* auch gezielt Leistung an Geräte übertragen werden [306]. Dies kann zwar eine interessante Energiequelle darstellen, wird für die Versorgung eines Kampfroboters aber auch nicht ausreichend sein und wäre ohne ausreichende eigene Kontrolle der Infrastruktur insbesondere im Feindesland auch zu unzuverlässig.

### Drahtlostechnologien im Fernfeld

Um Energie drahtlos über größere Distanzen zu übertragen, reicht die induktive, magnetische oder kapazitive Kopplung nicht aus: Dort kommen *Fernfeldtechnologien* zum Einsatz, welche elektromagnetische Strahlung in Form von Funk- (bis 300 MHz) beziehungsweise Mikrowellen (300 Mhz bis 300 GHz) oder in höheren Frequenzbereichen durch optischer Strahlung (THz) [286] nutzen.

*Funkwellen* bieten den Vorteil, allgegenwärtig zu sein, denn deren geradlinige Ausbreitung ändert bei Hindernissen ihren Verlauf. Somit kann Energie über einen großen Bereich und auch an unzugänglichen Orten gewonnen werden. Die geringe Leistungsdichte von Funkwellen reduziert jedoch die Einsatzmöglichkeiten. Gleichrichterantennen und Demonstrationen von Übertragungen im unteren Watt-Bereich [302] deuten an, was künftig erwartet werden kann. Insbesondere im Bereich von Industrie 4.0 und Smart Homes wird hierdurch auf Batterien verzichtet werden können [309]. Mittels der Nutzung von Mikrowellen sind höhere Leistungen möglich, aufgrund der geradlinigen Ausbreitung ist typischerweise jedoch eine Sichtverbindung (Line of Sight, LOS) erforderlich. Die Versorgung humanoider Roboter ist damit denkbar, aufgrund der erforderlichen Leistungen aber beschränkt auf entsprechende Fabrikanlagen und abgeschlossene Bereiche und nicht geeignet für den Terminator.

Eine weitere Möglichkeit der Fernübertragung besteht in der Nutzung von *Laserstrahlung*. In jüngerer Zeit wurden mehrfach Rekorde bezüglich Übertragungsdistanzen und -leistung erzielt [92]. Die noch immer sehr geringe Effizienz ist jedoch weiterhin eine Herausforderung und auch bei optischen Verfahren ist eine LOS erforderlich [340]. Langfristig könnten Photovoltaikanlagen in der geostationären Umlaufbahn eine kontinuierliche Energieübertragung per Laser zu Empfangsstationen auf der Erde ermöglichen [253].

Auf diese Weise könnte auch der Terminator versorgt werden, allerdings müsste ein großer Teil seiner Oberfläche, beispielsweise die Rückenpartie, für das Empfangsarray vorgesehen werden.

Gerade bei dynamischen Bewegungen wäre aber eine kontinuierliche Beleuchtung kaum möglich, ganz abgesehen von Operationen im urbanen Umfeld. Hat der Terminator eine Photovoltaikfläche von 0.2m<sup>2</sup> auf dem Rücken, wäre ein Laserstrahl mit 5000 W/m<sup>2</sup> für eine kontinuierliche Versorgung erforderlich. Dies wäre zum einen weit über den für den Menschen sicheren Grenzwerten, die permanente Illumination des Terminators würde ihn aber auch deutlich einfacher detektierbar machen.

Auch wenn verschiedene Technologien in Entwicklung sind, die eigene, autarke Energieversorgung wird entscheidend für den Terminator bleiben.

### 3.2.3 Die Extremitäten

*Arme, Beine und Hände* sind elementar für einen humanoiden Roboter und die Basis dafür, dass der Terminator seinen Auftrag ausführen kann. Der Antrieb humanoider Roboter wird heutzutage fast ausschließlich durch *Elektromotoren* sichergestellt, welche kontinuierlich weiterentwickelt werden. Pneumatische, mittels Druckluft angetriebene Aktuatoren in aktiven Exoskeletten sind mit Blick auf Ausdauer für einen Terminator nicht geeignet und wurden bezüglich Leistung von leistungsfähigen Elektromotoren überholt. Daneben sind aber noch alternative Verfahren im Bereich *Soft Robotik* und elektrostatische Konzepte in der Erforschung.

#### Leistungsfähigkeit von Elektromotoren

Für eine hohe Leistungsdichte kommen heutzutage vornehmlich Permanentmagnet-Synchronmotoren und bürstenlose *Gleichstrommotoren* zum Einsatz. Diese arbeiten in speziell für Exoskelette und Robotik konzi-

pierten Systemen mit präzisen Planetengetrieben als Quasi-Direktantriebsmotoren. Durch das hohe Drehmoment sowie minimales Spiel wird eine präzise und reaktionsschnelle Bewegungssteuerung ermöglicht. Das sehr niedrige Getriebeverhältnis (Quasi-Direkt) ermöglicht es dem Roboter weiterhin, durch die Messung des Motorstroms äußere Kräfte zu „spüren“, was auch ohne aufwändige Drehmomentsensoren ein dynamisches Laufen ermöglicht [278].

Gerade in der jüngeren Zeit haben die gestiegenen Leistungsdaten der Elektromotoren beeindruckende Demonstrationen ermöglicht, beispielsweise des neuen Atlas Roboters von Boston Dynamics oder des Unitree H1, welcher durch die enorme Drehmomentdichte von 360 nm an den Gelenken einen Rückwärtssalto vorzeigen konnte. Indem modellbasierte Regelungen durch Ansätze des bestärkenden Lernens (Reinforcement Learning) ersetzt wurden, können Roboter mittlerweile neue und viel natürliche Bewegungen durchführen [334] und auch aus den Beobachtungen von Menschen lernen [54].

#### Weiche Roboter, künstliche Muskeln und Hybridsysteme

Trotz der markanten Fortschritte im Bereich des Motorenbaus bleiben diese im Vergleich zum biologischen Vorbild aber schwerer und energiehungriger. Die Forschung beschäftigt sich unter dem Stichwort *Soft Robotik* allerdings schon geraume Zeit mit der Fragestellung, wie Roboter von Natur aus mittels weichen oder dehnbaren Materialien wie Silikonkautschuk, die sich verformen und einen Großteil der bei einer Kollision entstehenden Energie absorbieren können, gebaut werden können. Solche „weichen“ Roboter haben eine kontinuierlich verformbare Struktur mit muskelähnlicher Antriebskraft, die biologische Systeme nachahmt und im Vergleich zu regulären Robotern mit hartem Körper typischerweise auch eine höhere Anzahl von Freiheitsgraden aufweist [292].

Ein Ziel der Soft-Robotik-Forschung ist die Entwicklung biologisch inspirierter *künstlicher Muskeln*, um herkömmliche Motoren künftig zu ersetzen. Elektroaktive Polymere verändern beim Anlegen einer elektrischen Spannung ihre Form und lassen sich somit auch als Aktoren nutzen. Sie sind mit unterschiedlichen Wirkungsmechanismen verfügbar, manche davon sind schon seit den 1990ern Untersuchungsgegenstand [272]. Da bei diesem Ansatz allerdings sehr hohe Spannungen erforderlich sind, ist er für die Nutzung in humanoiden Robotern derzeit nur bedingt geeignet.

Selbiges gilt grundsätzlich für sogenannte Hydraulicly Amplified Self-healing Electrostatic (HASEL)-Aktoren, welche *hydraulische und elektrostatische Konzepte* vereinen und eine hohe Leistungsfähigkeit versprechen [1], aber ebenfalls noch mittels Hochspannung betrieben werden müssen. Bei HASEL wird mittels elektrostatischer Kräfte eine Flüssigkeit in einem weichen Beutel verdrängt, was zu einer Kontraktion führt. Vorteile sind unter anderem, dass die Geschwindigkeit der Elektrik mit der Kraft der Hydraulik kombiniert werden kann und das geschlossene System keine Pumpen benötigt. Auch hier ist, wie im Falle der Quasi-Direktmotoren, eine Eigenüberwachung möglich, so dass auf aufwändige Hochspannungsmessensorik verzichtet werden kann [289]. Weiterhin ermöglicht die Flüssigkeit bei Beschädigungen einen Selbstheilungseffekt – ideal für einen Terminator. Erste Produkte sind von Spin-Offs bereits kommerziell erhältlich, allerdings noch nicht für schwere Lasten.

Was die Technologie aber noch interessanter für die Integration in humanoide Roboter machen könnte, ist der derzeitige Forschungsschwerpunkt, die für den Betrieb erforderlichen Spannungen deutlich zu reduzieren. So konnten bei Hydraulically Amplified Low-Voltage Electrostatic (HALVE) muskelähnliche Leistungskennwerte bei einer fünfmal geringeren Ansteuerungsspannung (1100 Volt) erzielt werden [164]. Durch das aktive Vortreiben und Fortschritte in bisher limitierenden Bereichen kann davon ausgegangen werden, dass in knapp zehn Jahren modulare Muskelpakete in den Terminator integriert werden können – ein Gamechanger, da dies auch Selbstheilungseffekte eröffnet.

#### Die Hände

Die menschlichen *Hände* sind aufgrund ihres komplexen Aufbaus, der Fähigkeit, Kraft und Präzision zu vereinen und ihres hochentwickelten Tastsinns ein universelles Werkzeug, das nur schwer nachzubilden ist. Zuverlässige, genau gesteuerte Hände mit taktiler Manipulation sind für die Robotik noch eine Herausforderung, aber es konnten in letzter Zeit wesentliche Fortschritte erzielt werden. Die Geschicklichkeit, auch mit verformbaren Objekten und in engen Toleranzen zu arbeiten, wurde bereits spürbar verfeinert [354].

Die Verfügbarkeit taktiler Sensorik mit hohen Auflösungen [355] sowie die Implementierung multimodaler taktiler Sensorfelder, welche neben Kontaktkräften auch Mikrovibrationen sowie Wärmeströme messen können hat die Möglichkeiten, auf unbekannte, nicht vorprogrammierte Situationen wie beispielsweise das

Entgleiten eines Gegenstandes aus der Hand zu reagieren, deutlich verbessert. Dafür steigen allerdings auch die Anforderungen an die Sensorik, die vorhandenen Freiheitsgrade sowie die zu verarbeitende Datenmenge [284].

Ein Tastsinn ähnlich dem des Menschen, der eine elementare Funktion hat, um kurzfristige Korrekturen bei unvorhergesehenen Veränderungen zu initiieren, welche durch die optischen und andere Sensoren nicht aufgenommen werden können [225], ist daher von besonderer Bedeutung. Fortschritte im Bereich von Hydrogel-Membranen ebnet den Weg in Richtung entsprechender Ganzkörper-Tastsensorik, indem die „Haut“ aus einem einzigen, leitfähigen Material konstruiert wird, welches verschiedene Reizarten erfassen kann (sogenannte Electrical Impedance Tomography, EIT). Hierbei wird nicht mehr eine hohe Anzahl von Sensorelementen mit aufwändiger Verkabelung benötigt, sondern es werden Elektroden an wenigen Stellen wie beispielsweise den Handgelenken integriert, welche aufgrund von Spannungsmessungen die Veränderung der Leitfähigkeit mittels Druck, Dehnung oder Beschädigung erkennen und lokalisieren können [168]. Aufgrund der Elastizität des Materials ist es insbesondere auch für Soft Robotics geeignet.

Jüngere Arbeiten haben zudem demonstriert, wie humanoide Roboter auch ein Schmerzempfinden über ihre Haut bekommen, so dass sie auf entsprechende Reize reagieren können. Die sogenannte neuromorphe Roboter-E-Haut (NRE-Haut) kodiert dynamische taktile Reize in neuronale Impulsfolgen und verfügt über eine aktive Schmerzerkennung, die Schutzreflexe auslöst. Der modulare Aufbau und eine spezifische Verletzungserkennung ermöglichen eine präzise Lokalisierung beschädigter Bereiche [156].

### 3.2.4 Mit allen Sinnen – Die Sensorik

Während die Akteure durch die rasanten Weiterentwicklungen der jüngeren Zeit schon jetzt Übermenschliches ermöglichen und den Terminator in Zukunft im wahrsten Sinne nach vorne katapultieren können, präsentiert sich auch das Gebiet der *Sensorik* mit gewaltigen Fortschritten – nicht nur beim Tastsinn, sondern auch was *Sehen*, *Hören* und *Riechen* anbelangt.

#### Die Sicht des Terminators

*Sehen* wird für den Terminator weit mehr sein, als nur eine visuelle Wahrnehmung der Umgebung mittels Kameras – und wird wenig gemein haben mit der Art und Weise, wie Menschen die Welt sehen. Statt kontinuierliche Bilderströme zu verarbeiten, werden Daten größtenteils nur noch bei Änderung des Zustandes eines Bildpunktes übermittelt, beispielsweise der Helligkeit oder des Farbwertes. Dieses sogenannte ereignisbasierte Sehen (Event-based Vision) mittels eines Dynamic Vision Sensors (DVS) resultiert in einem minimalen Datenaufkommen. Hierzu kommen neue Algorithmen zur Bewegungskompensation, wodurch das „Sichtfeld“ des Terminators schon heute mühelos eine zeitliche Auflösung erreicht, welche 2.000 Bilder pro Sekunde entspricht – damit ergeben sich Latenzen im Mikrosekundenbereich [2].

Dies ermöglicht Wahrnehmungs- und Reaktionszeiten, welche erheblich schneller sind als die des Menschen. Ein neuromorpher Bildsensor kann Bewegungen innerhalb von Mikrosekunden erfassen, während die menschliche visuelle Reaktionszeit knapp 250 Millisekunden beträgt. Um die resultierenden Vorteile zu veranschaulichen, lässt sich eine Gefechtssituation heranziehen: Die visuelle Verarbeitung eines Mündungsfeuers wäre beim Roboter auf Basis neuromorpher Sensorik so schnell, dass er Gegenmaßnahmen initiieren kann, noch bevor der menschliche Schütze den Rückstoß der eigenen Waffe realisiert.

Auch ermöglicht diese Art der Wahrnehmung eine extrem hohe Schärfe – verschwommene Bilder oder Facetten, wie sie bei schnellen Bewegungen für das menschliche Auge entstehen, entfallen: Die Problematik, dass im Überwachungssystem gerade der wichtigste Aspekt unscharf und verwischt dargestellt ist, weil die Aufnahme der gesamten Umgebungsinformation das System verlangsamt, obwohl der größte Teil des Bildes konstant bleibt, verschwindet (Komprimierungsverfahren wie MP3 und MP4 veranschaulichen den Effekt, denn auch da werden große Datenmengen drastisch reduziert, indem beispielsweise statt kompletter Einzelbilder nur Änderungen gespeichert werden; der Unterschied ist dann allerdings, dass die unnötigen Daten erst gar nicht in den Sensoren generiert werden).

Da das Roboterauge auch nicht auf für den Menschen sichtbare Wellenlängenbereiche beschränkt ist, eröffnet sich eine extreme Wahrnehmungsmöglichkeit der gesamten Umgebung. Schon lange haben verbreitete Bildsensoren in CCTV-Kameras eine sehr hohe Empfindlichkeit im Bereich der nahen Infrarotstrahlung, da



Quelle: eigene Darstellung

Abbildung 21: Wolf im Schafspelz?

das Basismaterial Silizium nicht nur Photonen im sichtbaren Spektrum absorbiert, sondern auch im nahen Infrarotbereich. Neben Aufnahmen im Tageslicht können die Sensoren somit ebenfalls Schwarz-Weiß-Bilder bei Dunkelheit liefern. Die technologischen Möglichkeiten sind aber sehr viel umfassender als nur farbiges Sehen am Tag und Nachtsicht auf Basis von Infrarot. Durch die Verwendung hunderter schmaler Spektralbänder anstelle von nur drei Kanälen für Rot, Grün und Blau kann der Roboter mittels hyperspektraler Analyse beispielsweise Tarnung viel einfacher erkennen: Da Chlorophyll im nahen Infrarotspektrum stark reflektiert, Farbe jedoch nicht, kann zum Beispiel ein künstliches Objekt schneller identifiziert werden [224]. Um dies noch weiter zu verbessern, können Polarisationsensoren integriert werden. Da das von künstlichen Oberflächen reflektierte Licht anders polarisiert ist, als das von natürlichen Strukturen zurückgeworfene, kann hiermit ein polarimetrischer Fingerabdruck erkannt werden und dabei helfen, getarnte oder transparente Objekte zu identifizieren [322].

Wärmebilder oder UV-Bilder können weiterhin für Materialprüfungen genutzt werden. Auch können beispielsweise elektromagnetische Ausstrahlungen von Mobiltelefon-Antennen, WLANs usw. mittels Analyse der entsprechenden Bänder direkt erkannt werden, ebenso wie die Sendeleitungen der Smartwatch oder die Drahtlosverbindung des Hörgerätes, der Insulinpumpe oder des Herzschrittmachers. Dies ergibt für den Terminator ein sehr umfassendes Bild von der Umgebung – aber er „sieht“ noch viel mehr.

#### Erkennung von Angst

Durch die Kombination von verschiedenen technologischen Bereichen mit ihren schnellen Fortschritten wird sich eine sehr genaue Detektion von Gemütszuständen und Regungen realisieren lassen. Ziel ist es, dass eine Analyse Stress und Angst schon erkennt, bevor sich eine Person dessen selbst bewusst wird.

Die Herzfrequenzvariabilität (HRV) ist ein wichtiger Indikator für die Aktivität des autonomen Nervensystems und kann zur Identifizierung emotionaler Zustände herangezogen werden. Die Entwicklung der Fern-Photoplethysmographie-Technologie (rPPG) hat es möglich gemacht, die Pulsfrequenzvariabilität (PRV) mit einer Kamera aufgrund von durch den Pulsschlag erzeugten mikroskopischen Farbveränderungen der Haut kontaktlos zu analysieren. Da die PRV mit der HRV korreliert, wird hierdurch eine berührungslose Beurteilung emotionaler Zustände möglich [362]. Zwar sind die derzeitigen Verfahren insbesondere im Außenbereich oder bei schlechter Beleuchtung mit Blick auf eine Gemütsfeststellung noch ziemlich ungenau und fehleranfällig, künftig könnte eine entsprechende Sensorik aber Teil des umfassenden Analysesystems des Terminators sein. Auch ermöglicht die Nutzung von Hochfrequenz-Radarsensoren eine kontaktlose Messung von Vitalfunktionen wie Herz- und Atemfrequenz auf bis zu zehn Meter Entfernung und durch Kleidung, Bettdecken oder sogar Matratzen hindurch [152], [361]. Nicht in ferner Zukunft, sondern unmittelbar bevorstehend.

Der Radarsensor des Terminators wird somit nicht nur die Vitalparameter von Personen in seiner Umgebung messen können. Durch Verbesserungen multimodaler Ansätze der radarbasierten biometrischen Identifizierung, der Optimierung von Radarfrequenzen und Antennenkonfigurationen und der systematischen Untersuchung von Wandmaterialien und Umgebungsbedingungen kann die biometrische Identifizierung mittels Radar durch Wände hindurch perspektivisch so zuverlässig werden wie herkömmliche LOS-Verfahren [290]. Dies bedeutet, dass der Terminator auch durch eine Tür oder Wand *hindurch* erkennt, ob sich Personen in einem Raum befinden.

### Der Spürhund

In manchen Bereichen waren künstliche Systeme bisher jedoch nicht annähernd konkurrenzfähig mit der menschlichen Sensorik. Insbesondere bei der *olfaktorischen Detektion* sind Geräte bisher typischerweise relativ groß und sperrig, energiehungrig und auf ganz spezifische Gase wie beispielsweise Alkohol oder Kohlenstoffmonoxid beschränkt. Während die diesbezügliche Sensorik derzeit kleiner und günstiger wird und durch die Nutzung von KI-basierter Mustererkennung komplexere Geruchsmuster erkannt werden können [220], [333], steht der wirkliche Gamechanger aber erst in den Startlöchern. Zum einen ermöglichen fortschrittliche Materialien wie Graphen, Kohlenstoffnanoröhren und Silizium in Verbindung mit nachgeschalteten biomolekularen Sonden wie Aptameren, Antikörpern und Enzymen, neue Bio-Feldeffekttransistoren (FET) mit bisher unerreichter Empfindlichkeit und Präzision [268]. Zum anderen kann, wie schon im Bereich des Gehirns und Rechnens gesehen, Wetware auch in diesem Bereich genutzt werden, um Signale von biologischen Rezeptoren in direkt nutzbare, elektrische Signale umzuwandeln, welche in den Rechensystemen weiterverarbeitet werden können. Aufgrund der hohen Sensitivität biologischer Zellen können dadurch auch ganz spezifische Moleküle in geringster Konzentration erkannt werden [240].

Bio-olfaktorische Chips für den Sicherheitsbereich und die Medizintechnik werden schon seit einem Jahrzehnt erforscht, beispielsweise Geruchssensoren für die Detektion von Sprengstoffen und chemischen Kampfstoffen [153]. Der limitierende Faktor war bisher die Überlebensdauer der biologischen Komponenten, welche häufig in speziellen Nährlösungen und Umgebungen gehalten werden mussten. In jüngerer Zeit konnten jedoch deutliche Verbesserungen erreicht werden, so dass bereits erste Wetware-Systeme im kommerziellen

Markt erhältlich sind. Mit Blick auf die Fortschritte im Bereich der synthetischen Biologie, welche sich derzeit zwar noch im Grundlagenstadium befindet aber bereits erste marktreife Anwendungen hervorgebracht hat [241], sind stabile und deutlich langlebigere Systeme lediglich eine Frage der Zeit. Olfaktorische Sensorik wird damit in der Lage sein, beispielsweise früh Anzeichen von Krankheiten wie Krebs anhand der Detektion von Markern in der ausgeatmeten Luft einer Person zu erkennen oder Menschen zu identifizieren. Eingebunden in die Sensorik eines Terminators können solche Informationen sehr nützlich für das Kampfsystem werden – und schnell ethische Grenzen überschreiten.

Auch die Integration von Biosensorik in die Haut des Roboters macht große Fortschritte, was die Möglichkeiten des Gesamtsystems deutlich erhöht [359]. Über die Haut verteiltes Messen wird eine inhärente Eigenschaft kommander humanoider Roboter sein. Statt beispielsweise zwei im Sinne von Ohren im Kopf installierte Mikrofone wird die entsprechende Sensorik über die Körperfläche des humanoiden Roboters verteilt. Durch die Nutzung von Micro-Electro-Mechanical Systems (MEMS)-Mikrofonen kann die Apertur, der Abstand zwischen den Sensoren, vergrößert und dadurch die Lokalisierung insbesondere von niedrigen Frequenzen deutlich verbessert werden. Durch ereignisbasierte Auswertung, welche nicht konstant einen Frequenzbereich auf Änderungen hin analysiert, sondern wie schon im Falle der visuellen Bänder, nur im Falle des Auftretens eines Signals aktiv wird, lassen sich Reaktionszeiten minimieren und Ortungsgenauigkeiten maximieren. Durch multimodale Informationsverarbeitung, beispielsweise der Nutzung visueller Objekterkennung und deren Einbeziehung in die Berechnungen der Schallreflektion (Physics-Informed Neural Networks) [298], kann der Roboter akustische Quellen äußerst genau lokalisieren.

### Übermenschliches: der perfekte Jäger

Der Terminator wird künftig aber noch mehr Möglichkeiten haben, die ihn zu einem perfekten Jäger machen. Genomsequenzierung wird bereits heute an internationalen Flughäfen eingesetzt, um Viren wie beispielsweise SARS-CoV-2, Influenza oder Mpox zu erkennen [155]. Bisher wurde Reverse Transcription Polymerase Chain Reaction (RT-PCR) genutzt, um auf das Vorhandensein spezifischer Viren zu prüfen und im positiven Falle einer Gensequenzierung zur genauen Identifizierung der Varianten zu starten.

In den jüngsten Pilotphasen erfolgt nun aber der Übergang zu Metagenomsequenzierung. Bei dieser Technik erfolgt eine direkte genetische Analyse von Umweltproben, ohne dass Organismen zunächst im Labor kultiviert werden müssen. Hierbei können alle Mikroben einer Probe analysiert werden, nicht nur solche nach denen spezifisch gesucht wird. Dies ermöglicht auch die Erkennung unerwarteter und komplett neue Pathogene [274].

Mit der derzeit voranschreitenden Miniaturisierung beispielsweise im Bereich der Nanopore-Sequenzierung und den Fortschritten bei der Nutzbarmachung von Short Tandem Repeats (STR) ist es einem künftigen Terminator nicht nur möglich, Phänotypisierungen innerhalb von Minuten beispielsweise zur Feststellung der Haut- oder Haarfarbe des Verursachers einer DNA-Spur durchzuführen, sondern mittels Next Generation Sequencing (NGS) spezifisch Personen beziehungsweise Ziele zu identifizieren [228].

Die Analyse der in der Umgebung befindlichen DNA (environmental DNA, eDNA) kann den Terminator somit künftig auf die Spur seines Zieles bringen, wenn auch eher in Form eines lautlosen Jägers als einer schnellen Verfolgung.

In geeigneter Kombination kann die Robotersensorik somit nicht nur die Fähigkeit des Menschen, sondern auch von spezialisierten Tieren schon sehr zeitnah bei weitem übertreffen: In einer mehrstufigen Analyse kann der Terminator zunächst eine permanente Analyse der Umgebungssituation durchführen, um Anomalien zu detektieren. Dies kann auf Basis chemischer Festkörpersensoren wie Nanotubes erfolgen, welche zwar noch keine feine Differenzierung abgeben können, aber kontinuierlich betrieben werden können. Im nächsten Schritt können Proben aus der Umgebung aufgesaugt werden, ggf. unter Nutzung von Ultraschall, um Partikel kontaktlos von zu untersuchenden Oberflächen zu lösen. Diese werden im biologischen Sensorteil im Inneren des Terminators genauer mittels in Nährlösung eingebetteter Rezeptorzellen analysiert. Aufgrund der unterschiedlichen Pheromone und flüchtigen organischen Verbindungen, welche vom Menschen je nach Emotionszustand erzeugt werden, kann der Terminator dann beispielsweise nicht nur Stress unmittelbar erkennen, sondern unter anderem auch differenzieren, ob Tränen aufgrund von Trauer oder Wut entstehen. So können bei einer Verfolgung nicht nur DNA-Analysen durchgeführt werden, es können beispielsweise auch kurzlebige und flüchtige Stresshormone insbesondere in Gebäuden analysiert werden, um eine taktische Nahbereichsaufklärung durchzuführen: Der Terminator kann Angst

riechen, noch bevor er eine Person sieht – während hier keine Differenzierung möglich wäre, könnte er mit seinem Hochfrequenzradar jedoch die Vitalparameter verschiedener Personen analysieren, um letztendlich zwischen Freunden und Feinden zu unterscheiden.

## 3.2.5 Die Effektoren

Im Bereich der Effektoren ergeben sich ebenfalls umfassende Möglichkeiten für den künftigen Terminator. Er kann problemlos mit sämtlichen Systemen ausgestattet werden, welche auch Menschen einsetzen, von konventionellen *Schusswaffen* über Flammen- und Granatwerfern bis zu *Energiewaffen* und Micro-Drohnen. Insbesondere könnten sich aber auch Bio- und Chemiewaffen sowie *Insekten-Drohnen* und *Cyborg-Insekten* in seinem Arsenal befinden.

### Der perfekte Schuss

Die Integration von *Schusswaffen* in Roboter wurde bereits umfassend in der Praxis erprobt. China hat beispielsweise in einer Anlandeübung bewaffnete Robotdogs zum Freisprengen des Weges und Abfangen von gegnerischem Feuer mit in die vorstoßenden Truppen integriert.

Im Gegensatz zur meist unlimitierten Munition in Filmen, kann die mitgeführte Munition zugunsten der Ausdauer, Beweglichkeit oder Anzahl integrierter Waffensysteme des Terminators deutlich reduziert sein. Da Roboter im Gegensatz zu menschlichen Schützen keine Probleme mit Rückstoß haben, können größere Kaliber oder auch panzerbrechender Munition eingesetzt werden. Durch die Kombination verschiedener Sensorik wie LiDAR und Wärmebild sowie die Nutzung von Feuerleitsystemen kann der Roboter unter Berücksichtigung von Faktoren wie Windgeschwindigkeit, Luftfeuchtigkeit, Ziel- und Eigenbewegung den *optimalen* Schuss in Echtzeit berechnen. Die Antizipation des Rückstoßes und das punktgenaue Wirken der Aktoren gegen den Rückstoß im Moment des Brechens eines Schusses ermöglichen auch in dynamischer Bewegung eine hochpräzise Bekämpfung und nahezu hundertprozentige Treffsicherheit.

Zwar wird auch die menschliche Fehlerquote durch neue Technologien weiter reduziert werden. So ist das XM-157 der U.S. Army ein Feuerleitsystem mit variabler Optik, Laser-Entfernungsmesser, ballistischem Rechner und Umgebungssensoren, um korrigierte Zielpunkte für eine erhöhte Genauigkeit des Schützen



zu generieren [273] und künftig werden Lock-On-Technologien wie schon bei Großwaffensystemen wie Panzern das Brechen eines Schusses beim Auslösen des Abzugs solange verzögern, bis die Position des Laufes optimal über dem Ziel ist, um das Zittern des Schützen auszugleichen. Der stressresistente Roboter mit einer im Vergleich zum biologischen Gegner deutlich schnelleren Reaktionszeit (Sensor-to-Shoot Kette) und extrem hohen Trefferquote auch in Bewegung wird jedoch im Vorteil sein [296].

### Energiewaffen

*Laser- und Mikrowellenwaffen* können ebenso zur Ausrüstung gehören, auch wenn sie aufgrund ihres Energiebedarfs vermutlich nicht die präferierte Waffen des Terminators werden. Sie können aber beispielsweise zur Generierung von Bioeffekten mit dem Ziel von Active oder Cognitive Denial, also der Kontrolle von Menschenmengen ohne letales Wirken [266] oder der Erzeugung von kognitiven Störungen genutzt werden [352].

### Cyborg-Insekten und Co

Deutlich raffinierter und tückischer kann allerdings die Nutzung von *Bio- und Chemiewaffen* sein. Im Gegensatz zum Menschen ist der Terminator bei deren Transport und Handhabung nicht selbst gefährdet. Dies eröffnet sowohl eine Integration von Drohnen oder Micro-Drohnen-Schwärmen in das Kampfsystem als auch die Nutzung von Insekten-Drohnen. Diese können hierbei sowohl als intelligente und unauffällige (Loitering-) Munition, oder zur Verbringung von Kontaktgiften, die transdermal über die Haut wirken oder mittels Mikro-Injektionssystem zugeführt werden, zur Anwendung kommen.

*Insekten-Drohnen* können über zwei grundsätzliche Arten realisiert werden, als *biomimetische Roboter* oder als *biohybride Systeme*.

*Biomimetische Roboter* sind komplett künstlich geschaffene Drohnen, welche die Vorbilder der Natur nachahmen, beispielsweise in der Form von Vögeln. Während anfängliche Modelle lediglich den Flügelschlag nachgeahmt haben, verwenden jüngste Arbeiten sich der Umgebung anpassende, biomimetische Steuerungen und beispielsweise auch echte Federn [57].

Bei *biohybriden Systemen* handelt es sich wiederum um lebende Insekten, welche mittels Elektronik aufgerüstet werden, um sie fernzusteuern. Auf diese Weise wurden

zum Beispiel bereits Käfer, Libellen und Kakerlaken komplett dirigiert. Mittlerweile können aber auch ganz Schwärme gesteuert werden, indem lediglich ein Zielpunkt vorgeben wird [12].

Der Vorteil dieser Cyborg-Insekten ist, dass sie das Problem der Energieversorgung und des Antriebs (fast) inhärent lösen: Die Elektronik muss lediglich die Steuerungsfunktion durch Implantate, welche entsprechende Impulse an die Muskulatur sendet, realisieren während das Insekt die grundlegende Energieversorgung biologisch bereitstellen kann. Gerade in Verbindung mit einem Micro-Injektionssystem und einem hochwirksamen Gift kann hierdurch eine schwer detektierbare und äußerst unauffällige und mobile Waffe entstehen. Die Aufrüstung zu Cyborg-Insekten in einem Fließband-System für „Massenproduktion“, welches die Elektronik an Kakerlaken vollautomatisch anbringt, wurde bereits demonstriert [222].

Mittels der Micro-Drohnen und Cyborg-Insekten können auch Probensammlungen von Hautpartikeln potentieller Ziele erfolgen oder DNA-spezifische Wirkstoffe gegen einzelne Personen oder bestimmte ethnische Gruppen eingesetzt werden (genetische Zielerfassung) [218], [275].

### 3.2.6 Massenproduktion und autonome Weiterentwicklung

Die moderne Robotertechnologie ist in ihrer Entwicklungsgeschwindigkeit nur noch bedingt vom Menschen und seiner Vorstellungskraft abhängig. Während die bisherige Robotik einem Top-down-Ansatz unterworfen war, bei dem Maschinen für einen bestimmten Zweck entworfen und optimiert wurden, geht dies seit einiger Zeit zu einem evolutionären Ansatz über, bei dem sich die Morphologie und die Steuerung von Robotern in einem ko-evolutionären Prozess ohne menschliches Zutun weiterentwickeln [107]. Ziel ist eine autonome Morphogenese, bei denen Systeme ihre Gestalt an die Umweltbedingungen anpassen und dazu nicht auf die Optimierung eines gegebenen Bauplanes auf die Umgebung beschränkt sind [182].

### Fortpflanzung von Robotern

Projekte wie ARE (Autonomous Robot Evolution) und der Robot Fabricator (RoboFab) demonstrieren entsprechende Möglichkeiten bereits heute. In einer Symbiose aus additiver Fertigung und automatisierter Montage eröffnet RoboFab einen hybriden Fertigungsansatz, bei

dem das Skelett eines Roboters mittels 3D-Druck individuell auf Basis des genetischen Codes, erzeugt durch den Evolutionsalgorithmus, gefertigt wird. Für die funktionalen Komponenten greift das System auf eine „Organbank“ zurück. Diese Bank enthält vorgefertigte Module mit standardisierten Schnittstellen für Motoren, Sensoren und Mikrocontroller und überbrückt die derzeit noch vorhandene Lücke, dass komplexe Elektronik noch nicht in einem Durchgang mit Strukturmaterial gedruckt werden kann.

Die vollautomatische Montage erfolgt dann mittels eines Greifarms, welcher die „Organe“ aufnimmt und in das frisch gedruckte Skelett einsetzt. Aufgrund der Nutzung von Federklammermechanismen und Schnappverbindungen müssen keine Löt- oder Klebearbeiten durchgeführt werden (welche allerdings auch keine große technische Herausforderung mehr darstellen würden, sondern mehr eine Zeit- und Kostenfrage sind), die elektrischen Verbindungen werden durch das Einrasten der Module geschlossen. Der Gesamtprozess ermöglicht somit autonom einen funktionstüchtigen Roboter, der wiederum lernen und sich selbst „fortpflanzen“ kann.

### Selbstheilung

Mittels der Möglichkeiten von 4D-Druck, welche den bisher statischen Objekten die Dimension Zeit hinzufügt, werden die kommenden Roboter durch die Nutzung von Materialien, die ihre Form oder Funktion unter Einfluss von externen Stimuli wie Hitze, Feuchtigkeit oder Licht verändern können, zunehmend resilient. Dies eröffnet unter anderem auch die Fähigkeit zur Selbstheilung. Inspiriert von der biologischen Wundheilung werden in der Robotik zunehmend selbstheilende Materialien wie Vitrimere und Polymere erprobt. Mittels der thermisch reversiblen Diels-Alder-Reaktion kann beispielsweise das beschädigte Bein eines Roboters durch gezieltes Erwärmen des molekularen Netzwerks aufgebrochen und neu verknüpft werden – der Riss schließt sich auf molekularer Ebene [325].

In der Roboterhaut eingebettete, mikrovaskuläre Netzwerke können ähnlich Blutgefäßen ungehärtetes Harz oder Härter transportieren. Bei einer Verletzung bricht das jeweilige Gefäß auf, die Flüssigkeit tritt aus und polymerisiert, wodurch die Struktur versiegelt wird. Hierbei kann auch flüssiges Metall verwendet werden, um beispielsweise gebrochene elektrische Leiterbahnen wiederherzustellen [338].

Neben den Möglichkeiten der Selbstheilung auf Hardware-Ebene können sich Roboter aber auch algorithmisch bezüglich der Erfüllung ihres Auftrags wiederherstellen. Ein Roboter kann im Falle einer Verletzung diese analysieren und „verstehen“, welche Einschränkungen sich hierdurch ergeben, wie diese ausgeglichen werden können und sich entsprechend anpassen. Fällt beispielsweise ein Arm aus, kann sich das System innerhalb kürzester Zeit so adaptieren, dass die Mission mittels der verbliebenen Fähigkeiten fortgesetzt werden kann [215].

### 3.2.7 Eine Frage der Kosten?

Ob und in welchem Umfang sich solche Technologien in den nächsten Jahrzehnten durchsetzen werden, ist neben der grundsätzlichen technischen Realisierbarkeit aber insbesondere eine Kostenfrage. Mit Blick auf die von Marktforschungsinstituten prognostizierten Zahlen investiert China massiv, um sich bereits jetzt große Anteile des nicht mehr fernen Zukunftsmarktes zu sichern. Dies spiegelt sich auch in der Preisgestaltung bereits marktverfügbarer, humanoider Roboter wider. Humanoide Roboter von beispielsweise Unitree oder Figure AI liegen heute in einem Bereich von circa 16.000 bis 100.000 USD, je nach Modell und Fähigkeiten beziehungsweise der Optimierungen für Logistik, Hochpräzision, schwere Arbeit oder Forschung.

Für eine Einschätzung der Kostenentwicklung über die nächste Dekade ist ein Blick auf das Wright'sche Gesetz [350] hilfreich, das beispielsweise auch die Entwicklungen im Flugzeugbau und der Automobilindustrie gut abbildet. Es dürfte auch die künftigen Preise humanoider Roboter abschätzen können. Gemäß Wright führt eine Verdoppelung der produzierten Güter zur Senkung der Kosten um einen festen Anteil, typischerweise um jährlich circa 15-20 Prozent. Die Konstruktion eines Roboters der Terminator-Klasse mit entsprechenden Komponenten, hochwertiger Sensorik und Effektoren könnte demnach in zehn Jahren Materialkosten von insgesamt circa 20.000 USD verursachen.

Blickt man auf die Personalkosten in westlichen Streitkräften, schlägt schon die reine Ausbildung eines Soldaten mit circa 50.000 bis 100.000 USD zu Buche [303] – hiermit wären bereits mehrere Terminator produzierbar. Die massiven Kostenvorteile entstehen jedoch in der Folge, denn Personal- und Versorgungskosten sind mit etwa. 40 Prozent ein beträchtlicher Anteil in westlichen Verteidigungsbudgets [39]. Wird der Terminator im Gefecht beschädigt, kann er gegebenenfalls kostengünstig repariert werden und wird ansonsten

entsorgt und durch ein schon wieder autonom weiterentwickeltes Modell ersetzt. Eine aufwändige Versorgung oder kostspielige Zurruesetzung verletzter Soldaten entfällt.

Die Kosten werden somit kein Hinderungsgrund für den Terminator auf dem Gefechtsfeld sein, sondern ganz im Gegenteil dessen Erscheinen beschleunigen.

### 3.3 FAZIT

Schaut man auf die rasante technologische Entwicklung wird klar, dass ein leistungsfähiger Terminator schon heute keine Science-Fiction mehr ist, noch nicht einmal mehr große Zukunftsmusik. Humanoide Roboter haben insbesondere im letzten Jahr im wahrsten Sinne große Saltos vor- und rückwärts gemacht und selbst optimistische Erwartungen mehrfach übertroffen. Auch wenn man noch immer schmunzeln kann, wenn das eine oder andere mal Vorführungen missglücken oder wieder ein kleiner Trick auffliegt und der angeblich autonome Roboter eben doch noch ferngesteuert wird – es ist nur eine Frage der Zeit, bis irgendwo *vollautonome* Waffensysteme auftauchen werden. Auch ein Kampfroboter à la Terminator ist nur noch eine Frage des „wann“, und nicht des „ob“.

Wenn sich die demokratische Wertegemeinschaft bezüglich der Entwicklung und Nutzung solcher Systeme nachvollziehbare und absolut sinnvolle ethische Grenzen setzt, so müssen trotzdem Antworten gefunden werden, wie mit solchen gegnerischen Systemen umzugehen ist. Während in zahlreichen Konflikten bewaffnete Drohnen einen immer größeren Stellenwert einnahmen, führte man in Deutschland über zehn Jahre eine von der Realität entrückte politische Debatte darüber. Die demokratische Wertegemeinschaft muss davon ausgehen, dass andere Staaten die Entwicklung vorantreiben werden und kann leider nicht warten, bis hunderte Kampfroboter hinter der Grenze stehen. Die große Herausforderung bei den Kernaspekten solcher Dual-Use Technologien ist, dass der Unterschied zwischen erlaubt und verboten oftmals nur in einem Algorithmus oder ein paar Zeilen Code liegt.

Womit bei einem künftigen Terminator *genau* zu rechnen ist, hängt davon ab, ob der eine oder andere technologische Sprung zu einer rasanten Entwicklung in bestimmten Bereichen führt oder die weitere technologische Entwicklung eher konservativ verläuft.

#### Terminator – „Lightweight“

Im Fall des „konservativen“ Terminators ist mit einem hochpräzisen Kampfroboter zu rechnen, der auf Basis konventioneller Bewaffnung eine nahezu perfekte Zielbekämpfung verspricht. Detektion, Aktion und Reaktion stellen jegliche menschliche Möglichkeiten in den Schatten, auch wenn diese durch den ebenso fortschreitenden Einsatz von Technologie weiter verbessert werden. Die Geschwindigkeit von autonomen Maschinen, insbesondere wenn sie teilweise auf biologischen Elementen und Prozessen basiert, kann nur durch Maschinen beantwortet werden. Auch Man-Unmanned-Teaming (MUT), bei dem beispielsweise ein menschlicher Pilot den Einsatz mehrerer (teil-)autonomer Luftsysteme überwacht, ist eher das Beharren auf alten Traditionen und der Versuch, Zeit zu erkaufen. Schaut man auf die Entwicklungszeiten, ist es fraglich, ob auch solche Systeme nicht jetzt schon der Vergangenheit angehören und Kampfflugzeuge der 6. Generation wie beispielsweise das von Deutschland, Frankreich und Spanien geplante Future Combat Air System (FCAS) bei seinem Zulauf ab circa 2040 überhaupt noch durchsetzungsfähig ist – auch mit unbemannter Begleitung. Die g-Kräfte, welche unbemannte Systeme bei Manövern aushalten, sind deutlich höher als was ein trainierter Kampfpilot aushalten kann. Mit Fortschritten in der Materialforschung wird dieser Abstand nur umso größer werden.

#### Terminator – „Worst Case“

Beim Auftreten von technologischen Sprüngen oder optimalen Entwicklungsverläufen wird der Terminator weitaus mächtiger. Im Zentrum stehen hier sowohl eine multimodale Sensorintegration, als auch ein resilienter, selbstheilender Aufbau des Gesamtsystems – unter den Möglichkeiten autarker Weiterentwicklung. Im Bereich der Effektoren ist zunächst weiterhin eine konventionelle Bewaffnung unter höchster Präzision zu erwarten, jedoch auch die Nutzung biologischer oder chemischer Waffen sowie von genetischen Markern. Kern ist jedoch, dass der Terminator aufgrund seiner umfassenden und überragenden Sensorik ein ultimativer Jäger wird, der sich auf unbekannte Situationen und Umgebungen einstellen, schnell lernen und sich adaptieren kann – das genaue Waffenarsenal wird für die erfolgreiche Auftragsausführung eher nebensächlich sein.

#### Wolf im Schafspelz

Ein zentraler Aspekt ist aber auch, dass ein übermächtiger „Terminator“ eben gerade nicht ein spezieller, hochentwickelter Kampfroboter sein muss. Findet die Robotik nach mittlerweile weitverbreiteten, nützlichen Helfern wie beispielsweise Saugrobotern weiter Einzug in unsere Haushalte und entwickeln sich die Fähigkeiten humanoider Roboter annähernd wie versprochen, so kann die künftige Haushalts- oder Pflegehilfe ein viel größeres Problem darstellen, als der Kampfroboter im Feld: Denn auch da gilt, zwischen gut und böse liegen oftmals nur ein paar Zeilen Code (siehe Abbildung 21).

Dass aufgrund des Gefahrenpotentials solcher System von einer besonders hochqualitativen Softwareentwicklung mit Fokus auf Sicherheit à la DevSecOps zu rechnen ist, erweist sich schon jetzt als Trugschluss. Beim deutschen Hackerkongress des Chaos Computer Clubs (39C3) wurde erst kürzlich demonstriert, wie einfach Roboter zu übernehmen sind. Neuartige Ansätze waren dafür nicht nötig [285]. Die selben Angriffsvektoren, welche seit Jahrzehnten funktionieren, haben auch hier wieder zur vollen Kontrolle und administrativer Rechteeskalation geführt. Verwunderlich ist das nicht, denn mit Blick auf Marktanteile haben viele Unternehmen in Fernost eine klare Priorität: Geschwindigkeit und Dominanz um jeden Preis.

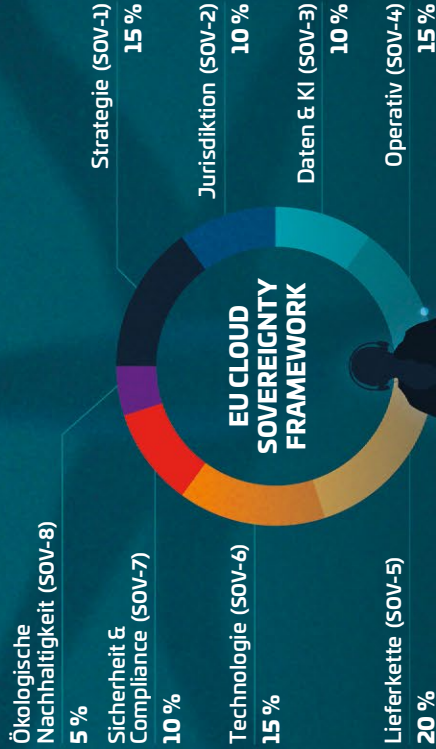
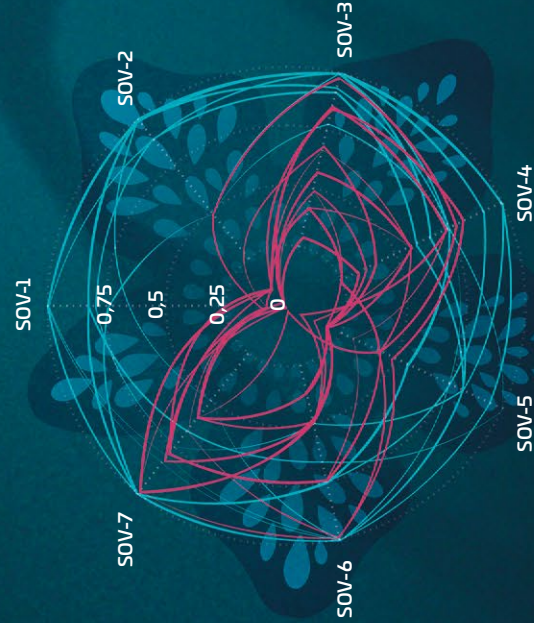
Die Bedeutung der eigenen Kontrolle über entsprechende Systeme und insbesondere deren Software, Algorithmen und „Gedanken“ wird daher existentiell. Die schleppende Diskussion über Software-Souveränität und halbherzige Minimaldefinitionen war schon bisher nicht hilfreich. Der Saugroboter hat allerdings deutlich weniger Möglichkeiten, seinen Besitzer zu terminieren, als dies künftige humanoide Haushaltshelfer haben werden. Der Zug ist fast schon abgefahren. Wenn Cybersicherheit nicht endlich ernsthaft angegangen wird, können die Konsequenzen schon in naher Zukunft gigantisch werden.

# KAPITEL 4



## Souveränitäts-Score (SOV)

- EU-Anbieter (ø 0,84 Punkte)
- Nicht-EU-Anbieter (ø 0,37 Punkte)



**TOP SCORES:** OpenProject  
axelor  
NextCloud

**GAME OVER:** Miro  
Confluence  
ChatGPT

— INSERT COIN —



**Marktkonzentration**

Während IaaS und PaaS klar von US-Hyperscalern dominiert werden, ist der SaaS Markt sehr viel fragmentierter

- AWS
- Microsoft Cloud
- Google Cloud
- Andere

**Enterprise-Software weltweit**

Umsatz in Mrd. USD



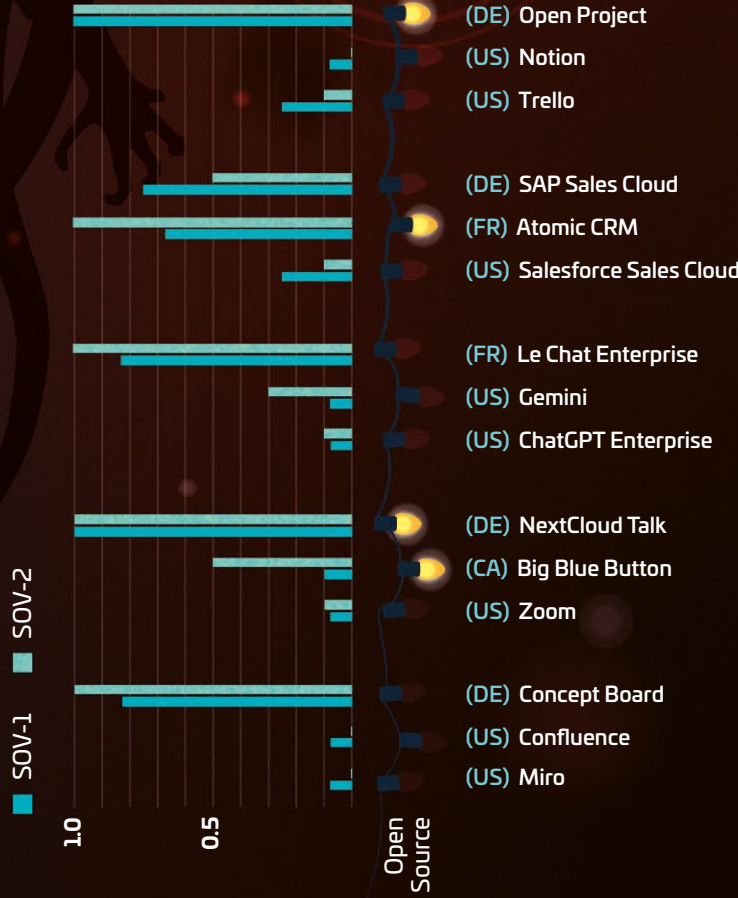
## Wahrgenommene Abhängigkeit

von digitalen Produkten aus den USA und China



## Vergleich von EU- und Nicht-EU-Lösungen

in Bezug auf den Score in SOV-1 (Strategie) und SOV-2 (Juristische Souveränität)



## US-Hyperscaler greifen in sämtliche Software-Kategorien

Verfügbare Hosting-Optionen



**96 %**

aller KI-fähigen Public Cloud  
Regionen werden von US-Chips  
angetrieben  
(hauptsächlich NVIDIA)



## 4 SOVEREIGN THINGS – SOFTWARESOVERÄNITÄT IN EUROPA

Die Debatte um die digitale Souveränität Europas hat sich in den vergangenen Jahren zu einer strategischen Notwendigkeit entwickelt. In einem verschärften geopolitischen Klima hat das Thema nach einem zuvor wissenschaftlich-geprägten Diskurs nun auf politischer und wirtschaftlicher Ebene Umsetzungsreife erlangt. Heute geht es nicht mehr nur um die Fragen nach dem „Was“ und „Warum“, sondern um operative Lösungen, die nationale Sicherheit, globalen Wettbewerb und regulatorische Compliance miteinander verknüpfen.

Vor diesem Hintergrund adressiert dieses Kapitel die Notwendigkeit, digitale Souveränität auf der Anwendungsebene greifbar zu machen. Während Infrastruktur-Fragen oft im Fokus stehen, stellt Software einen der kostenintensivsten Posten der digitalen Infrastruktur von Organisationen dar [318]. Zur Bewertung eines organisationsrelevanten Softwareportfolios operationalisiert dieses Kapitel erstmals das EU Cloud Sovereignty Framework (EU CSF) der Generaldirektion Digitale Dienste (DG DIGIT) von Oktober 2025.

Um diesen Weg von der Theorie zur messbaren Praxis zu ebnen, verfolgt das Kapitel drei Ziele: (1) Einordnung des Diskurses: Es bietet eine Einführung in die aktuelle Debatte zur digitalen Souveränität in Europa. (2) Methodische Operationalisierung: Es stellt das EU CSF vor und präsentiert das darauf aufbauende, für die Anwendungsebene angepasste Software Sovereignty Framework (EU SSF). (3) Evidenzbasierte Analyse: Es unterzieht 27 in Europa verfügbare Softwareprodukte einer explorativen Analyse auf Basis des EU SSF.

### 4.1 HINTERGRUND ZUM DISKURS ZUR DIGITALEN SOVERÄNITÄT IN EUROPA

Die digitale Souveränität Deutschlands und Europas ist weit mehr als eine technologische Debatte; sie stellt eine strategische Notwendigkeit dar, die nationale Sicherheit, globalen Wettbewerb und regulatorische Compliance untrennbar miteinander verknüpft. Unkontrollierte Abhängigkeiten schaffen tiefgreifende

Verwundbarkeiten, die von geopolitischen Risiken und extraterritorialen Datenzugriffen bis hin zum klassischen Vendor-Lock-in reichen. Vor diesem Hintergrund bedeutet digitale Souveränität nicht nur kurzfristige Absicherung, sondern „Enkelfähigkeit“: die Gestaltung einer resilienten, nachhaltigen und zukunftssicheren digitalen Gesellschaft für kommende Generationen [300].

#### Souveränität im Wandel

Der Begriff der Souveränität existiert seit Jahrhunderten und hat über die Zeit einen Bedeutungswandel vollzogen [15]. Seit dem 17. Jahrhundert reflektierte er die Vorstellung von souveräner Herrschaft als oberste, allumfassende und territorial begrenzte Macht [161]. In der modernen internationalen Ordnung bedeutet Souveränität vor allem die Unabhängigkeit eines Staates gegenüber anderen Staaten (externe Souveränität) sowie die höchste Befehlsgewalt innerhalb des eigenen Territoriums (interne Souveränität) [280].

Mit dem Aufkommen des Internets und der Globalisierung wurde diese umfassende territoriale Kontrolle allerdings teilweise infrage gestellt. Zum einen entziehen sich grenzüberschreitende Datenströme der traditionellen geographischen Logik [141], zum anderen haben internationale Konzerne rivalisierende, quasi-souveräne Macht aufgebaut [270]. Während die Digitalisierung in den 1990er Jahren noch als Beschleuniger einer post-territorialen Welt ohne staatliche Grenzen gefeiert wurde [14], wird sie heute zunehmend als Bedrohung für die staatliche Handlungsfähigkeit wahrgenommen.

Digitale Souveränität wird heute häufig als die Fähigkeit zur unabhängigen Entscheidung und Handlung im digitalen Raum definiert [122], [207], [280]. Sie umfasst den gesamten „digitalen Stack“ – von der Hardware wie Halbleitern und Chips über Standards und Protokolle bis hin zu Software, Daten und Infrastrukturen wie Cloud-Systemen [141]. Dabei lassen sich drei zentrale Ebenen der Selbstbestimmung unterscheiden: Staat, Ökonomie und Individuum [280]. Auf der staatlichen Ebene wird die nationale Sicherheit, Regulierung und Schutz kritischer Infrastrukturen betrachtet. Auf ökonomischer



Ebene werden Wettbewerbsfähigkeit und Reduktion technologischer Abhängigkeiten von ausländischen Anbietern forciert. Die individuelle Ebene bezieht sich auf die Fähigkeit Einzelner zur informationellen Selbstbestimmung, digitalen Kompetenzen und eine unabhängige Gestaltung der digitalen Transformation [79].

Die Interpretation des Begriffs variiert allerdings international. Während autoritär geprägte Staaten wie Russland und China Internet- oder Cyber-Souveränität oft als staatliche Kontrolle über das nationale Internet und den Cyberraum begreifen, um sich gegen äußere Einflüsse abzusichern [56], verfolgt die EU einen wertebasierten Ansatz. Das Joint Research Centre (JRC) der EU konkretisiert diesen Ansatz durch ein mehrschichtiges konzeptionelles Framework, das digitale Souveränität als die Fähigkeit zur Ausübung strategischer Unabhängigkeit bei gleichzeitiger Offenheit gegenüber globalen Netzwerken definiert [122]. In den BRICS-Staaten wird digitale Souveränität zudem verstärkt als Instrument zur Ausübung von Macht und Kontrolle über Infrastrukturen verstanden, um Bedingungen eines „digitalen Kolonialismus“ herauszufordern und technologische Unabhängigkeit zu erlangen [19]. In Deutschland ist der Diskurs durch eine Vielfalt an Narrativen geprägt, die von wirtschaftlicher Prosperität bis hin zu individueller Ermächtigung reichen [217].

Der Diskurs verlagerte sich in den letzten Jahren von einer wissenschaftlich-geprägten zu einer praktischen politischen und wirtschaftlichen Debatte in der EU. Schon die Snowden-Enthüllungen (2013) verdeutlichten die Überwachungsmöglichkeiten durch ausländische Geheimdienste und führten zu Forderungen nach territorialen Schutzstrategien [161]. Die COVID-19-Pandemie wirkte als weiterer Katalysator, da sie globale Lieferkettenunterbrechungen und die Abhängigkeit von US-amerikanischen Plattformen und Hardware-Produzenten offenlegte. In einem Brief an Kommissionspräsidentin Ursula von der Leyen forderten die Regierungschefs von Deutschland, Dänemark, Finnland und Estland 2021 die digitale Souveränität als Leitmotiv europäischer Politik zu etablieren und kritische technologische Abhängigkeiten abzubauen [244].

Das verschärfte geopolitische Klima und die Handlungen der amerikanischen Regierung seit 2025 haben die Diskussion deutlich verstärkt. Der Fokus für staatliche Organe und viele Organisationen liegt nun auf der kurzfristigen Reduktion von Abhängigkeiten und dem Aufbau von starken europäischen Digital-Lösungen. Diese Entwicklung wird durch eine intensive politische und wirtschaftliche „Stack“-Debatte (z. B. EuroStack; Deutschland-Stack) und Initiativen wie den Gipfel zur

Europäischen Digitalen Souveränität im November 2025 in Berlin flankiert [36], [37], [45], [133]. Das EuroStack-Konzept schlägt dabei ein umfängliches, aufeinander aufbauendes Technologie-Ökosystem von Chips über Cloud bis hin zu Software und KI vor, um eine föderierte europäische Infrastruktur als Alternative zu globalen Hyperscalern zu etablieren [133].

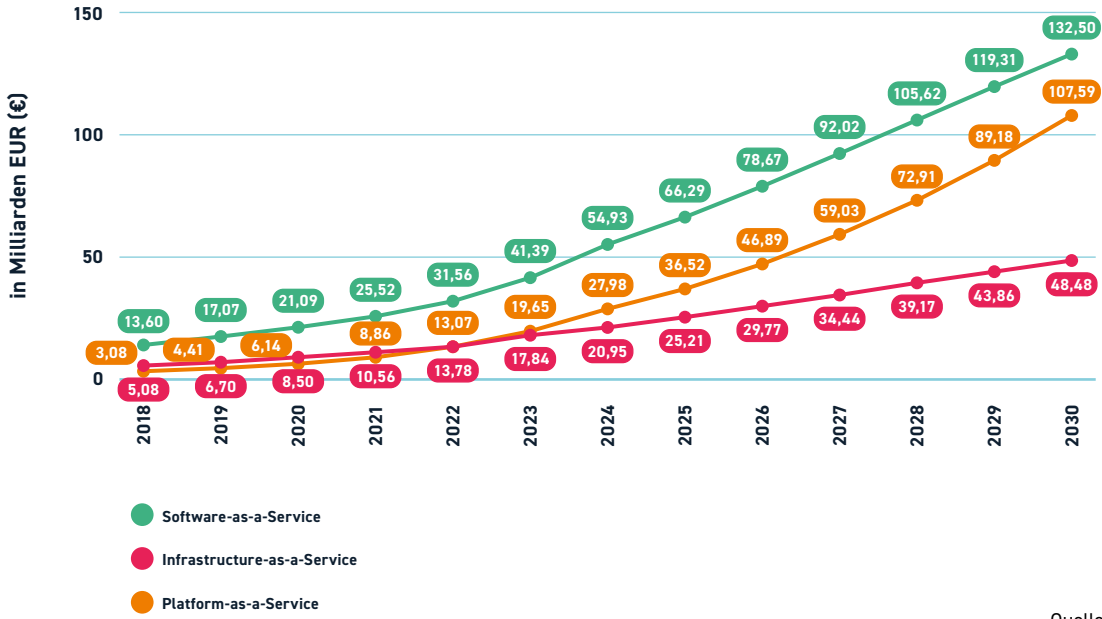
### Messbarkeit und Operationalisierung von Digitaler Souveränität

Trotz der politischen Relevanz bleibt die Messung von digitaler Souveränität schwierig, da es sich nicht um ein präzises politisches Instrument oder klar abgegrenztes Handlungsfeld handelt. Ansätze wie das Schichtenmodell (Stack-Modell) [207] oder das vom EU JRC vorgeschlagene mehrschichtige Framework versuchen, digitale Souveränität zu strukturieren [122].

Als Reaktion auf diese Herausforderungen veröffentlichte die DG DIGIT der EU Kommission im Oktober 2025 das EU Cloud Sovereignty Framework (EU CSF) [122]. Zur Selbsteinschätzung von Cloud-Anbietern und der anschließenden Auswertung durch die DG DIGIT in ihrem Beschaffungsprozess konzipiert, bieten die Metriken eine wertvolle Grundlage für eine wesentlich breitere Anwendung für weitere IT-Lösungen. Zusätzliche Relevanz erfährt dieses Vorhaben durch den geplanten EU Cloud and AI Development Act (CADA) [126] sowie die Überarbeitung der EU-Vergaberichtlinien (Public Procurement Act 2014/23/EU, 2014/24/EU, 2014/25/EU). CADA wird für das erste Quartal 2026 erwartet und basiert auf Empfehlungen des Draghi-Berichts [101]. Er soll die EU-Kapazitäten zur Entwicklung unabhängiger Cloud-Technologie und Künstlicher Intelligenz (KI) stärken und Abhängigkeiten von US-Anbietern durch eine klare Definition und Zielvorgaben für Cloud-Souveränität gezielt reduzieren. Analog dazu werden bei der Überarbeitung der Vergaberichtlinie die politische Leitlinie „Buy European“ sowie Sicherheitsinteressen verfolgt. Ein erster Entwurf ist für das zweite Quartal 2026 terminiert [125].

### Von Cloud-Infrastruktur zur Betrachtung von Software

Die bisherige praktische Debatte um digitale Souveränität konzentrierte sich häufig auf die Cloud-Infrastruktur der US-Hyperscaler und Bedenken hinsichtlich unbeachteten Datenzugriff legitimiert durch amerikanische Gesetze wie den Clarifying Lawful Overseas Use of Data Act (CLOUD Act) oder des US Foreign Intelligence Sur-



Quelle: [318]

Abbildung 22: Umsätze von Public Cloud in Europa im Vergleich

veillance Act (FISA) [142]. Nun rücken in der Betrachtung von Abhängigkeiten, Wettbewerbsfähigkeit und langfristiger Resilienz zunehmend auch andere Technologien in den strategischen Fokus.

Im Vergleich zu anderen Technologiefeldern fühlen sich Unternehmen aktuell am stärksten im Bereich der Software von nicht-europäischen Anbietern abhängig (36 Prozent) [357]. 72 Prozent der deutschen Unternehmen beziehen Software aus dem Ausland [25], auf europäischer Ebene fließen 80 Prozent der Ausgaben für Software und Cloud allein an US Anbieter [160]. Noch stärker als im Privatsektor werden Abhängigkeiten von außereuropäischen Anbietern in der öffentlichen IT wahrgenommen, besonders im Bereich Bürosoftware (81 Prozent) und Kollaborationstools (47 Prozent) [257].

Dass Software ein relevanter Wachstumsmarkt ist, zeigen aktuelle Prognosen: Der Umsatz im europäischen Software-as-a-Service (SaaS) Cloud Markt soll von 66,29 Milliarden Euro in 2025 auf 132,5 Milliarden Euro im Jahr 2030 steigen – ein Volumen, das die Segmente Platform-as-a-Service (PaaS) und Infrastructure-as-a-Service (IaaS) deutlich übersteigt (siehe Abbildung 22) [319]. Mit durchschnittlichen Ausgaben von 107,78 Euro pro Arbeitnehmer ist SaaS zudem der kostenintensivste Posten der digitalen Organisations-Infrastruktur [318]. Die Digitalwirtschaft wächst in Deutschland mit einem Plus von 10,2 Prozent in 2025 [26]. Gleichzeitig entfallen rund 80 Prozent der Ausgaben für Software und Cloud in der EU auf US-Anbieter [160]. Somit besteht ein Schwungrad-Effekt („Flywheel“), ein selbstverstärken-

der Geschäftskreislauf, bei dem die Ausgaben der EU US-Firmenprofite steigern und Reinvestitionen in Forschung und Entwicklung ermöglichen. Dadurch konnte in diversen Bereichen ein Innovationsvorsprung aufgebaut werden, der die Marktbherrschaft und Burggraben der US-Anbieter vor der europäischen Konkurrenz festigt.

Abhängigkeiten im Bereich der Bürosoftware sind seit Jahren bekannt und werden spätestens seit 2025 durch Wechsel-Entscheidungen gerade im öffentlichen Sektor in Angriff genommen. Beispielsweise stellen das Kultusministerium in Baden-Württemberg [247] und der Internationale Strafgerichtshof (IStGH) [116] digitale Arbeitsplätze von Microsoft 365 auf openDesk des Zentrums für Digitale Souveränität (ZenDiS) um. Letzteres nach Sanktionen der USA gegen Richter und Chefankläger [172]. 80 Prozent der Landesverwaltung von Schleswig-Holstein wurden bis Dezember 2025 auf LibreOffice migriert [170]. Auch das dänische Digitalministerium hat diesen Wechsel 2025 angekündigt [291]. Das österreichische Sozial- und Gesundheitsministerium nutzt neuerdings das quelloffene Nextcloud Hub als Kollaborationsplattform [256] und französische Beamte sollen ab 2027 nur noch das quelloffene und in Frankreich entwickelte Videokonferenz-Tool Visio anstelle von Microsoft Teams, Cisco Webex oder Zoom verwenden [356].

Im Kontrast zu Bürosoftware-Suiten finden andere Arten von Software bisher vergleichsweise wenig Beachtung. Auch strukturelle Souveränitätsrisiken über

| Framework                       | Herausgeber          | Ansatz             | Technologie                                         | Daten                                       | Vergleichsebene | Ziel                                          |
|---------------------------------|----------------------|--------------------|-----------------------------------------------------|---------------------------------------------|-----------------|-----------------------------------------------|
| C5                              | BSI                  | Kriterienkatalog   | Cloud                                               | Prüfbericht                                 | Produkt         | Zertifizierung                                |
| Deutsche Verwaltungscloud (DVC) | DVC/ IT Planungsrat  | Reifegradbewertung | Cloud                                               | Anbieter-Selbstauskunft                     | Produkt         | Beschaffungsprozess                           |
| Digital Sovereignty Index       | NextCloud            | Ländervergleich    | Open-Source Kollaborations- und Kommunikationstools | Öffentliche Daten                           | Land            | Internationaler Vergleich                     |
| EU Cloud Sovereignty Framework  | DG DIGIT             | Reifegradbewertung | Cloud                                               | Anbieter-Selbstauskunft & öffentliche Daten | Produkt         | Beschaffungsprozess                           |
| GAIA-X Level 3 Zertifizierung   | CISPE                | Produktkatalog     | Cloud                                               | Anbieter-Selbstauskunft                     | Produkt         | Anbieterübersicht – GAIA-X compliant Lösungen |
| SecNumCloud                     | ANSSI                | Kriterienkatalog   | Cloud                                               | Prüfbericht                                 | Produkt         | Zertifizierung                                |
| Tech Sovereignty Catalogue      | Digital SME Alliance | Produktkatalog     | Digitale Produkte                                   | Anbieter-Selbstauskunft                     | Produkt         | Anbieterübersicht – Europäische Lösungen      |

Quelle: eigene Darstellung

Tabelle 3: Frameworks, Zertifizierungen und Indizes für digitale Souveränität im Vergleich

Softwarekategorien hinweg (Talentmanagement, Transparenz, Wechselfähigkeit) müssen erst noch stärker in den Fokus rücken. Angesichts der tiefen Durchdringung der Arbeitswelt und der massiven Kapitalströme für außereuropäische Software ist die Untersuchung der digitalen Souveränität in diesem Bereich essentiell, um Risiken und Handlungsbedarfe zu identifizieren.

Die vorliegende Analyse nutzt das von der EU Kommission veröffentlichte CSF als Basis, um ein modernes, organisationsrelevantes Softwareportfolio in seiner digitalen Souveränität zu bewerten und die Anwendbarkeit eines solchen Rahmenwerks zu testen.

## 4.2 OPERATIONALISIERUNG UND MESSBARKEIT VON DIGITALER SOUVERÄNITÄT

Die größte Hürde bei der Messung digitaler Souveränität liegt in der inhärenten Unschärfe und allgemein akzeptierten Methoden für die Erfassung des Begriffs. Digitale Souveränität fungiert oft als politisches Schlagwort – ein „Konsensvokabular“, das zwar strategische Relevanz signalisiert, konzeptionell jedoch vage bleibt [348]. Um diese Rhetorik in eine operative Umsetzung zu überführen, müssen entsprechende Ziele in messbare Indikatoren übersetzt werden.

### 4.2.1 Die bestehende Framework-Landschaft

Die bestehende Framework-Landschaft lässt sich in drei Kategorien unterteilen: Produktkataloge, Kriterienkataloge mit Zertifizierungen und Reifegradmodelle. Während Produktkataloge primär die Marktverfügbarkeit oder -diffusion bestimmter Lösungen darstellen, konzentrieren sich Anforderungskataloge mit Zertifizierungen auf die Einhaltung technischer und regulatorischer Mindeststandards. Reifegradmodelle bilden digitale Souveränität als einen dynamischen Entwicklungspfad eines Produkts oder einer Organisation ab.

Trotz dieser Vielfalt eint die meisten Ansätze bisher eine starke Fokussierung auf Cloud-Infrastruktur, während die Bewertung der Anwendungsebene (Software) unterrepräsentiert bleibt (siehe Tabelle 3).

Während digitale Souveränität häufig im Kontext der Handlungsfähigkeit von Staaten und Organisationen diskutiert wird, bilden aktuelle Frameworks vor allem Anforderungen an Produkte und Services ab. Es wird nicht die digitale Souveränität ganzer Staaten oder Organisationen verglichen, sondern Ausprägungen konkreter Produkte, die hierzu beitragen. Auch Frameworks von EU und nationalen Sicherheitsbehörden beziehen sich auf konkrete (Cloud-)Dienste. Beispiele hierfür sind nationale Zertifizierungen wie SecNumCloud der französischen Agentur für Sicherheit der Informationssysteme (ANSSI) und der Cloud Computing Compliance Criteria Catalogue (C5) des deutschen

BSI [46]. Diese liefern prüfbare Kriterienkataloge für Cloud-Anbieter in ihren jeweiligen Ländern und unterstützen somit die Bewertung der digitalen Souveränität für Organisationen.

Die Bewertungsgrundlagen reichen von öffentlich verfügbaren Daten über Anbieter-Selbstauskünfte zu Prüfberichten durch Auditierer. Der Tech Sovereignty Katalog der Digital SME Alliance beispielsweise kuratiert eine Übersicht europäischer Lösungen für Organisationen und Individuen [95]. Dieser basiert, wie auch der CISPE Katalog [76], auf Anbieter-Selbstauskünften über Produkte (Tech Sovereignty Katalog) bzw. Einhaltung verschiedener Standards (CISPE Katalog). Im Kontrast dazu basiert der Nextcloud Digital Sovereignty Index auf öffentlich verfügbaren Daten zur Verbreitung von selbst gehosteten Kollaborations- und Kommunikationstools in verschiedenen Ländern [255].

Die Deutsche Verwaltungscloud setzt auf Reifegradbewertungen und Architekturprinzipien durch Anbieter-Selbstauskünfte [94].

Diese Vielfalt verdeutlicht, dass es bisher keine singuläre Metrik für digitale Souveränität gibt; vielmehr hängt die Wahl des Messverfahrens von den spezifischen Zielvorstellungen, dem Untersuchungsgegenstand und der verfügbaren Datenbasis ab.

| ID    | Souveränitätsdimension (Ziel)              | Gewichtung im Scoring |
|-------|--------------------------------------------|-----------------------|
| SOV-1 | Strategische Souveränität                  | 15 %                  |
| SOV-2 | Rechtliche & jurisdiktionelle Souveränität | 10 %                  |
| SOV-3 | Daten- & KI-Souveränität                   | 10 %                  |
| SOV-4 | Operative Souveränität                     | 15 %                  |
| SOV-5 | Lieferketten-Souveränität                  | 20 %                  |
| SOV-6 | Technologische Souveränität                | 15 %                  |
| SOV-7 | Sicherheit & Compliance                    | 10 %                  |
| SOV-8 | Ökologische Nachhaltigkeit                 | 5%                    |

Quelle: [122]

Tabelle 4: Souveränitätsdimensionen des EU Sovereign Cloud Frameworks mit Gewichtung

### 4.2.2 Das EU Cloud Sovereignty Framework als neuer Referenzrahmen

Das von DG DIGIT etablierte Framework definiert digitale Souveränität nicht als binären Zustand, sondern als messbares Spektrum. Das Framework dient als methodische Grundlage für einen EU-Beschaffungsprozess, der darauf abzielt, Cloud-Lösungen mit hoher digitaler Souveränität für die europäischen Institutionen zu identifizieren. In diesem Verfahren wurden Cloud-Anbieter im Rahmen einer Ausschreibung aufgefordert, ihre Services anhand der vordefinierten Kriterien selbst einzuschätzen und eine umfangreiche Nachweisdokumentation bis Ende 2025 einzureichen. Das Framework unterteilt die digitale Souveränität in acht Dimensionen (siehe Tabelle 4) mit jeweils vier bis sechs Einflussfaktoren und nutzt ein zweistufiges Bewertungssystem basierend auf „Sovereignty Effectiveness Assurance Levels“ (SEALs) und einer Gesamtpunktzahl (Souveränitäts Score).

#### Sovereignty Effectiveness Assurance Level (SEAL):

Ein Anbieter muss für jede der acht Dimensionen ein spezifisches Mindest-Souveränitätslevel erreichen; wird dieses in nur einer der Dimensionen unterschritten, fungiert dies als Ausschlusskriterium. Die SEALs beschreiben dabei ein Spektrum von SEAL-0 (keine digitale Souveränität, exklusive Kontrolle durch Nicht-EU-Dritte) über Zwischenstufen wie SEAL-2 (Datensouveränität mit durchsetzbarem EU-Recht, aber verbleibenden Abhängigkeiten) bis hin zu SEAL-4 (vollständige digitale Souveränität durch EU-Kontrolle ohne kritische Abhängigkeiten). Das Minimum-SEAL kann für verschiedene Anforderungen unterschiedlich definiert werden (in einem Prozess bei SEAL-2, in einem anderen bei SEAL-4 liegen). Nur Angebote, die das vordefinierte Minimum-SEAL in allen Dimensionen erreichen, werden über den Souveränitäts Score bewertet und verglichen. Während die SEAL-Mindestanforderungen somit die grundlegende Zulassung regeln, ermöglicht der Score eine differenzierte Rangfolge der verbleibenden Lösungen.

**Souveränitäts Score:** Der Souveränitäts Score dient der granularen, vergleichenden Bewertung der Angebote. Für jede der acht Dimensionen wird ein Punktwert ermittelt. Die Berechnung des Gesamtergebnisses folgt dabei einer gewichteten Aggregation: Die einzelnen Kategorien fließen mit unterschiedlicher Priorisierung in den Endwert ein (siehe Tabelle 4).

Die Gewichtung der acht Dimensionen zeigt eine Priorisierung: Die technologische Souveränität (15 %) und die Lieferketten-Souveränität (20 %) bilden den Kern,



während rechtliche und jurisdiktionelle Aspekte mit 10 % gewichtet werden. Diese Verteilung basiert auf der Annahme der DG DIGIT, dass rechtliche Schutzmaßnahmen bereits durch Standard-Vergabeverfahren abgedeckt sind [122].

Der Ansatz birgt Schwachpunkte. Anbieter könnten einen Mangel an rechtlicher Immunität durch hohe Effizienz in der Lieferkette oder Nachhaltigkeit teilweise ausgleichen, sofern das SEAL-Mindestlevel je Dimension erreicht wird. Somit birgt das „Souveränitätsspektrum“ das Risiko, dass Anbieter hohe Souveränitätswerte erzielen, auch wenn sie fundamentale Abhängigkeiten ins Ausland haben. Zudem wird befürchtet, dass der hohe administrative Aufwand zur Erfüllung der SEAL-Metriken große Konzerne bevorzugen und kleinere europäische Anbieter überfordern könnte [77], [143].

Es wird erwartet, dass dieses Framework von verschiedenen Akteuren aufgegriffen, erweitert und angepasst wird. Beispielsweise haben BSI und ANSSI im November 2025 die gemeinsame Entwicklung eines auf dem EU CSF aufbauenden Kriterien-Sets inklusive Auditierungsmethode angekündigt [277].

Um das primär für Cloud-Infrastrukturen gedachte EU CSF für die Bewertung eines Softwareportfolios nutzbar zu machen, wurden die Kriterien in dieser Analyse angepasst und für die Zwecke ihrer praktischen Messbarkeit in einem EU Software-Souveränitäts-Framework (EU SSF) präzisiert.

4.3 ANPASSUNG DES EU CSF ZUR MESSUNG VON SOFTWARE-SOUVERÄNITÄT

Der Kern der vorliegenden Analyse besteht darin, die im EU CSF formulierten Einflussfaktoren durch die Definition von Assessment Kriterien für Software zu operationalisieren. Das resultierende EU SSF besteht aus sieben Dimensionen mit je vier bis sechs Assessment Kriterien, sowie der Bewertungs-Methodik mit Souveränitäts Score und SEALs. Die Entwicklung des EU SSF erfolgte zum Zweck der vorliegenden Analyse, mit dem Ziel der Vertestung des EU CSF, dessen Spezifizierung für das bisher wenig betrachtete Software Ökosystem und der explorativen Analyse für Unternehmens-Software verschiedener Kategorien. Zum Zeitpunkt der Veröffentlichung liegt keine vergleichbare Analyse vor.

Die Dimensionen der digitalen Souveränität

Sieben der acht Dimensionen des EU CSF wurden in das EU SSF übertragen. Die Dimension der ökologischen Souveränität (SOV-8) wird ausgeklammert, da sie im Kontext von Softwaretechnologien nur eingeschränkt anwendbar und Daten begrenzt verfügbar sind.

Die Einflussfaktoren der jeweiligen Dimensionen wurden für die Erstellung von Assessment Kriterien und Antwortkategorien präzisiert. Im ursprünglichen Framework erweisen sich Kriterien als vage oder es werden mehrere, teils heterogene Elemente in einem einzigen Faktor zusammengeführt (siehe beispielsweise Tabelle 6 und Tabelle 7).

Souveränitäts Score und SEALs

Analog zum CSF wird ein Scoring basierend auf einem gewichteten Mittelwert berechnet. Hierbei wird die Gewichtung des EU CSF zur Vergleichbarkeit übernommen. Im EU SSF sind alle Einflussfaktoren innerhalb einer Dimension gleich gewichtet (es gibt keine Information zur Gewichtung im CSF). Hierbei werden die einzelnen Faktoren entweder binär als 0 oder 1 (Hauptsitz innerhalb der EU, SOV-1.1) oder mit Abstufungen (0,25; 0,5; 0,75) (Datenlokalisierung, SOV-3.3) bewertet.

Da bislang Unklarheit über die exakten Schwellenwerte für die SEALs (0–4) im CSF besteht, wurden in dieser Analyse des EU SSF alle Werte unter 0,2 – unter Annahme einer uniformen Verteilung der fünf SEAL-Stufen zwischen 0 und 1 – als SEAL-0 bewertet. Hierbei basieren die SEALs nicht auf spezifischen Ausprägungen der einzelnen Kriterien, sondern auf den gewichteten Scores je Souveränitätsdimension.

Die untersuchte Software

Das EU SSF wird auf ein klassisches Softwareportfolio von Organisationen in den Bereichen Datenbanken, Ressourcenplanung (ERP), Kundenbeziehungsmanagement (CRM), Projektmanagement, Videokonferenz-Tools, KI, Identitäts- und Zugriffsverwaltung (Identity and Access Management, IAM), Kollaboration und Cybersicherheit angewendet (siehe Tabelle 5). Die Auswahl an Softwareprodukten basiert auf einer Balance zwischen europäischen und nicht europäischen Anbietern. Es wird kein Anspruch auf Repräsentativität erhoben und nur öffentliche Daten herangezogen.

| Kategorie                    | Softwareprodukt            | Anbieter/Hauptentwickler | Open Source | Land |
|------------------------------|----------------------------|--------------------------|-------------|------|
| Datenbanken                  | Microsoft SQL Server       | Microsoft                | nein        | US   |
|                              | Mimer SQL                  | Mimer                    | nein        | SWE  |
|                              | Apache Cassandra           | Apache                   | ja          | US   |
| ERP-Systeme                  | SAP Business One           | SAP                      | nein        | DE   |
|                              | Oracle Fusion Cloud ERP    | Oracle                   | nein        | US   |
|                              | Axelor Open Suite          | Axelor                   | ja          | FR   |
|                              | Salesforce Sales Cloud     | Salesforce               | nein        | US   |
| CRM                          | Atomic CRM                 | Marmelab                 | ja          | FR   |
|                              | SAP Sales Cloud            | SAP                      | nein        | DE   |
|                              | Trello                     | Atlassian                | nein        | US   |
| Projektmanagement            | Notion                     | Notion Labs              | nein        | US   |
|                              | Open Project               | Open Project             | ja          | DE   |
|                              | Zoom                       | Zoom                     | nein        | US   |
| Videokonferenz-Tools         | BigBlueButton              | Blindside Networks       | ja          | CA   |
|                              | Nextcloud Talk             | Nextcloud                | ja          | DE   |
|                              | ChatGPT Enterprise         | OpenAI                   | nein        | US   |
| Große Sprachmodelle (LLMs)   | LeChat Enterprise          | Mistral                  | nein        | FR   |
|                              | Gemini                     | Google                   | nein        | US   |
|                              | Okta Identity Engine       | Okta                     | nein        | US   |
| Identity & Access Management | cidaas                     | WidasConcepts            | nein        | DE   |
|                              | Entra ID                   | Microsoft                | nein        | US   |
|                              | Miro                       | Tactivos                 | nein        | US   |
| Kollaboration                | Conceptboard               | Conceptboard             | nein        | DE   |
|                              | Confluence                 | Atlassian                | nein        | US   |
|                              | Akamai App & API Protector | Akamai Technologies      | nein        | US   |
| Cybersicherheit (WAF)        | Myra Hyperscale WAF        | Myra Security            | nein        | DE   |
|                              | Cloudflare WAF             | Cloudflare               | nein        | US   |

Quelle: eigene Darstellung

Tabelle 5: Exemplarisch untersuchte Softwarelösungen aus verschiedenen Softwarekategorien

Im Kontext dieser Analyse wird der Begriff „Software“ auf die im geschäftlichen Alltag typischerweise eingesetzte Anwendungssoftware begrenzt, die unmittelbar geschäftskritische Prozesse wie ERP, CRM oder die digitale Kollaboration unterstützt. Dieser Fokus auf den Business-Kontext ist bewusst gewählt, um eine klare Abgrenzung zur weitaus umfassenderen Softwarelandschaft und zu tieferen Infrastrukturkomponenten vorzunehmen, die oft eher indirekt über komplexe Architekturen genutzt werden. Ebenso werden individualisierte Eigenentwicklungen ausgeklammert, da diese aufgrund ihres spezifischen Charakters andere Anforderungen an die digitale Souveränität stellen als marktübliche Standardlösungen.

Die besondere Rolle von KI

Die Betrachtung der Souveränität von KI geht über die Metriken klassischer Softwareprodukte hinaus. Das SSF findet Anwendung auf Softwareprodukte, die KI-Systeme als Teilsysteme integrieren, sowie auf KI-zentrierte Softwarelösungen, beispielsweise bei Großen Sprachmodellen (Large Language Models, LLMs). Die LLM Produktkategorie adressiert den Bedarf der eigenständigen Bewertung von KI-Software. KI birgt Herausforderungen bei der Analyse der digitalen Souveränität aufgrund ihres „Black-Box“-Charakter, spezifischen Anforderungen an die Recheninfrastruktur sowie technologische Komplexität der Modellarchitekturen.

| ID       | Souveränitätsziel         | Einflussfaktoren (Originalfassung des Frameworks, eigene Übersetzung)                                                                                                                                                    | Inkludiert | Prüf-Item (Angepasst)                                                                                                               |
|----------|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|-------------------------------------------------------------------------------------------------------------------------------------|
| SOV1.1   | Strategische Souveränität | Sicherstellung, dass Stellen mit maßgeblicher Entscheidungsgewalt über Ihre Dienste innerhalb der EU ansässig sind.                                                                                                      | ja         | Hauptsitz innerhalb der EU.                                                                                                         |
| SOV1.2   |                           | Bewertung der Zusicherungen gegen einen Kontrollwechsel.                                                                                                                                                                 | ja         | Schutzvorkehrungen, die verhindern, dass Unternehmen von außerhalb der EU eine maßgebliche Kontrolle über das Unternehmen erlangen. |
| SOV1.3   |                           | Grad der Abhängigkeit des Anbieters von Finanzierungen aus EU-Quellen.                                                                                                                                                   | ja         | Grad der Finanzierung durch Akteure innerhalb der EU.                                                                               |
| SOV1.4.1 |                           | Ausmaß der <b>Investitionen</b> , Arbeitsplätze und Wertschöpfung innerhalb der EU.                                                                                                                                      | nein       | Summe der Investitionen in den letzten fünf Jahren.                                                                                 |
| SOV1.4.2 |                           | Ausmaß der Investitionen, <b>Arbeitsplätze</b> und Wertschöpfung innerhalb der EU.                                                                                                                                       | ja         | Anteil der Beschäftigten innerhalb der EU.                                                                                          |
| SOV1.5.1 |                           | <b>Beteiligung an EU-Initiativen</b> ; Kohärenz mit den auf EU-Ebene definierten Zielen für digitale, ökologische und industrielle Souveränität.                                                                         | ja         | Dokumentierte Beteiligung an EU-Initiativen.                                                                                        |
| SOV1.5.2 |                           | Beteiligung an EU-Initiativen; <b>Kohärenz mit den auf EU-Ebene definierten Zielen</b> für digitale, ökologische und industrielle Souveränität.                                                                          | nein       | Übereinstimmung der Unternehmensstrategien mit den ökologischen, industriellen und digitalen Zielen der EU.                         |
| SOV1.6   |                           | Fähigkeit zur Aufrechterhaltung eines sicheren Betriebs bei Aufforderungen zur Einstellung oder Aussetzung des Dienstes oder für den Fall, dass die Unterstützung durch den Anbieter eingestellt oder unterbrochen wird. | ja         | Hauptsitz innerhalb der EU.                                                                                                         |

Quelle: [122]; Eigene Darstellung

Tabelle 6: Operationalisierung der Einflussfaktoren für Strategische Souveränität im SSF

4.4 ERLÄUTERUNG DES SOFTWARE-SOUVERÄNITÄTS-FRAMEWORK (SSF)

Das EU SSF formuliert, analog zum CSF, Dimensionen und Einflussfaktoren für digitale Souveränität und überträgt diese in den Software-Kontext. Die Dimensionen, ihre Ziele und formulierte Assessment Kriterien werden nachfolgend eingeführt. Abweichungen und Spezifikationen für den Software-Kontext werden in Abgrenzung zum CSF eingeordnet.

**SOV-1: Strategische Souveränität** konzentriert sich auf die Verankerung des Anbieters im „rechtlichen, finanziellen und industriellen“ Ökosystem der EU. Sie zielt auf Eigentümerstabilität, Steuerungseinfluss und Ausrichtung an den strategischen Prioritäten der EU [122].

Strategische Souveränität setzt auf europäische Jurisdiktion (SOV-1.1), Zusicherungen gegen einen Kontrollwechsel (SOV-1.2), Finanzierungsquellen (SOV-1.3) und Beiträgen zu Wertschöpfung innerhalb der EU (SOV-1.4). Auch berücksichtigt diese Dimension die Beteiligung und Ausrichtung an strategischen Prioritäten der EU (SOV-1.5) und die Fähigkeit, den sicheren Betrieb auch bei Aufforderungen zur Einstellung oder Aussetzung von Diensten aufrechterhalten zu können (SOV-1.6).

Das CSF bleibt bislang vage, ob Präferenzen zu Finanzierungsoptionen bestehen oder bestimmte Gesellschaftsformen bevorzugt werden. Während die jurisdiktionelle Verankerung eindeutig über den juristischen Hauptsitz identifiziert werden kann, können Aspekte wie „Beteiligung an EU-Initiativen“ oder „Investitionen, Arbeitsplätze und Wertschöpfung innerhalb der EU“ unterschiedlich ausgelegt werden. Ein möglicher Proxy für „Investitionen, Arbeitsplätze und Wertschöpfung“ ist beispielsweise der Anteil der Mitarbeitenden innerhalb der EU, um das Ausmaß der Wertschöpfung und Verankerung eines Anbieters in der EU zu messen, wie es in der vorliegenden Umsetzung verwendet wurde. Eine Übersicht zur Operationalisierung der ursprünglichen Einflussfaktoren in Messkriterien findet sich beispielhaft für andere Dimensionen in Tabelle 6.

**SOV-2: Rechtliche & jurisdiktionelle Souveränität** spiegelt die Kontrolle über den Anbieter und dessen operativen Betrieb wider. Ziel ist es, festzustellen, inwieweit digitale Dienste in der europäischen Gerichtsbarkeit verankert und vor externen Rechtsansprüchen geschützt sind [122].

SOV-2 bewertet die Verankerung in EU Jurisdiktion (SOV-2.1), die Durchsetzbarkeit von Nicht-EU-Gesetzen mit extraterritorialer Reichweite (z. B. Chinesisches Cybersicherheits-Gesetz, US CLOUD Act oder FISA) (SOV-

| ID       | Souveränitätsziel     | Einflussfaktoren (Originalfassung des Frameworks, eigene Übersetzung)                                                                                                                                                                             | Inkludiert | Prüf-Item (Angepasst)                                                                                                 |
|----------|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|-----------------------------------------------------------------------------------------------------------------------|
| SOV3.1.1 | Data & AI Sovereignty | Sicherstellung, dass ausschließlich der Kunde und nicht der Anbieter die wirksame Kontrolle über den kryptografischen Zugriff auf seine Daten hat.                                                                                                | ja         | Optionen für Sicherheitsschlüssel und Verschlüsselungsmanagement.                                                     |
| SOV3.1.2 |                       | Sicherstellung, dass ausschließlich der Kunde und nicht der Anbieter die wirksame Kontrolle über den kryptografischen Zugriff auf seine Daten hat.                                                                                                | ja         | Standort der Hardware-Sicherheitsmodule (HSM).                                                                        |
| SOV3.2.1 |                       | <b>Transparenz darüber, wann, wo und durch wen</b> auf Daten zugegriffen wird, einschließlich der Auditierbarkeit der KI-Modellnutzung sowie Mechanismen, die eine unwiderrufliche Löschung von Daten mit verifizierbaren Nachweisen garantieren. | ja         | Zugriff auf Echtzeit-Audit-Logs.                                                                                      |
| SOV3.2.2 |                       | Transparenz darüber, wann, wo und durch wen auf Daten zugegriffen wird, einschließlich der <b>Auditierbarkeit der KI-Modellnutzung</b> sowie Mechanismen, die eine unwiderrufliche Löschung von Daten mit verifizierbaren Nachweisen garantieren. | ja         | Mechanismen zur Auditierung der KI-Modellnutzung.                                                                     |
| SOV3.2.3 |                       | Transparenz darüber, wann, wo und durch wen auf Daten zugegriffen wird, einschließlich der Auditierbarkeit der KI-Modellnutzung sowie Mechanismen, die eine <b>unwiderrufliche Löschung von Daten</b> mit verifizierbaren Nachweisen garantieren. | ja         | Technische oder vertragliche Mechanismen zur Gewährleistung der unwiderruflichen Datenlöschung.                       |
| SOV3.2.4 |                       | Transparenz darüber, wann, wo und durch wen auf Daten zugegriffen wird, einschließlich der Auditierbarkeit der KI-Modellnutzung sowie Mechanismen, die eine <b>unwiderrufliche Löschung von Daten mit verifizierbaren Nachweisen</b> garantieren. | nein       | Verfügbarkeit kryptografischer Löschnachweise.                                                                        |
| SOV3.3   |                       | Strikte Beschränkung der Speicherung und Verarbeitung auf europäische Rechtsräume (Jurisdiktionen) ohne Rückfalloptionen (Fallback) auf Drittstaaten.                                                                                             | ja         | Datenlokalisierung strikt innerhalb der EU, keine Rückfalloptionen auf Drittstaaten.                                  |
| SOV3.4   |                       | Grad, in dem KI-Modelle und Datenpipelines unter EU-Kontrolle entwickelt, trainiert, gehostet und verwaltet werden, um die Abhängigkeit von Technologie-Stacks außerhalb der EU zu minimieren.                                                    | ja         | Ausmaß, in dem KI-Modelle und Datenpipelines unter EU-Kontrolle entwickelt, trainiert, gehostet und verwaltet werden. |

Quelle: [122]; Eigene Darstellung

Tabelle 7: Operationalisierung der Einflussfaktoren für Daten- und KI-Souveränität im SSF

2.2) und die Exponiertheit gegenüber ausländischen Behörden (SOV-2.3). Auch die Anwendbarkeit internationaler Regime (SOV-2.4) und die Jurisdiktion für die Entwicklung und Registrierung von Geistigem Eigentum („Intellectual Property“, IP) fließt in die Bewertung ein (SOV-2.5).

Wie wichtig rechtliche Souveränität ist, zeigte sich im Juni 2025 und Januar 2026. Microsoft musste einräumen, dass der Schutz von EU Daten vor Anfragen durch US Behörden rechtlich nicht lückenlos garantiert werden kann [142] und sich Zusammenarbeit mit Behörden bis hin zur Herausgabe von BitLocker-Wiederherstellungsschlüssel erstreckt [44]. Zu einem ähnlichen Ergebnis kommt ein 2025 veröffentlichtes Gutachten deutscher Rechtswissenschaftler für das Bundesinnenministerium [213]. Eine Gegenperspektive weist darauf hin, dass EU-Tochtergesellschaften als eigenständige Auftragsverarbeiter strikt dem europäischen Recht und der Weisungsgebundenheit der DSGVO unterliegen sollten [142].

**SOV-3: Daten- & KI-Souveränität** adressiert den Schutz, die Kontrolle und die digitale Unabhängigkeit von Datenbeständen und KI-Diensten innerhalb der EU (siehe Tabelle 7). Ziel ist die Gewährleistung der Datensicherheit am Verarbeitungsort sowie ein hoher Grad technologischer Autonomie der Kunden über die eingesetzten KI-Fähigkeiten [122].

Diese Dimension umfasst die Kontrolle über den kryptographischen Zugang zu Daten (Key Management Optionen, Standort von Hardware-Sicherheitsmodulen, welche kryptografische Schlüssel sichern) (SOV-3.1) sowie umfassende Transparenzmechanismen (SOV-3.2). Hierzu zählen Echtzeit-Audit-Logs für Datenflüsse und die Nutzung von KI-Modellen (SOV-3.2.1), Mechanismen zur Auditierung von KI-Modellen (SOV-3.2.2), sowie die nachweisbare und unwiderrufliche Löschung von Daten (SOV-3.2.3). Datensouveränität wird zudem über Datenlokalisierung definiert: Speicherung und Verarbeitung erfolgen ohne Rückfalloptionen („Fallback“) in Drittstaaten (SOV-3.3) und der Grad der EU-Kontrolle über Entwicklung, Training, Hosting und Steuerung von KI-Modellen wird betrachtet (SOV-3.4).



Standard-SaaS-Anbieter (wie Kollaborations- oder CRM-Tools) nutzen für Metadaten oft globale Indizes, um Funktionen wie eine weltweite Suche zu ermöglichen, wodurch ein relevanter Teil des Datenflusses die europäische Jurisdiktion verlässt. Strikte Datensouveränität erreichen nur Lösungen, die eine Lokalisierung von Arbeitsdaten, Metadaten und Service- bzw. Betriebsdaten garantieren. Hierbei werden auch Service-Logs und Telemetriedaten konsequent in der europäischen Jurisdiktion isoliert.

**SOV-4: Operative Souveränität** zielt auf die Sicherstellung der praktischen Fähigkeit europäischer Akteure, Technologien unabhängig von ausländischer Kontrolle zu betreiben und weiterzuentwickeln. Im Fokus stehen die Betriebskontinuität und die Reduzierung externer Abhängigkeiten [122].

Für operative Souveränität werden Möglichkeiten zur barrierefreien Migration von Workloads durch die Nutzung standardisierter Export-Formate (SOV-4.1) sowie Plattformunabhängigkeit (SOV-4.2) betrachtet, um technologische Lock-in-Effekte zu reduzieren. Ein weiteres Kriterium ist die Verfügbarkeit eines EU-basierten Expertenpools mit der Fähigkeit, Services zu operieren und langfristig aufrechtzuerhalten (SOV-4.3). In Erweiterung der in SOV-3 betrachteten Datenlokalisierung wird zudem erfasst, ob Wartung und Support vollständig aus der EU und unter lokaler Gesetzgebung erbracht werden können, ohne dass eine operative Abhängigkeit von Herstellern im Nicht-EU-Ausland besteht (SOV-4.4). Auch tragen die Bereitstellung technischer Dokumentation und Zugang zum Quellcode (SOV-4.5), sowie die örtliche und juristische Kontrolle von kritischen Zulieferern und Subunternehmern in der Servicebereitstellung (SOV-4.6) zur operativen Souveränität bei.

In den letzten Jahren sind neue „souveräne“ Bereitstellungsmodelle entstanden, die – neben Datenlokalisierung, physischer Entkopplung der Server und eigenen EU-Tochtergesellschaften, einen exklusiven Betrieb innerhalb der EU anbieten [52]. Dies kann auch durch Self-Hosting, beispielsweise von OSS, ermöglicht werden, da die operative Kontrolle beim Anwender liegt.

**SOV-5: Lieferketten-Souveränität** bewertet die geografische Herkunft, Transparenz und Resilienz der technologischen Lieferkette. Ziel ist ein resilientes Management globaler Abhängigkeiten. Im Kern steht die Analyse, inwieweit kritische Komponenten und Prozesse unter EU-Kontrolle verbleiben oder Abhängigkeiten von Nicht-EU-Akteuren ausgesetzt sind [122].

Für die Bewertung der Souveränität der Lieferkette von Software rücken die Jurisdiktion von Code-kontrollierender Hardware („code-controlling hardware“) (SOV-5.1), die Herkunft der Software („Origin of Software“ und Jurisdiktion der Entwicklungsteams) (SOV-5.2), Drittanbieter-Abhängigkeit durch Rückgriff auf Nicht-EU-Vendoren, Standorte oder proprietären Code (SOV-5.3), sowie die Transparenz durch Audit-Rechte (SOV-5.4) in den Vordergrund.

Während das EU CSF auch die Herkunft und Fertigung physischer Hardwarekomponenten sowie Rohstoffabhängigkeiten inkludiert, wurden diese Punkte in der vorliegenden Analyse ausgeklammert. Informationen über die Herkunft von Mikrochips oder in Hardware enthaltenen Rohstoffen sind für Softwarehersteller nicht öffentlich zugänglich oder für den Untersuchungsgegenstand von Bedeutung. Außerdem sind die Abhängigkeiten – etwa von Herstellern wie AMD, Intel oder NVIDIA – für nahezu alle Marktteilnehmer gleich und derzeit kaum substituierbar.

**SOV-6: Technologische Souveränität** fokussiert auf Offenheit, Transparenz und Unabhängigkeit im technologischen beziehungsweise Software-Stack ab. Dies soll sicherstellen, dass EU-Akteure Lösungen interoperabel nutzen, auditieren und weiterentwickeln können, ohne in eine Abhängigkeit (Lock-in) von außereuropäischen proprietären Systemen zu geraten [122].

SOV-6 umfasst die Verwendung dokumentierter, nicht-propietärer Schnittstellen (SOV-6.1), die Verfügbarkeit von Software unter Open-Source-Lizenzen (SOV-6.2) sowie die Dokumentation von Architekturen, Datenflüssen und Abhängigkeiten (SOV-6.3). Auch die Abhängigkeit von Nicht-EU Computing, beziehungsweise High-Performance-Computing, Kapazitäten wird betrachtet (SOV-6.4).

Transparenz über Abhängigkeiten kann neben externen Audits über eine Software Bill of Materials (SBOMs) abgebildet werden, welche Bibliotheken und Abhängigkeiten im Code offenlegt. Das Erstellen von SBOMs ist mit dem ab 2026 in Kraft tretenden EU Cyber Resilience Act verpflichtend für „Hersteller von Produkten mit digitalen Elementen“ [115], einschließlich Software-Produkten. Nur für gewisse Produkte werden sie auch überprüft. SBOMs werden allerdings aufgrund von Sicherheitsbedenken in den seltensten Fällen veröffentlicht und nur Geschäftskunden zur Verfügung gestellt. Entsprechend ist die Verfügbarkeit von öffentlichen Daten für dieses Kriterium stark begrenzt.

**SOV-7: Sicherheits- & Compliance-Souveränität** fokussiert auf Cybersicherheit und die Einhaltung europäischer Regulierungen und Standards zur Sicherstellung der Unabhängigkeit von Drittstaaten und der langfristigen Gewährleistung des Betriebs [122].

In die Bewertung fließt ein, inwieweit ein Anbieter durch Zertifizierungen – etwa nach internationalen ISO-Standards (z. B. ISO27001, ISO27017/18, ISO27701, ISO42001), Common Criteria (CC) oder spezifischen nationalen Testaten (BSI C5, SecNumCloud) – nachweisen kann, dass er Sicherheitsanforderungen gerecht wird (SOV-7.1). Außerdem fließen die Dokumentation zur DSGVO-Konformität (SOV-7.2), die Existenz eines exklusiv unter EU-Kontrolle operierenden Security Operations Center (SOC) (SOV-7.3) und EU-konforme Meldung von Sicherheitsvorfällen (SOV-7.4) in die Bewertung ein. Auch vertragliche und technische Möglichkeiten für unabhängige Audits durch EU-Instanzen werden berücksichtigt, wodurch eine transparente und eigenständige Überprüfbarkeit der Sicherheitsmaßnahmen durch europäische Akteure gewährleistet werden soll (SOV-7.5).

Allerdings ist die Existenz eines SOC oder spezifischer Sicherheitszertifizierungen wie Common Criteria maßgeblich von der Kritikalität der Software, dem Kundensegment, der Größe oder Finanzkraft des Softwareanbieters und dem entsprechenden Risikoprofil der verarbeiteten Daten abhängig. Eine differenzierte Einordnung ist daher je nach Softwarekategorie und Einsatzbereich notwendig.

**SOV-8: Ökologische Souveränität.** Nachhaltigkeit wird als Faktor für die langfristige Resilienz und Autonomie gegenüber Rohstoffknappheit und Energieabhängigkeiten betrachtet [122].

Im CSF werden Metriken wie Energieeffizienz (Power Usage Efficiency, PUE), Praktiken der Kreislaufwirtschaft und Bezug von Energie aus erneuerbaren oder kohlenstoffarmen Quellen für den Betrieb bewertet. Während diese Metriken für Cloud etabliert sind, finden sie nur bedingt Anwendung für Softwareprodukte: Software induziert Energieverbrauch in der Hardware. Die gewählte Bereitstellungs-Option (beispielsweise On-Premise selbst-gehostet oder Public Cloud) einer Software hat starken Einfluss auf die Nachhaltigkeit. Auch mit neuen Generationen der Hardware (RAM, CPU, GPU) verändern sich die Nachhaltigkeitsmetriken unabhängig der betriebenen Software. Entsprechend fließt ökologische Souveränität im EU SSF nicht in die Betrachtung ein.

## 4.5 ERGEBNISSE: WIE SOUVERÄN IST DAS SOFTWARE-PORTFOLIO EUROPÄISCHER ORGANISATIONEN HEUTE?

Es existieren zwei primäre Indikatoren für hohe Souveränität von Software: Die Unternehmenszentrale liegt innerhalb der EU und die Bereitstellung erfolgt als Open Source Software (OSS). In der Anwendung des Frameworks korrelieren diese Merkmale eindeutig mit hohen Gesamtwerten (Score) digitaler Souveränität.

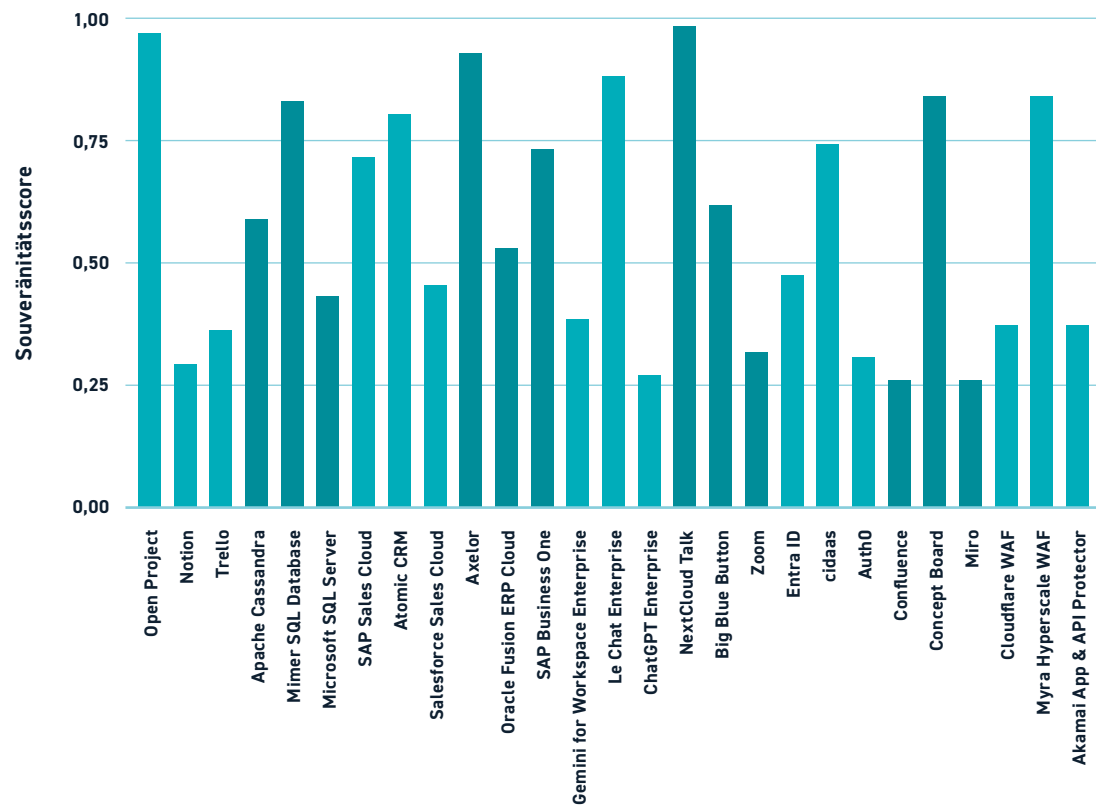
### Dominanz EU-basierter Open-Source-Lösungen

Im Vergleich setzen sich im EU SSF Open-Source-Lösungen (z. B. Open Project, Axelor ERP, Nextcloud Talk) konsistent gegen proprietäre Wettbewerber durch, wobei die spezifische Jurisdiktion (z. B. Deutschland vs. Kanada) über die Spitzenplatzierung entscheidet (siehe Abbildung 23). Im Gegensatz dazu erreichen marktführende Tools wie Trello, Notion, Miro, ChatGPT oder Zoom geringe Souveränitäts Scores (siehe auch Abbildung 24, Abbildung 25 und Abbildung 26).

### Das Souveränitäts-Fundament: Strategische Verankerung und rechtliche Immunität (SOV-1 und SOV-2)

Die Dimensionen der strategischen und jurisdiktionellen Souveränität analysieren die wirtschaftliche Verankerung eines Anbieters im europäischen Wirtschaftsraum sowie dessen rechtliche Bindung an EU-Jurisdiktionen zum Schutz vor extraterritorialen Einflüssen.

**Gesamtergebnis:** Eine jurisdiktionelle Abhängigkeit (SOV-2) durch einen Nicht-EU-Hauptsitz ist kaum durch andere Faktoren kompensierbar. Unter der Annahme eines Schwellenwertes für SEALs bei 0,2 fallen die meisten Nicht-EU-Anbieter bereits aufgrund ihrer Hauptsitze und damit einhergehenden Implikationen aus der Bewertung (zur Erinnerung: Produkte müssen in jeder Dimension ein definiertes Mindestniveau erreichen, hier unter der Annahme, dass mindestens SEAL-1 erreicht werden soll: 0,2).



Quelle: Eigene Darstellung

Abbildung 23: Übersicht der Gesamtergebnisse

**EU versus Nicht-EU:** Nicht-EU-Anbieter, die Arbeitsplätze und Investitionen in der EU generieren oder in EU-Initiativen involviert sind, können in der strategischen Souveränität (SOV-1) punkten, doch bleibt die jurisdiktionelle Abhängigkeit (SOV-2) bestehen. Dies zeigt sich beispielsweise bei Microsoft, Oracle oder Salesforce aufgrund ihrer Firmenzentralen in den USA sowie Entwicklung und primäre Patentanmeldungen außerhalb der EU.

Ergebnisse für CRM und Datenbanken verdeutlichen den Rückstand in den Dimensionen SOV-1, SOV-2 und SOV-5 beispielhaft (siehe Abbildung 27 und Abbildung 28). Während europäische Anbieter mit starker europäischer Präsenz (Mimer und Atomic) gerade bei der jurisdiktionellen Souveränität (SOV-2) punkten, erzielen nicht-europäische Anbieter (Microsoft, Salesforce) geringe Werte. Auch für eine deutsche SAP kann es – je nach Auslegung – Abzüge aufgrund der möglichen Anwendbarkeit internationaler Regime, beispielsweise durch ihren amerikanischen Co-Hauptsitz und eine starke Präsenz auf dem US-Markt geben (siehe Abbildung 27). Auch bei der Betrachtung der Finanzierung durch Nicht-EU Einheiten kann bei SAP auf die Unternehmensanteile institutioneller Investoren aus den USA verwiesen werden [294].

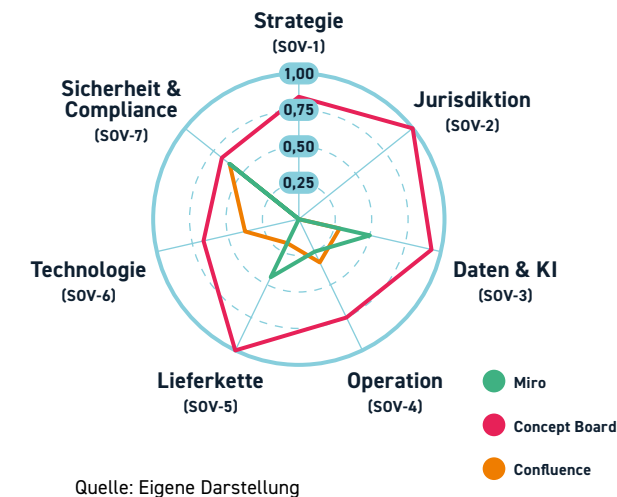
Auch bei Stiftungen für Open Source bestehen, beispielsweise für die Apache Stiftung, trotz dezentraler Kontributoren, Defizite durch die Jurisdiktion des Hauptsitzes und IP Entwicklung und Registrierung in den USA (siehe Abbildung 28).

### Daten- und KI-Souveränität (SOV-3)

Diese Dimension bewertet die Kontrolle über die physische Datenhaltung sowie die kryptografische Hoheit über Informationen und KI-Modelle.

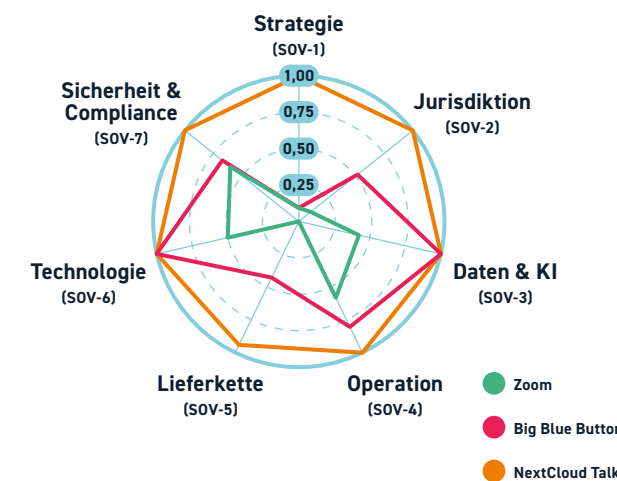
**Gesamtergebnis:** Europäische Anbieter und Open-Source-Lösungen erzielen in SOV-3 hohe Werte, da sie häufig sowohl die physische Datenhaltung innerhalb der EU als auch die vollständige Kontrolle über Verschlüsselung auf europäischer Hardware gewährleisten. Im Gegensatz dazu erreichen Nicht-EU-basierte Lösungen meist nur mittlere Werte (ca. 0,5 bis 0,7).

**SOV-3.3:** Software bieten unterschiedliche Möglichkeiten für Datenlokalisierung, mit Einfluss auf die Anforderung, Daten ohne Rückfalloptionen in Europa zu halten (SOV-3.3). Während eine EU-Lokalisierung von Arbeitsdaten oder Kundinhalten („Customer Content“) bei



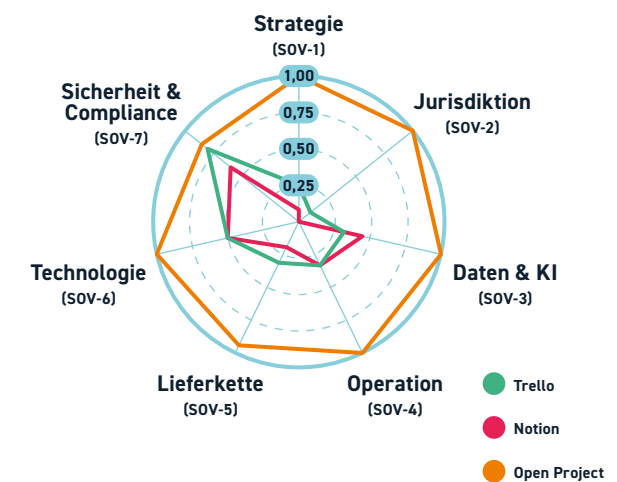
Quelle: Eigene Darstellung

Abbildung 24: Ergebnisse des Scorings – Kollaboration



Quelle: Eigene Darstellung

Abbildung 25: Ergebnisse des Scorings – Videokonferenz-Tools



Quelle: Eigene Darstellung

Abbildung 26: Ergebnisse des Scorings – Projektmanagement

fast allen Softwarelösungen möglich ist, trennt sich das Angebot bei Meta- und Servicedaten (siehe Abbildung 29). Europäische Softwarelösungen, die konsequent innerhalb der EU hosten und operieren, erfüllen Datenresidenz meist über Datentypen hinweg, da sie eine lückenlose Datenlokalisierung ohne die bei globalen Plattformen üblichen Rückfalloptionen auf Drittstaaten sicherstellen. In mehreren Softwarekategorien (bspw. Datenbanken, OSS bzw. Open-Core mit Enterprise Versionen) ist strikte Datenlokalisierung grundsätzlich möglich. In einigen Fällen ermöglichen „souveräne“ Bereitstellungsmodelle (SAP Sovereign Cloud, Oracle Sovereign Cloud oder Microsoft EU Data Boundary) die Lokalisierung der verschiedenen Datentypen.

### Hosting als Einflussfaktor für operationelle Souveränität (SOV-4)

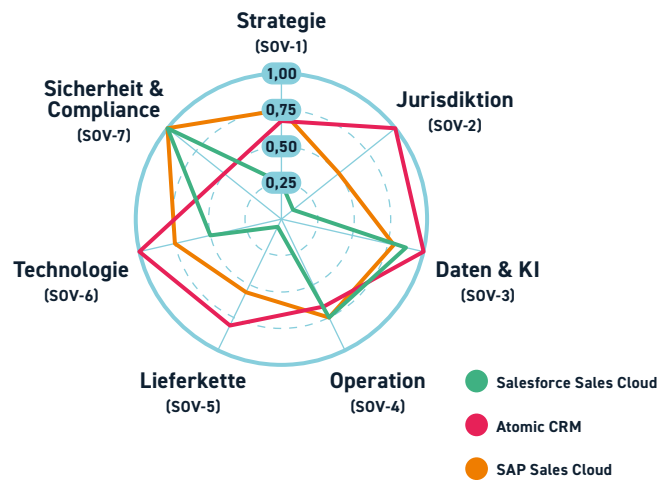
Operationale Souveränität betrachtet die Unabhängigkeit im laufenden Betrieb sowie die Kontrolle über administrative Zugriffe und die Abhängigkeit von kritischen Zulieferern.

**Gesamtergebnis:** Das gewählte Betriebsmodell stellt einen entscheidenden Hebel für die operationelle Souveränität dar. Während Eigenbetrieb (on-prem) maximale Unabhängigkeit von externen Infrastrukturen verspricht, ist dieser für viele Organisationen wegen Ressourcenmangel nicht realistisch oder für bestimmte Software nicht mehr verfügbar. Souveräne Cloud- oder Private Cloud Angebote bieten Alternativen. Während Datenportabilität (SOV-4.1) häufig gewährleistet ist, stellt die Abhängigkeit von kritischen Zulieferern außerhalb der EU (SOV 4.6) mit einem Tiefstwert von 0,19 die größte Schwachstelle dar – auch europäische Anbieter greifen häufig auf kritische Subdienstleister aus Drittstaaten zurück.

**OSS versus proprietär:** OSS dominieren diese Kategorie mit einem Durchschnittswert von 0,88 (gegenüber 0,56 für proprietäre Software), aufgrund von vollständigem Zugriff auf den Quellcode (SOV-4.5), volle Datenportabilität und die Möglichkeit, die Software überall zu betreiben (SOV-4.1). Open-Source-Lösungen ermöglichen durch Eigenbetrieb eine höhere Unabhängigkeit und Gestaltungsmöglichkeiten im operativen Betrieb.

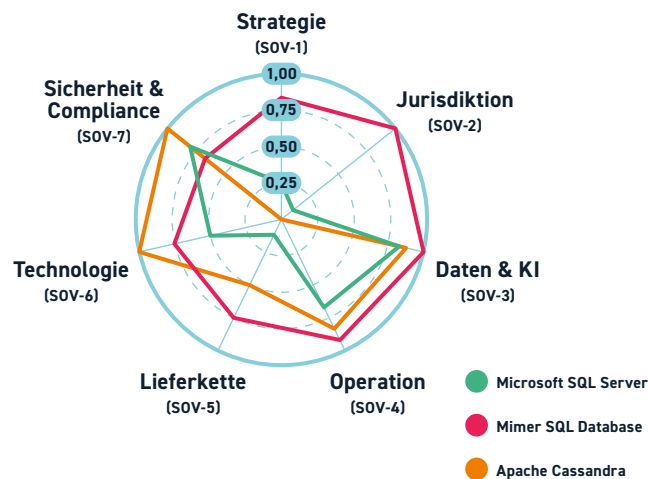
SaaS-Lösungen mit starkem Plattform Lock-in, keiner Möglichkeit zum Selbstbetrieb und Support außerhalb der EU sind mit Werten unter 0,3 Schlusslichter. Viele der untersuchten Produkte werden als SaaS-Modell angeboten, häufig (10 von 27) in den Rechenzentren der US-Hyperscaler AWS, Microsoft Azure oder Google





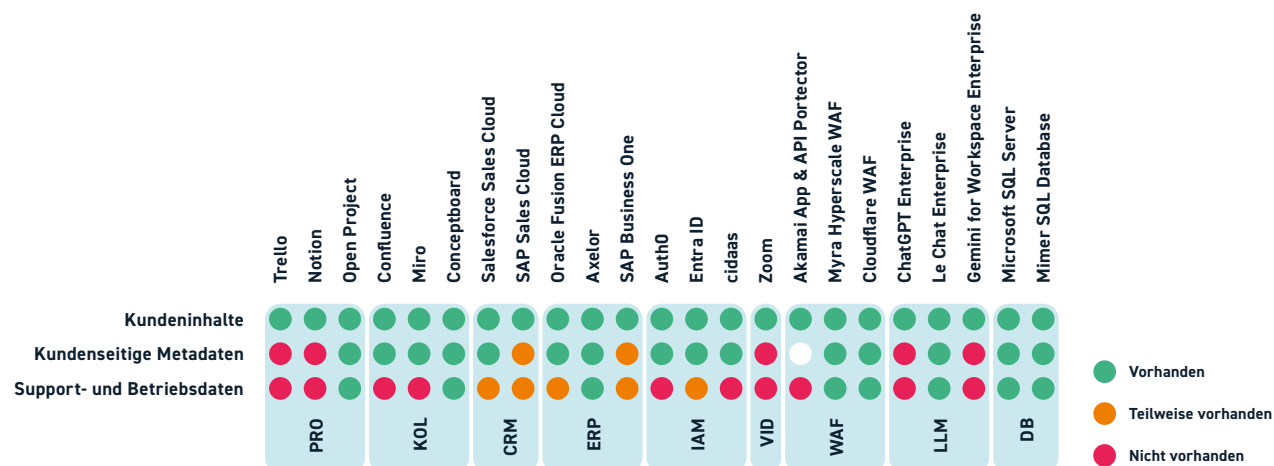
Quelle: Eigene Darstellung

Abbildung 27: Ergebnisse des Scorings – CRM



Quelle: Eigene Darstellung

Abbildung 28: Ergebnisse des Scorings – Datenbanken



Quelle: Eigene Darstellung

Abbildung 29: Optionen für Datenlokalisierung verschiedener Datentypen (exkl. OSS ohne Enterprise Versionen)

Cloud (siehe Tabelle 8). Lösungen wie Trello, Notion und Miro sind als Cloud-native Anwendungen konzipiert, ohne Alternative für den On-Premise Betrieb.

**EU versus Nicht-EU:** Europäische Anbieter erfüllen die Anforderungen an operative Souveränität in den meisten Fällen (siehe Tabelle 8), da die grundlegenden Fähigkeiten und Kapazitäten zum Betrieb ihrer Software in Europa gelagert sind. Auch Modelle wie die Salesforce EU Operating Zone oder die „Sovereign Cloud“-Modelle von Oracle und SAP ermöglichen, dass technischer Support und Wartungsarbeiten von Personal innerhalb der EU erbracht werden.

### Lieferketten-Souveränität als größtes Risiko neben rechtlicher Souveränität (SOV-5)

Die Souveränität der Lieferkette fokussiert sich auf die geografische Herkunft des Quellcodes sowie die Kontrolle über die an der Entwicklung beteiligten Standorte und Infrastrukturen.

**Gesamtergebnis:** Die Lieferketten-Souveränität (SOV-5) zeigt neben der rechtlichen Souveränität die größten Schwachstellen für Nicht-EU Anbieter. Zehn der untersuchten Lösungen fallen unter das Minimum SEAL aufgrund der Standorte von Entwicklungsteams, der Abhängigkeit von Nicht-EU Standorten und dem Standort von Code-kontrollierender Hardware (SOV-5.1) (siehe exemplarische Ergebnisse in Abbildung 30).

| Software                        | Public Cloud |       |     |        | Self-Hosting Option | Private Cloud Option |
|---------------------------------|--------------|-------|-----|--------|---------------------|----------------------|
|                                 | AWS          | Azure | GCP | Andere |                     |                      |
| Trello                          | ●            | ●     | ●   | ●      | ●                   | ●                    |
| Confluence                      | ●            | ●     | ●   | ●      | ●                   | ●                    |
| Notion                          | ●            | ●     | ●   | ●      | ●                   | ●                    |
| Miro                            | ●            | ●     | ●   | ●      | ●                   | ●                    |
| Salesforce Sales Cloud          | ●            | ●     | ●   | ●      | ●                   | ●                    |
| SAP Business One                | ●            | ●     | ●   | ●      | ●                   | ●                    |
| SAP Sales Cloud                 | ●            | ●     | ●   | ●      | ●                   | ●                    |
| Oracle Fusion ERP Cloud         | ●            | ●     | ●   | ●      | ●                   | ●                    |
| Zoom                            | ●            | ●     | ●   | ●      | ●                   | ●                    |
| ChatGPT Enterprise              | ●            | ●     | ●   | ●      | ●                   | ●                    |
| Le Chat Enterprise              | ●            | ●     | ●   | ●      | ●                   | ●                    |
| Gemini for Workspace Enterprise | ●            | ●     | ●   | ●      | ●                   | ●                    |
| Axelor                          | ●            | ●     | ●   | ●      | ●                   | ●                    |
| Conceptboard                    | ●            | ●     | ●   | ●      | ●                   | ●                    |
| Open Project                    | ●            | ●     | ●   | ●      | ●                   | ●                    |
| BigBlueButton                   | ●            | ●     | ●   | ●      | ●                   | ●                    |
| NextCloud Talk                  | ●            | ●     | ●   | ●      | ●                   | ●                    |
| Atomic CRM                      | ●            | ●     | ●   | ●      | ●                   | ●                    |

Quelle: Eigene Darstellung

Tabelle 8: Verfügbare Hostingmodelle

**EU versus Nicht-EU:** Während viele außereuropäische Anbieter zumindest Teile ihrer Entwicklungsteams innerhalb der EU verorten (SOV-5.2), können sie eine Abhängigkeit von außereuropäischen Standorten nicht umgehen (SOV-5.3). Einige europäische Anbieter setzen hingegen vorrangig auf europäische Entwicklerteams, was die Kontrolle über kritische Komponenten und Prozesse der Software-Lieferkette unter EU-Kontrolle belässt.

**SOV-5.2:** Die Verteilung der Entwicklungsstandorte verdeutlicht die Herausforderung: Die Mehrheit der analysierten Anbieter entwickelt ihre Software zumindest teilweise in den USA, was je nach Einbeziehung von Open-Source-Contributoren einen Anteil von 64 % bis 84 % ausmacht. Weitere relevante Standorte außerhalb der EU sind Indien (8 der untersuchten Unternehmen), das Vereinigte Königreich (5), Kanada (4), Australien (4) und Japan (4). Innerhalb Europas sind vor allem Deutschland (7), Frankreich (5) und Irland (3) als Entwicklungsstandorte vertreten. Während größere europäische Unternehmen wie SAP mit den SAP Labs in über 20 Ländern, aber auch Axelor und Mistral, global aufgestellt sind, gibt es Beispiele wie Mimer, welche ihre gesamte Entwicklung in Schweden verorten [210].

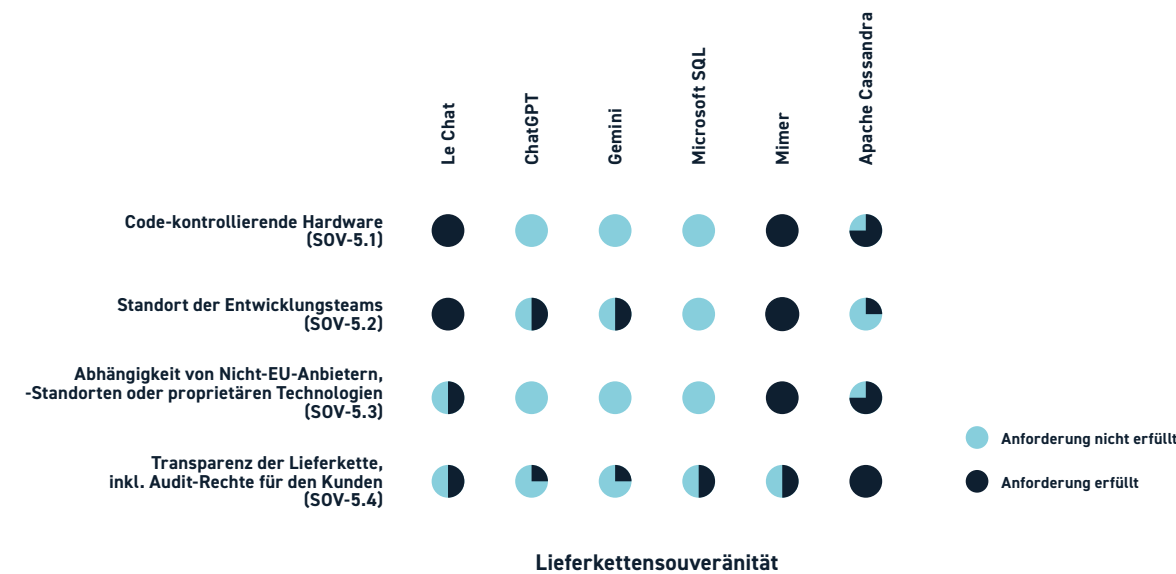
### Technologische Souveränität (SOV-6)

Technologische Souveränität wird durch Offenheit, Transparenz und Unabhängigkeit im zugrunde liegenden Technologie-Stack geprägt.

**Gesamtergebnis:** Während OSS bei Offenheit, Transparenz und Unabhängigkeit unschlagbar ist, können auch proprietäre Lösungen mit standardisierten und offenen APIs und transparenter Dokumentation punkten. Das größte Risiko für technologische Souveränität im Sinne dieses Frameworks sind geschlossene SaaS-Plattformen.

**OSS versus proprietär:** OSS ist in diesem Kontext per Definition transparent und erzielt durch die Nutzung standardisierter und offener Schnittstellen (SOV-6.2) und offener Lizenzen (SOV-6.2) sowie transparente Dokumentation (SOV-6.3) Höchstpunktzahlen in der gesamten Dimension. Geschlossene SaaS-Plattformen fallen im Vergleich dazu deutlich ab (siehe Abbildung 31).

**SOV-6.1:** Eine hohe Schnittstellen-Offenheit zeigen fast alle Anbieter, egal ob OSS oder proprietär. Sie setzen auf gut dokumentierte, REST-basierte APIs. Auch proprietäre Anbieter gewähren zunehmend Einblicke in ihre Architektur über Dokumentation und Whitepaper (Durchschnittswert: 0,87).



Quelle: Eigene Darstellung

**Abbildung 30: Exemplarische Ergebnisse der Lieferketten-Souveränität – LLMs und Datenbanken**

### Compliance Souveränität und das Ökosystem der Zertifizierungen (SOV-7)

Compliance-Souveränität wird durch den Nachweis anerkannter Sicherheitszertifizierungen sowie die Erfüllung spezifischer hoheitlicher Anforderungen an das gesamte Software-Ökosystem definiert.

**Gesamtergebnis:** Sicherheits- und Compliance-Souveränität (SOV-7) stellt die Kategorie mit den höchsten Scores über alle Softwarekategorien hinweg dar (Mittelwert 0,78). Ein Unterschied lässt sich besonders zwischen großen Nicht-EU Anbietern (0,84) und mittelgroßen Nicht-EU Anbietern (0,64) erkennen.

**SOV-7.1:** In der Bewertung zeigt sich eine Differenzierung zwischen allgemeiner Sicherheitskonformität und spezifischen Souveränitätsnachweisen. Während nahezu alle Akteure eine Sicherheitszertifizierung nach ISO 27001 für ihre Organisation vorweisen können, verfügen nur wenige Anbieter über ein BSI C5 oder SecNumCloud Testat. US-amerikanische Anbieter wie Microsoft haben in europäische Standards und Testate wie das deutsche C5, das spanische ENS oder das französische SecNumCloud investiert.

Im Bereich der Open-Source-Lösungen wie OpenProject oder Nextcloud verschiebt sich der Fokus, da hier oft nicht allein die Software zertifiziert ist, sondern das gesamte Ökosystem inklusive der europäischen Hosting-Partner wie Hetzner, OVHcloud oder StackIT. Da

Open-Source-Tools häufig als selbst gehostete Varianten betrieben werden, findet man seltener Zertifikate des Softwareherstellers; die Souveränitätsbewertung erfolgt hier stattdessen über die tatsächliche Bereitstellung. Wird eine Lösung in einem deutschen Rechenzentrum mit ISO 27001 und BSI C5 betrieben, erreicht das Gesamtsystem höhere Werte als eine zertifizierte US-SaaS-Lösung.

### Der Einfluss der Unternehmensgröße auf Souveränitäts-Scores

Außereuropäische Großkonzerne (mehr als 10.000 Mitarbeitende) erzielen im Vergleich zu mittelgroßen außereuropäischen Unternehmen (500–10.000 Mitarbeitende) rundum bessere Werte (siehe Abbildung 32). Besonders deutlich (mehr als 15 %) sind Unterschiede in den Dimensionen Daten/KI (SOV-3), Betrieb (SOV-4), Technologie (SOV-6) und Sicherheit/Compliance (SOV-7). Dies lässt sich auf umfangreiche Compliance-Ressourcen und Zertifizierungen, teils in Europa ansässige Entwicklungs- und Supporteinheiten, sowie die Bereitstellung spezialisierter, souveräner Angebote bei größeren Anbietern zurückführen.

## 4.6 EINORDNUNG DER ERGEBNISSE

Der folgende Abschnitt kontextualisiert die Analyseergebnisse über die betrachteten Dimensionen hinweg. Im Zentrum stehen dabei die Ergebnisse zu Open Source und KI sowie Erkenntnisse über den gewählten Ansatz zur Operationalisierung digitaler Souveränität.

### 4.6.1 Open Source als souveräne Alternative?

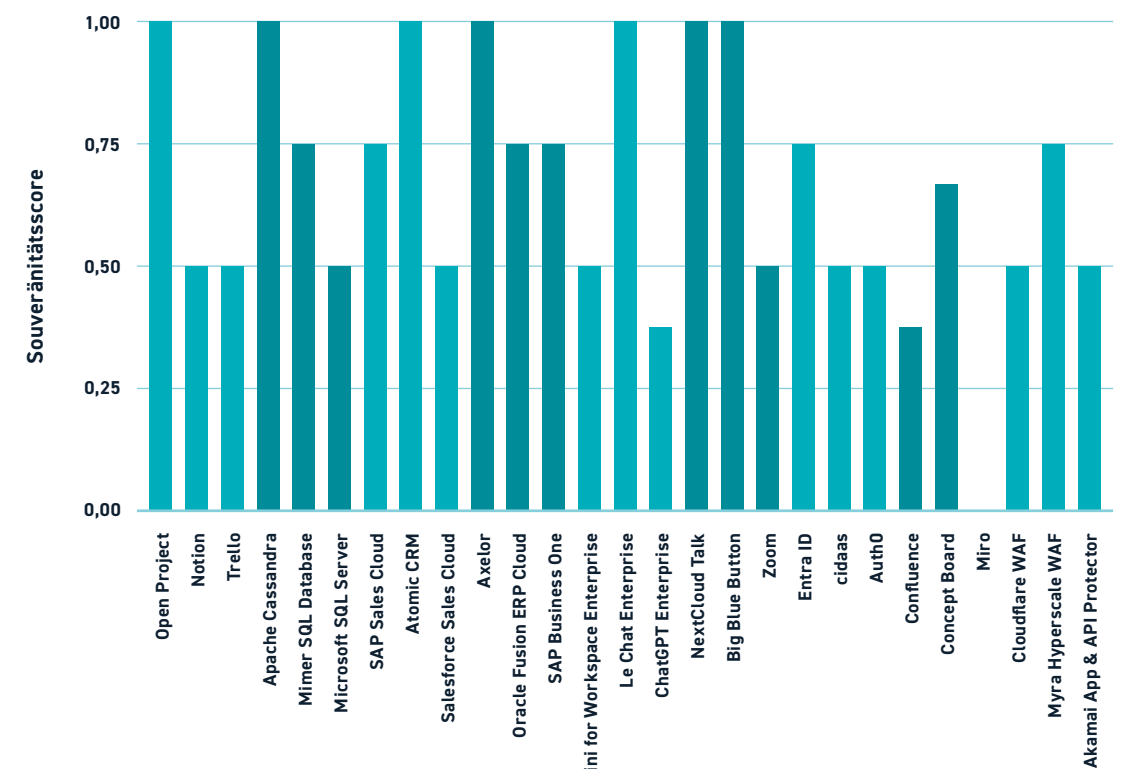
Die politische und strategische Debatte identifiziert Open Source häufig als zentrales Instrument zur Erlangung digitaler Souveränität. Doch eine rein lizenzrechtliche Betrachtung greift zu kurz, da digitale Souveränität über bloße Quelloffenheit hinausgeht.

### Das EU CSF Framework präferiert Eigenschaften von Open Source

Open Source bietet klare Vorteile in den technisch-operativen Dimensionen des Frameworks. OSS punktet durch die Verfügbarkeit unter offenen Lizenzen, die umfassende Rechte zur Prüfung, Modifikation und Umverteilung einräumen. Diese technologische Freiheit erfordert jedoch eine hinreichende Eigenkompetenz; es stellt sich die Frage, inwieweit eine souveräne Nutzung möglich bleibt, wenn die strategische Weiterentwicklung ohne eigene Beiträge („Contributions“) weiterhin maßgeblich von außereuropäischen Kern-Maintainern geprägt wird.

### Abhängigkeiten bestehen durch Konzentration globaler Entwicklungsinfrastruktur

Besonderes Augenmerk verdient die Ebene der Code-kontrollierenden Hardware. Während der Betrieb der Software innerhalb der EU sichergestellt werden kann, sind Implikationen der Konzentration von globaler Entwicklungsinfrastruktur auf US-basierten Plattformen



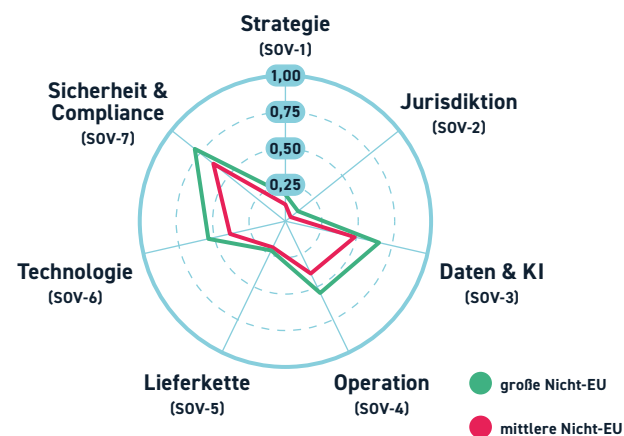
Quelle: Eigene Darstellung

**Abbildung 31: Gesamtscores Technologische Souveränität**



wie GitHub oder HuggingFace zu betrachten. Dass GitHub mittlerweile zum US-Konzern Microsoft gehört, wirft Fragen zur jurisdiktionellen Kontrolle über die „Fabriken“ der Softwareproduktion auf. Auch wenn lokale Kopien oder Forks des Codes eine gewisse Resilienz bieten, bleibt offen, inwieweit die Integrität von Build-Pipelines und der Zugriff auf die weltweite Entwickler-Community gewahrt werden können, wenn die zentrale Koordinationsplattform nicht der EU-Jurisdiktion unterliegt. Dies gilt nicht nur für Plattformen wie GitHub, sondern auch für die Ökosysteme der OSS-Bausteine, die für moderne Softwarearchitekturen verwendet werden, welche gleichfalls im Wesentlichen von US-basierten Unternehmen und Stiftungen geprägt sind.

Offenheit darf nicht pauschal mit Sicherheit oder wirtschaftlicher Überlegenheit gleichgesetzt werden. Bestehende Sicherheitsrisiken unterstreichen, dass Europa robuste Governance-Strukturen entwickeln muss, die Rechenschaftspflicht gewährleisten und sich nicht bloß auf die Code-Inspektion der Community verlassen [16]. Ein Vergleich der Gesamtkosten (TCO) bei Funktionsgleichheit zwischen Open Source und proprietären Tools bleibt weiterhin eine wesentliche Anforderung für den öffentlichen Sektor.



Quelle: Eigene Darstellung

**Abbildung 32: Durchschnittliche Scores für große und mittlere Nicht-EU Anbieter**

## Souveräner Code muss nicht zwangsweise quelloffen sein

Die Debatte über digitale Souveränität muss über die reine Lizenzfrage hinausgehen. Im Sinne der EU-Zielsetzungen für Auditierbarkeit und Autonomie sind kontrollierte Transparenz und Code-Souveränität entscheidend. Ziel ist es, Systeme zu schaffen, die unabhängig von ihrem Geschäftsmodell nachvollziehbar, überprüfbar und unter europäischer Kontrolle bleiben. Souveräner Code in diesem Sinne ist demnach Software, deren Prüfbarkeit nicht nur ein theoretisches Recht ist, sondern durch europäische Instanzen praktisch und unabhängig vollzogen werden kann. Quelloffener Code erfüllt diese Bedingung, stellt jedoch nicht die einzige Option dar.

## 4.6.2 Wie souverän kann ein KI-System sein?

KI verschärft die Souveränitätsdebatte durch eine neue Qualität technologischer Interdependenzen. KI-Systeme benötigen massive Rechenressourcen und hochspezialisiertes Fachwissen, was die im Framework verankerte Kontrolle über den KI-Lebenszyklus – von der Modellentwicklung bis zur Inferenz – vor Herausforderungen stellt.

## Vollständige Kontrolle über den KI-Lebenszyklus ist bislang schwer zu erlangen

Die EU erhebt den Anspruch zur Kontrollierbarkeit über den gesamten KI-Lebenszyklus von der Entwicklung über das Training bis hin zur Bereitstellung und Governance (SOV-3.4). Der EU AI Act stellt zwar eine regulatorische Basis für eine gewisse Kontrollfähigkeit der EU sicher, jedoch führt die Abhängigkeit von proprietären Modellen nicht-europäischer Anbieter zu Defiziten. Diese zeigen sich angesichts fehlender Kontrolle über den Entwicklungsprozess besonders in den Bereichen Strategie und Lieferkette.

Enterprise-Lösungen erfüllen gängigerweise Sichtbarkeit und Nachvollziehbarkeit des Systemzugriffs sowie die Integrität der Datenbehandlung (SOV-3.2). Im EU CSF wird primär die Protokollierung der Modellnutzung gefordert, um eine lückenlose Auditierbarkeit des Nutzerverhaltens und des System-Outputs sicherzustellen. Dies ermöglichen viele Anbieter, damit Organisationen, aus Sicherheitsmotiven, auf Mitarbeiterinteraktionen zugreifen können.

Ein weiterer Kontroll-Aspekt ist die Garantie einer irreversiblen Löschung von Daten (SOV-3.2.3). Für LLMs bedeutet dies auch die Unterbindung von KI-Training auf Unternehmensdaten, was sich schon als Standard im aktuellen Marktangebot etabliert hat. In spezialisierten Fällen, in denen Modelle (z. B. durch Fine-Tuning) auf eigenen Datenbeständen trainiert wurden, erweitert sich dieser Anspruch zum „Machine Unlearning“. Vollwertige Methoden zum selektiven Verlernen von Informationen bei LLMs sind allerdings noch kaum belastbar abzubilden [221], was die praktische Durchsetzbarkeit dieses Kriteriums gegenüber Modellanbietern bislang erschwert.

## Fachkräfte sind eine Säule der KI-Souveränität

Die technologische Komplexität von KI-Systemen bedingt eine Unterscheidung zwischen operativer Beherrschung und strategischer Entwicklungshoheit. Digitale Souveränität bemisst sich nicht nur an der generischen IT-Kompetenz, sondern an den Fähigkeiten, ein KI-System sicher zu operieren und es eigenständig (weiter-)zuentwickeln. Letzteres gestaltet sich im Falle leistungsfähiger KI-Systeme innerhalb der EU als unverhältnismäßig schwierig, angesichts der ungleichen Verteilung von Spitzenkräften im globalen Wettbewerb [53]. So arbeitete eine Mehrheit von KI-Spitzenforschern im Jahr 2022 in den USA (57 %), gefolgt von China (12 %) und dem Vereinigten Königreich (8 %) [238]. Auf Deutschland und Frankreich entfielen jeweils 4 %.

## KI-Inferenz kann Infrastrukturabhängigkeiten und Sicherheitsdefizite befördern

Die Nutzung spezialisierter Computing-Cluster für Inferenz- und Trainingsprozesse nimmt für KI-Systeme eine zentrale Rolle ein (relevant für SOV-3.4 und SOV-5.2). Gleichzeitig stellt dies Anbieter vor Herausforderungen durch weltweit hohe Nachfrage und entsprechende Kosten von europäischer Verfügbarkeit [169]. Dies verdeutlicht das Beispiel von Mistral AI, das in seiner SaaS-Produktversion seit Februar 2025 auch US-amerikanische Rechenkapazitäten der Google Cloud bezieht, um die notwendige Skalierbarkeit für seinen Chatbot-Service zu gewährleisten [297].

Somit entstehen Jurisdiktionsrisiken für Daten im Arbeitsspeicher (*data-in-use*). Als technischer Ausweg können Trusted Execution Environments (TEEs) eine hardwarebasierte Isolierung der Verarbeitung und somit Datensicherheit bei der KI-Inferenz ermöglichen. Die untersuchten nicht europäischen LLM-Angebote

von Google und OpenAI verarbeiten Daten auf Infrastruktur in US-amerikanischem Besitz, ohne die durch TEEs möglichen technischen Garantien für die Vertraulichkeit der *Data-in-use* zu implementieren. Mistral AI ermöglicht durch eine Self-Hosting Option die Wahl vollständig europäischer Serverinfrastruktur.

Das SSF nimmt keine Bewertung der inhaltlichen Funktionalität eines Modells vor. Aspekte wie inhärente Wertvorstellungen oder die kulturelle Anpasstheit von KI-Modellen, die für gesellschaftliche Resilienz von Bedeutung sein können, werden nicht erfasst und finden sich allenfalls indirekt in der Bewertung der Kontrolle über den Trainingsprozess wieder.

## 4.6.3 Limitationen des Ansatzes

Eine fundierte Einordnung der Ergebnisse erfordert auch eine kritische Reflexion der methodischen Rahmenbedingungen und der zugrunde liegenden Datenbasis. Die Übertragung des CSF auf Software offenbart spezifische Herausforderungen, insbesondere hinsichtlich der Übertragbarkeit von Standards aus der öffentlichen EU-Beschaffung auf die heterogenen Bedarfsprofile des breiteren Marktes.

## Explorative Adaption eines neuen Frameworks

Die Anwendung des ursprünglich für Cloud-Infrastrukturen konzipierten Frameworks auf Software-Anwendungen dient primär dem Zweck, die Funktionsmechanismen der Souveränitätsmessung zu validieren und auf den bisher wenig untersuchten Softwarebereich zu übertragen. Diese Übertragung offenbart jedoch methodische Herausforderungen und Limitationen, die bei der Interpretation der Ergebnisse berücksichtigt werden müssen.

Die Beibehaltung der Dimensionen und Gewichtungen des EU CSF ermöglicht eine direkte Gegenüberstellung, zeigt jedoch auch Grenzen auf. Während für Infrastruktur ökologische Aspekte oder physische Sicherheit relevant sind, erfordern Technologien wie KI oder spezialisierte Softwareanwendungen potenziell eine angepasste Gewichtung – etwa mit stärkerem Fokus auf Dateninteroperabilität oder algorithmische Transparenz. Ein flexibles Framework erlaubt zwar diese Anpassung an spezifische Schutzbedarfe über veränderte Gewichtung, birgt jedoch gleichzeitig das Risiko der Manipulation, da sich Ergebnisse durch die Justierung von Gewichtungen stark unterscheiden können. Zudem basiert die Definition der Schwellenwerte für SEALs in

dieser Untersuchung auf mathematischen Mittelwerten, da die internen Berechnungsmethoden der EU DG DIGIT nicht öffentlich verfügbar sind.

**Validität der Informationsbasis und Kontextabhängigkeit**

Aufgrund des explorativen Charakters dieser Analyse basiert sie ausschließlich auf öffentlich zugänglichen Informationen. Dies führt unweigerlich zu Informationsasymmetrien, da interne Audit-Berichte oder vertrauliche Vertragsdetails nicht berücksichtigt werden können. Für belastbare Entscheidungen im Beschaffungswesen ist eine Validierung dieser Indizien durch primäre Datenquellen und detaillierte Befragungen der Softwareanbieter zwingend erforderlich.

Des Weiteren ist zu beachten, dass das zugrundeliegende Framework aus dem Kontext öffentlicher EU-Beschaffungsprozesse stammt. Diese stellen naturgemäß höchste Souveränitätsanforderungen, insbesondere für kritische Daten. Der breitere Markt jenseits des öffentlichen Sektors weist jedoch heterogene Bedarfsprofile auf. Unternehmen in weniger kritischen Industrien priorisieren möglicherweise andere Aspekte der digitalen Souveränität als staatliche Akteure. Das Framework bildet somit einen spezifischen, hochregulierten Standard ab, der nicht uneingeschränkt auf alle marktwirtschaftlichen Szenarien übertragbar ist.

**Abgrenzung zu marktökonomischen Faktoren**

Die vorliegende Analyse nimmt eine Produkt-Betrachtung vor, jedoch keine darüber hinausgehende Analyse auf Organisationsebene. Explizit ausgeklammert bleiben Aspekte wie (Risiko-) Analysen der Lieferketten sowie Untersuchungen zur Marktkonzentration, obwohl diese Faktoren maßgeblich zu Abhängigkeiten beitragen können. Ebenso wurden keine Vergleiche hinsichtlich Feature-Parität oder TCO durchgeführt. Da Kosten und Funktionalität in der Praxis oft entscheidende Auswahlkriterien darstellen, bildet die hier diskutierte Bewertung nur eine – wenn auch kritische – Facette ab.

**4.7 AUSBLICK: JENSEITS TECHNISCHER METRIKEN**

Über die Metriken in Beschaffungs-Frameworks wie dem vorgestellten hinaus sollten zukünftige Analysen zu digitaler Souveränität auch ökonomische Faktoren wie Innovationskraft, Performance und Kosten integrieren, sowie eine präzise Definition der Untersuchungsziele voranstellen. Öffentliche Beschaffung wird ein starker Hebel für digitale Souveränität in Europa bleiben, doch sollten auch andere Aspekte und andere Akteure in Betracht gezogen werden. Beispielsweise werden Investitionen in Zukunftstechnologien und Bereiche mit bestehenden Stärken in der EU ein zentraler Faktor für zukünftige Wettbewerbsfähigkeit darstellen.

**4.7.1 Was können wir aus der Übertragung des CSF auf Software lernen?**

Die Adaption des EU Cloud Sovereignty Frameworks (EU CSF) auf die Software-Ebene (EU SSF) erlaubt nicht nur eine Bewertung einzelner Produkte, sondern liefert einige Erkenntnisse über die Struktur digitaler Abhängigkeiten.

**Interdependenz von Software und Infrastruktur**

Die Bewertung von Softwaresouveränität ist eng verbunden mit den verfügbaren Bereitstellungsoptionen. Da die Wahl des Hosting-Modells direkte Auswirkungen auf die Transparenz der Lieferkette, die physische Datenlokalisierung und den Schutz vor extraterritorialen Zugriffsrechten hat, stellt eine souveräne Cloud-Strategie ein Fundament für Softwaresouveränität dar. Diese Relevanz wird durch die fortschreitende Transformation hin zu Cloud-Native-Strukturen verstärkt: Da moderne digitale Wertschöpfungsprozesse und insbesondere leistungsfähige KI-Systeme zunehmend auf skalierbaren Architekturen fußen, ist die Souveränitätsfrage nicht isoliert auf Ebene der Softwarelizenz, sondern auch hinsichtlich der Kontrolle und Governance des betrieblichen Ökosystems zu beantworten. Die Analyse zeigt, dass Anbieter zunehmend ein Spektrum an Bereitstellungsmodellen entwickeln, um diesen Anforderungen zu begegnen. Für Organisationen bedeutet dies, dass digitale Souveränität nicht mehr zwingend den Verzicht auf Cloud-Technologien impliziert, sondern die bewusste Wahl eines Modells erfordert, das technologische Skalierbarkeit mit rechtlicher und operativer Sicherheit verbindet.

Gleichzeitig verdeutlicht die Übertragung des Frameworks, dass die Dimensionen des CSF für den Software-Layer neu kontextualisiert werden müssen. Während im Infrastruktur-Kontext die physische Kontrolle dominiert, liegt der Fokus bei Software mehr auf rechtlicher und logischer Verfügungsgewalt. Ein „Sovereign Cloud“-Hosting ist eine notwendige, aber keine hinreichende Bedingung: Auch auf souveräner Infrastruktur kann Software durch restriktive Lizenzen (Vendor-Lock-in) oder proprietäre Datenformate Abhängigkeiten erzeugen. Zudem offenbart die Anwendung des Frameworks die Notwendigkeit einer tieferen Betrachtung der Software Supply Chain (z. B. durch SBOMs), da Abhängigkeiten hier granulare Bibliotheken betreffen.

**Marktkonzentration und internationale Akteure**

Die konsequente Anwendung des Frameworks und seiner Ausschlusskriterien (SEALs) auf das untersuchte Portfolio führt dazu, dass lediglich 10 der 27 analysierten Softwareprodukte die Mindestanforderungen an digitale Souveränität erfüllen. Zwar lassen sich in nahezu allen betrachteten Technologiefeldern europäische Alternativen identifizieren, doch mit Ausnahme der SAP im ERP-Segment verfügen diese nur selten über eine marktbeherrschende Stellung. Während auf der Hardwareebene China als zweiter zentraler Akteur neben den USA auftritt, ist das europäische Software-Ökosystem fast ausschließlich durch eine tiefe Verflechtung mit US-Anbietern geprägt. Der Trend zur Cloud-Migration bringt weitere Verflechtungen mit (Cloud) Infrastrukturen, die häufig bei US-Hyperscalern verortet sind.

**4.7.2 Der Beitrag von öffentlicher Beschaffung zur digitalen Souveränität der EU**

Öffentliche Beschaffung kann als strategischer Hebel für die digitale Souveränität Europas dienen. Über die Deckung des unmittelbaren Eigenbedarfs hinaus entfaltet die staatliche Nachfrage eine Signalwirkung am Markt und fungiert als Finanzierungsinstrument für die europäische Industrie.

**Steuerungsfunktion und Hebelwirkung durch Nachfrage**

Das Potenzial der Steuerungsfunktion durch Nachfrage wird durch die makroökonomischen Kennzahlen unterstrichen: Jährlich fließen rund 264 Milliarden Euro – was etwa 1,5 Prozent des EU-BIP entspricht – aus dem europäischen Wirtschaftsraum an außereuropäische

Anbieter ab [160]. Eine auch nur teilweise Neuausrichtung dieser Mittel, über den öffentlichen Sektor, könnte den Aufholprozess von „Made in Europe“-Lösungen unterstützen. Dabei sollte das Ziel jedoch keine Isolation oder Autarkie sein; vielmehr muss die Erlangung strategischer Handlungsfähigkeit in kritischen Bereichen im Vordergrund stehen. Digitale Souveränität fungiert in diesem Kontext als Vorsorge gegen geopolitische Instabilitäten und Etablierung strategischer Handlungsfähigkeit, wobei die öffentliche Beschaffung den Aufbau von Resilienz fördern sollte.

**Die Grenzen der Beschaffung**

Trotz ihrer strategischen Bedeutung darf die öffentliche Beschaffung nicht als alleiniges Allheilmittel für die digitale Souveränität Europas missverstanden werden. Die öffentliche Beschaffung darf nicht die gesamte Last der nationalen Digitalstrategie tragen. Schon heute sind Vergabestellen häufig durch erhebliche bürokratische Hürden in ihrer Handlungsfähigkeit eingeschränkt, was die Umsetzung komplexer Souveränitätskriterien erschwert [160]. Zudem stößt die Beschaffung dort an ihre Grenzen, wo fundamentale technologische Abhängigkeiten bestehen, die marktseitig aktuell nicht aufgelöst werden können: So bleibt etwa der Hardware-Stack eine kritische Abhängigkeit, die durch keinen aktuellen Anbieter im Feld allein durch Nachfragesteuerung kurzfristig behoben werden kann.

Darüber sollte es nicht Aufgabe des Staates, den Markt selbst zu tragen. Die öffentliche Beschaffung muss auch darauf abzielen, private Investitionen durch „Crowding-in“ zu mobilisieren, statt durch staatliche Alleingänge Marktmechanismen zu verdrängen („Crowding-out“).

Letztlich ist digitale Souveränität auch eine Frage des Humankapitals und der internationalen Kooperation. Der Bedarf an Fähigkeiten erfordert eine Bildungs- und Innovationspolitik, die über den Wirkungskreis von Beschaffungsämtern hinausgeht. In einer global vernetzten Welt muss digitale Souveränität zudem im Kontext internationaler Zusammenarbeit und Partnerschaften betrachtet werden, um nicht als Hindernis für globale Kooperationen zu wirken. Die öffentliche Beschaffung ist somit ein Werkzeug, aber nur als Teil eines abgestimmten Instrumentariums aus Wirtschafts-, Bildungs- und Außenpolitik wirksam.



### Fokus auf den „Future Stack“ und Interoperabilität

Eine zukunftsorientierte Beschaffungsstrategie muss anerkennen, dass die Souveränitätsfrage je nach Technologiefeld unterschiedlich beantwortet werden muss. Während bei betriebswirtschaftlicher Standardsoftware wie CRM, ERP und Datenbanken bereits leistungsfähige europäische Alternativen mit hoher operativer Souveränität existieren, stellen SaaS-Lösungen und LLMs in einigen Bereichen neue Herausforderungen dar. Hier muss zwischen kurzfristiger operativer Kontrolle und langfristiger Unabhängigkeit unterschieden werden. Da der Hardware-Stack auf absehbare Zeit eine kritische externe Abhängigkeit bleibt, sollte sich die europäische Förderung – über Beschaffung hinaus – auf Bereiche konzentrieren, in denen bereits Stärken vorhanden sind.

Für die Gestaltung des zukünftigen „Stack“ wird Interoperabilität zu einem entscheidenden Faktor. Wenn Softwareökosysteme durch mögliche KI-gestützte Individualisierung kosteneffizienter werden, drohen nicht-interoperable Systeme auch wirtschaftlich unattraktiv zu werden. Die Beschaffung sollte daher auch auf die Interoperabilität der Middleware fokussieren, um Wahlfreiheit zwischen verschiedenen Anbietern dauerhaft zu sichern.

### 4.7.3 Bedeutet „made in Europe“ automatisch „souverän“?

Ein europäischer Hauptsitz und eine operative Verankerung innerhalb der EU korrelieren mit höheren Scores in der vorliegenden Analyse. Allerdings stellt sie lediglich eine Grundvoraussetzung, keine absolute Garantie für digitale Souveränität dar.

### Geographie als notwendige Bedingung für bestimmte Anforderungen

Europäische Software schneiden in den bewerteten Dimensionen deutlich besser ab als ihre außereuropäischen Vergleichsprodukte. Ein juristischer Hauptsitz und eine starke operative Präsenz innerhalb der EU korrelieren positiv mit höherer Rechtssicherheit, robusteren Datenschutzstandards und einer möglicherweise besseren Auditierbarkeit. Dennoch wäre es ein Trugschluss, das Label „Made in Europe“ mit garantierter digitaler Souveränität gleichzusetzen. Geographie ist in einer global vernetzten technologischen Wertschöpfungskette eine notwendige Bedingung für be-

stimmte Aspekte der digitalen Souveränität, jedoch keinesfalls eine hinreichende oder umfassend garantiert. Außerdem gilt es zu definieren, was ein europäisches Produkt oder Anbieter genau charakterisiert (Hauptsitz, Finanzierungsquellen, Nationalität der Geschäftsführung, etc.).

### Betrachtung des gesamten Technologie-Stack

Europäische Anbieter gewährleisten administrative Kontrolle (durch Rechtsform und Standort), können im technologischen Unterbau jedoch auch auf Abhängigkeiten stoßen. Auch Software-Plattformen mit Sitz in Europa operieren häufig auf einer globalisierten Hardware- und Virtualisierungsebene, die von außereuropäischen Technologien dominiert wird – seien es Chipsätze, Hypervisor oder Container-Orchestrierungen. So besteht zwar Schutz vor direktem rechtlichen Zugriff, aber keine Resilienz gegenüber technologischen Sanktionen oder strategischen Kurswechseln der Zulieferer. Digitale Souveränität definiert sich hier in den nächsten Jahren nicht durch Isolation, sondern durch Handlungsfähigkeit: Die Freiheit, Systeme zu ändern, zu migrieren oder Komponenten auszutauschen, ohne die Betriebsfähigkeit zu verlieren.

Das Modell der sieben (SSF) beziehungsweise acht (CSF) Souveränitätsdimensionen verdeutlicht, dass ein europäischer Firmensitz allein noch keine Garantie für digitale Souveränität ist. Auch Anbieter mit Hauptsitz in der EU können in Teilbereichen – etwa bei der Transparenz ihrer Lieferketten, der Auditierbarkeit oder der Abhängigkeit von proprietären Drittkomponenten – unzureichend abschneiden. Digitale Souveränität darf daher nicht auf einen bloßen Herkunftsnachweis reduziert werden, sondern manifestiert sich primär in den technischen und logischen Charakteristiken eines Produkts, die den Kunden Handlungs- und Wechselfähigkeit ermöglichen.

### Investitionen und das Innovationsdilemma

Digitale Souveränität ist mit Eigentumsverhältnissen und Finanzströmen verbunden. Ein Unternehmen mag juristisch in Europa verwurzelt sein, doch wenn Skalierungskapital primär durch außereuropäisches Venture Capital bereitgestellt wird, verschieben sich strategische Loyalitäten. Darüber hinaus wiegt der Effekt des abfließenden Kapitals mit Ausgaben für Cloud-Infrastruktur und Software-Plattformen im europäischen Markt an Anbieter aus den USA [160]. Dies verhindert, dass Gewinne in Europa akkumuliert und in lokale For-

schung und Entwicklung reinvestiert werden. Es entsteht ein negatives „Flywheel“: Während US-Anbieter teils durch europäische Umsätze ihre Innovationszyklen beschleunigen und ihre technologische Überlegenheit ausbauen, fehlt europäischen Anbietern genau dieses Kapital, um technologisch aufzuschließen. Ohne ein souveränes Ökosystem der Finanzierung, das diesen Kreislauf durchbricht, bleibt das Label „Made in Europe“ möglicherweise nur eine Phase im Lebenszyklus eines Unternehmens oder beschränkt sich auf Nischenmärkte, während die technologische Großwetterlage extern bestimmt wird.

### Digitale Souveränität als Organisationsaufgabe

Abschließend zeigt die Analyse, dass digitale Souveränität kein statischer Endzustand ist, der durch die Beschaffung eines zertifizierten „Made in Europe“-Produkts erreicht und abgehakt werden kann. Vielmehr handelt es sich um einen kontinuierlichen Prozess des Risikomanagements, der tief in der Organisation verankert sein muss. Für Anwenderunternehmen verlagert sich die Verantwortung von der reinen IT-Beschaffung hin zu einer strategischen Governance digitaler Souveränität. Dies erfordert, dass Daten und Anwendungen nach Kritikalität betrachtet und ihnen passende Bereitstellungsmodelle zugewiesen werden – von der Public Cloud für unkritische Workloads bis hin zu streng isolierten Umgebungen für sensible Kernprozesse. Gleichzeitig müssen Organisationen proaktiv Rollen und Verantwortlichkeiten definieren, etwa im Risikomanagement oder der Enterprise Architecture, die Abhängigkeiten in der Software-Lieferkette kontinuierlich überwachen und „Exit-Strategien“ für zentrale Komponenten entwickeln. Digitale Souveränität entsteht innerhalb der Organisationen, wenn die Mechanismen des europäischen Rechtsrahmens, wie dem Data Act, aktiv genutzt werden, um Portabilität vertraglich durchzusetzen und somit eine Wahlfreiheit etablieren, die technologische Lock-in-Effekte verhindert. Digitale Souveränität ist in diesem Sinne weniger eine reine Eigenschaft der Software als vielmehr eine Kompetenz des Anwenders.

# KAPITEL 5



# DIGITAL AFTERLIFE ÜBER DEN DIGITALEN NACHLASS

Weltweites Ranking sozialer Netzwerke  
monatlich aktive Nutzer in Millionen



**62 %**  
der Nutzer verwenden dasselbe  
Passwort für mehrere Dienste

## QUICK-CHECK: DIGITALER NACHLASS

- ☐ **INVENTAR**  
Liste aller Konten, Abos und Krypto-Assets führen
- ☐ **BACKUP**  
Fotos und Dokumente regelmäßig lokal sichern
- ☐ **PRIVATSPHÄRE**  
Festlegen, was ungelesen gelöscht werden soll
- ☐ **VOLLMACHT**  
„Digitalen Bevollmächtigten“ benennen  
– idealerweise notariell –
- ☐ **PASSWÖRTER**  
Master-Passwort für Passwort-Manager sicher hinterlegen
- ☐ **GERÄTE-PIN**  
Zugriff auf Smartphone für MFA-Codes sicherstellen
- ☐ **PLATTFORM-TOOLS**  
Nachlass-Funktionen bei Google, Apple & Meta aktivieren

**68 %**  
der Internetnutzer haben **keinerlei**  
Regelung für ihren digitalen  
Nachlass getroffen

**60 %**  
der Nutzer möchten nicht, dass  
jemand nach ihrem Tod Zugriff  
auf ihre digitalen Inhalte hat

Wofür  
wir  
Accounts  
im Netz  
nutzen

|                    |        |
|--------------------|--------|
| E-Mails:           | 87,8 % |
| Online-Einkäufe:   | 85,9 % |
| Informationssuche: | 80,1 % |
| (Video-)Telefonie: | 78,7 % |
| Online-Banking:    | 70,7 % |
| Soziale Netzwerke: | 59,2 % |
| Online-Verkäufe:   | 29,6 % |

Der Sektor „Grief Tech“ hat weltweit  
einen geschätzten Wert von etwa

**120 Mrd. EUR**

**Fast jeder  
5. Bitcoin**

ist aufgrund fehlender Zugangs-  
daten unwiederbringlich verloren

## Identitätsdiebstahl

**16 Mrd.**  
kompromittierte Zugangsdaten

**1.8 Mrd.**  
davon für Hackerangriffe  
missbraucht

Anzahl eigener Accounts  
Tatsächliche Menge:  
**80–170**

Anzahl eigener Accounts  
Was Nutzer denken:  
**15–20**

**40.000 Alltags-Apps**  
liefern lückenlose Bewegungsprofile  
für den globalen Datenmarkt

**4,9 Mrd.**

Profile Verstorbener könnten bis zum Jahr  
2100 auf Facebook existieren, wodurch die  
Plattform zu einem „digitalen Friedhof“ wird



## 5 DIGITAL AFTERLIFE – ÜBER DEN DIGITALEN NACHLASS

Am 14. März wurde der plötzliche Tod von Erika M. festgestellt. Der Totenschein wies keine Auffälligkeiten auf. Drei Tage später wurde unter ihrem Namen – ohne Kenntnis der Angehörigen – ein Ratenkredit beantragt.

Der Tod von Erika war ruhig, beinahe unspektakulär. Kein Unfall, keine Krankheit, die sich angekündigt hätte. Erika war 52 Jahre alt. Der Abend vor ihrem Tod verlief in alltäglicher Routine: Abendessen mit ihrem Mann Max, Gespräche über Termine und eine anstehende Dienstreise. Am nächsten Morgen war sie nicht mehr aufgewacht. Für ihren Mann, Mitglied der Geschäftsführung eines Industriekonzerns, wurde berufliche Routine nun zur Überlebensstrategie: Er versuchte den Schock zu bewältigen, indem er tat, was er am besten konnte – Dinge ordnen, Abläufe strukturieren und Verantwortung übernehmen.

Erika hatte viele Jahre darauf geachtet, dass die gemeinsamen Angelegenheiten geregelt waren. Sie arbeitete als Juristin, Ordnung war für sie kein Selbstzweck, sondern eine Form von Vorsorge. Im Arbeitszimmer standen mehrere Ordner, sauber beschriftet. Versicherungen, Hausfinanzierung, Vorsorgevollmachten, Patientenverfügung. Verträge, die sie gemeinsam abgeschlossen hatten, andere, die Erika eigenständig geregelt hatte. Max arbeitete sich durch die Unterlagen. Vieles kannte er, manches hatte er lange nicht gesehen, anderes war ihm neu, ohne ihn zu überraschen.

Was er nicht fand, fiel ihm zunächst nicht auf. Das Smartphone seiner Frau lag gesperrt auf dem Schreibtisch, ihr Laptop daneben, zugeklappt. Beide Geräte waren gesichert, Passwörter hatte Erika nie notiert. Max legte sie beiseite. Für die laufenden Angelegenheiten brauchte er sie nicht. Das glaubte er zumindest.

In den ersten Wochen nach Erikas Tod verlief vieles erwartbar. Daueraufträge liefen weiter, Abonnements wurden gekündigt, Rechnungen beglichen. Max regelte die gemeinsamen Konten, die Kinder unterstützten ihn, soweit sie konnten. Es war anstrengend, aber überschaubar. E-Mails gingen weiterhin in Erikas Postfach ein. Max sah die Benachrichtigungen auf dem Sperrbildschirm ihres Handys, las die Betreffzeilen, ließ sie

liegen. Er wollte sich keinen Zugang zu etwas verschaffen, das Erika gehört hatte, solange es nicht notwendig war.

Etwa zwei Wochen nach ihrem Tod begann Max, die Kontoauszüge genauer zu prüfen. Zunächst aus Routine, dann aus Irritation. Es waren keine großen Beträge, die ihm auffielen, sondern kleine, wiederkehrende Abbuchungen über einen Zahlungsdienstleister, den Erika zu Lebzeiten genutzt hatte. 49,90 Euro. 27,30 Euro. 12,00 Euro. Die Beträge wirkten harmlos, aber sie passten zu keinem Vertrag, den Max kannte. Er suchte in den Ordnern, fand nichts. Er fragte die Kinder, niemand wusste etwas davon.



Kurz darauf kam ein Schreiben der Hausbank bezüglich eines gemeinsamen Kontos. Es ging um eine Änderung der Kontaktdaten: Eine E-Mail-Adresse sei kürzlich als primäre Kontaktadresse für Online-Banking-Mitteilungen hinterlegt worden. Max erkannte sie sofort. Es war Erikas E-Mail-Adresse. Dass jemand diese Änderung vorgenommen hatte, während Erika bereits verstorben war, löste bei ihm eine starke Unruhe aus. Ein kurzer Anruf bei der Bank bestätigte: Die Änderung war systemseitig autorisiert worden. Max erstarrte. Das war unmöglich. Er erstattete Anzeige.

In den folgenden Tagen häuften sich ähnliche Hinweise auf Passwortänderungen und neue Logins. Max entschloss sich, das Smartphone entsperren zu lassen. Da er keine PIN hatte, wandte er sich mit der Sterbeurkunde und dem Erbschein direkt an den Hersteller und den Mobilfunkprovider. Unterstützt von einem spezialisierten IT-Forensiker, durchlief er den langwierigen Prozess, um eine Zurücksetzung der Zugangssperren zu erwirken.

Als er schließlich Zugriff hatte, sah er das Ausmaß: In Erikas Posteingang fanden sich Dutzende Nachrichten über Passwort-Zurücksetzungen und Sicherheits-codes. Jemand hatte Zugriff auf Erikas E-Mail-Konto erlangt – vermutlich über ein altes Datenleck und ein wiederverwendetes Passwort. Über die E-Mail-Adresse waren bestehende Konten übernommen worden. Zahlungsdienste, Kundenkonten, Online-Zugänge. Nichts davon war neu angelegt worden. Alles hatte bereits existiert.

Erst Wochen später erhielt Max Post eines ihm unbekannten Finanzdienstleisters, adressiert an Erika M., mit der Bestätigung eines laufenden Kreditverfahrens über einen mittleren fünfstelligen Betrag. Max rief sofort an und erklärte den Todesfall. Die Antwort war ernüchternd: Der Antrag sei korrekt gestellt und die Identität eindeutig verifiziert worden. Mehrfach. Erst durch die polizeilichen Ermittlungen kam die Wahrheit ans Licht: Die Täter hatten hochmoderne Deepfake-Filter genutzt, um Erikas Gesicht auf Basis ihrer Social-Media-Fotos in Echtzeit über das eines Komplizen zu legen. Bei einem Video-Ident-Verfahren war die Täuschung am Bildschirm für den Mitarbeiter nicht zu erkennen gewesen. Für das System war Erika M. eine lebende, aktive Person geblieben.

Max sprach mit Anwälten und Behörden. Es dauerte Monate, bis die meisten Vorgänge geklärt waren. Einiges ließ sich rückgängig machen. Abbuchungen wurden gestoppt, Konten geschlossen. Max führte diesen Kampf zwischen den unzähligen Erledigungen, die ein

Trauerfall mit sich bringt – immer unter der emotionalen Belastung des unmittelbaren Verlustes. Nicht mehr rückgängig machen ließ sich die Erkenntnis, wie schutzlos dieser Zeitraum zwischen dem physischen Tod und der endgültigen Stilllegung des digitalen Nachlasses gewesen war. Erika hatte vieles richtig gemacht. Was sie versäumt hatte, war der digitale Teil ihrer Vorsorge. Nicht aus Gleichgültigkeit, sondern mangels Bewusstsein über die Folgen.

## 5.1 DIGITALE EXISTENZ UND DAS SCHUTZVAKUUM NACH DEM TOD

Identität ist längst nicht mehr ausschließlich an den physischen Körper oder staatlich dokumentierte Merkmale gebunden. Sie definiert sich heute als die Gesamtheit aller personenbezogenen Daten, Online-Accounts, biometrischen Merkmalen und digitalen Spuren, die eine Person im Laufe ihres Lebens erzeugt [214]. Diese Identität manifestiert sich in digitalen Infrastrukturen, Kommunikationsarchiven und algorithmisch verarbeiteten Verhaltensmustern und entwickelt sich von simplen Daten hin zu einem komplexen digitalen Schatten, der E-Mail-Konten, soziale Netzwerke, Cloud-Speicher und digitale Vertragsverhältnisse umfasst. Dieser Zustand wird zunehmend als „informativer Körper“ beschrieben. Diese Daten – einschließlich gespeicherter Stimmen, Texte und Verhaltensmuster – sind kein bloßer Besitz. Da sie Werte, Gedanken und soziale Beziehungen widerspiegeln, werden sie als eine Erweiterung des menschlichen Körpers betrachtet: Unsere Daten sind wir selbst in digitaler Form [20], [78], [140], [261].

Diese digitale Existenz endet nicht automatisch mit dem biologischen Tod eines Menschen. Während dieser juristisch einen klaren Statuswechsel markiert, entsteht digital ein Zustand der Unschärfe [20], [214]. Zwischen dem Lebensende und dem tatsächlichen Ende der digitalen Existenz öffnet sich ein Übergangszeitraum, der weder technisch noch rechtlich eindeutig geregelt ist [214]. In diesem Zeitraum laufen Systeme weiter und Konten bleiben aktiv. Da digitale Identitäten hochgradig vernetzt sind und über technische Schnittstellen sowie Datenaustauschmechanismen ineinandergreifen, bewerten automatisierte Systeme die Authentizität einer Identität nicht anhand des biologischen Status, sondern anhand konsistenter Nutzungsmuster, erfolgreicher Logins und historischer Zahlungsströme. Für diese Prüfmechanismen bleibt eine verstorbene Person daher unter Umständen eine vollständig valide Identität. Diese Entkopplung von menschlichem Lebensende und

digitaler Persistenz erzeugt ein Schutzvakuum, das erhebliche Risiken für Hinterbliebene, Institutionen und die Integrität digitaler Systeme birgt [78].

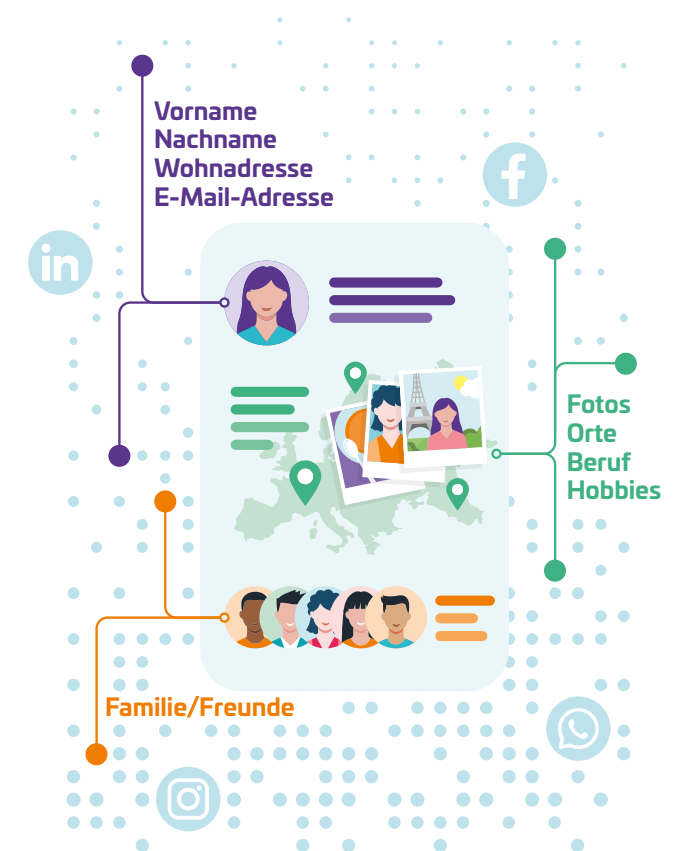
Daraus ergibt sich die Notwendigkeit eines umfassenden digitalen Identitätsschutzes. Dieser definiert sich als die Gesamtheit aller präventiven und reaktiven Maßnahmen, die darauf abzielen, die Integrität, Authentizität und Vertraulichkeit einer digitalen Existenz über ihren gesamten Lebenszyklus und darüber hinaus zu bewahren. Er dient dazu, die vernetzte Identität vor unbefugtem Zugriff, Manipulation oder missbräuchlicher Aneignung durch Dritte zu schützen. Damit ist der Identitätsschutz keine reine Frage des technischen Datenschutzes, sondern eine Frage der Menschenwürde, da er die Integrität der Person selbst betrifft. Während sich dieser Schutz bereits zu Lebzeiten als komplex erweist, wird er nach dem Tod besonders fragil, da die aktive Kontrolle durch die betroffene Person entfällt [78], während die digitale Identität in den Systemen technisch weiterlebt.

Ein wirksamer Identitätsschutz muss daher die postmortale Ebene zwingend einschließen, da durch den Missbrauch der Daten Verstorbener die Integrität der Person über den Tod hinaus verletzt wird [261].

Bereits heute sind Kriminelle in der Lage, aus wenigen öffentlich zugänglichen Datenpunkten detaillierte Profile zu erstellen. Namen, Fotos, berufliche Angaben, frühere Wohnorte oder öffentlich sichtbare Beziehungen reichen aus, um digitale Identitäten anzureichern und glaubwürdig fortzuführen. Diese Praxis wird durch soziale Netzwerke und offene Plattformen deutlich erleichtert. Der digitale Schatten eines Menschen ist dynamisch, wächst mit jeder Interaktion, jedem Beitrag und jeder gespeicherten Information, oft ohne dass den Nutzern das Ausmaß dieser Datenspur bewusst ist [214], [248]. Außerdem ist er reproduzierbar und potenziell manipulierbar.

Mit dem Einsatz Künstlicher Intelligenz (KI) entsteht dabei eine neue Dimension des Missbrauchs. Deepfakes sind längst kein Nischenphänomen mehr, sondern finden zunehmend Eingang in alltägliche Kommunikationskontexte. Bild-, Video- und Audiofälschungen erreichen ein Niveau, das für Laien kaum noch von authentischem Material zu unterscheiden ist. Diese Entwicklung verschärft das Problem digitaler Identität nach dem Tod erheblich, da sie nicht nur bestehende Daten nutzt, sondern aktiv neue, scheinbar authentische Inhalte erzeugt. Besonders problematisch sind Deepfakes Verstorbener, die gezielt für politische Einflussnahme, Betrugsdelikte oder finanzielle Manipu-

lation eingesetzt werden können. Auch Formen einer sogenannten digitalen Wiederauferstehung gewinnen an Bedeutung, etwa durch Voicebots oder Chatbots, die auf Basis vorhandener Daten Kommunikationsverhalten imitieren [6]. Im Bereich der Re-Creation der Digital Afterlife Industry (siehe Kapitel 5.3) nutzen sogenannte Griefbots generative KI, um aktiv neue Inhalte in der Tonalität des Verstorbenen zu erzeugen, statt lediglich statische Datensätze zu wiederholen [6], [173]. Wie weit diese technologische Simulation der Präsenz bereits reicht, zeigt das Beispiel des verstorbenen Robert Kardashian, dessen Hologramm eine vorbereitete Botschaft in lebensechter Optik und Stimme wiedergab [17]. Parallel zu diesen High-Tech-Simulationen verändern hybride Bestattungskonzepte zunehmend die analoge Gedenkkultur. QR-Codes auf physischen Grabsteinen verknüpfen dabei den Friedhofsort mit digitalen Gedenkseiten, auf denen multimediale Inhalte wie Fotos und Lebensläufe für Besucher hinterlegt sind [6].





Diese Situation stellt Hinterbliebene vor erhebliche Herausforderungen. Während analoge Nachlässe klaren rechtlichen Regelungen folgen, bleibt der digitale Nachlass häufig fragmentiert und unübersichtlich. Er ist als konsequente Erweiterung des analogen Erbes zu verstehen und umfasst alle Spuren und Werte, die eine Person im Netz hinterlässt – von Benutzerkonten bei sozialen Netzwerken und E-Mail-Postfächern über Kryptowerte bis hin zu privaten Fotos in der Cloud [214].

Die Umsetzung des digitalen Nachlasses scheitert oft an der technischen Realität: Zugriffsrechte fehlen, Passwörter sind unbekannt und Anbieter reagieren nicht oder verlangen schwer zu erbringende formale Nachweise. Gleichzeitig laufen digitale Systeme weiter und erzeugen neue Risiken.

Digitale Nachlässe sind somit kein Randthema, sondern ein strukturelles Phänomen mit rechtlichen, technischen und ethischen Implikationen. Die fehlende Synchronisation zwischen menschlichem Lebensende und digitaler Persistenz macht deutlich, dass bestehende Konzepte von Identität, Verantwortung und Schutz nicht mehr ausreichen, um den Anforderungen digitaler Infrastrukturen gerecht zu werden [214], [269].

## 5.2 UNSER DIGITALER FUSS- ABDRUCK UND DIE ILLUSION DER KONTROLLE

Ein zentrales strukturelles Risiko liegt in den alltäglichen digitalen Routinen der Nutzenden selbst. Sicherheitskritische Praktiken sind weit verbreitet und wirken über den Tod hinaus fort. So verwenden laut weltweiten Erhebungen 62 Prozent der Nutzer identische oder nur leicht variierte Passwörter für verschiedene Online-Dienste parallel [219]. Demgegenüber steht eine noch geringe Verbreitung von Hilfsmitteln: In Deutschland nutzen lediglich etwa 50 Prozent der Anwender einen Passwort-Manager zur Sicherung ihrer digitalen Identitäten [47]. Diese Gewohnheit mag im Alltag aus Bequemlichkeit oder Zeitmangel entstehen, entfaltet jedoch nach dem Tod eine besondere Brisanz. Gelingt es Dritten, Zugriff auf ein zentrales Konto – etwa ein E-Mail-Postfach – zu erlangen, lassen sich darüber zahlreiche weitere Konten übernehmen, ohne dass jemand eingreift. Passwort-Zurücksetzungen, Authentifizierungsprozesse und Identitätsprüfungen greifen auf genau diese zentralen Knotenpunkte zurück.

Diese Risiken sind eingebettet in eine fast flächendeckende Internetnutzung in Deutschland. 97 Prozent der 16- bis 74-Jährigen sind online, wobei die Nutzungsrate selbst bei den 65- bis 74-Jährigen bei 90 Prozent liegt. Neben der Kommunikation via E-Mail (88 Prozent) und Videotelefonie (79 Prozent) ist die aktive Teilnahme an sozialen Netzwerken für 59 Prozent der Bevölkerung ein fester Bestandteil des Alltags und digitalen Fußabdrucks [320]. Diese Vernetzung wird durch die digitale Verwaltung ergänzt, wobei 59 Prozent der Bürger online mit Behörden kommunizieren und 34 Prozent ihre Termine bei öffentlichen Einrichtungen oder Krankenkassen über das Internet koordinieren [320].

Besonders intensiv spiegelt sich auch das E-Commerce-Verhalten wider. 86 Prozent der über 16-Jährigen bestellen Waren oder Dienstleistungen im Internet. Außerdem zeigt sich ein ausgeprägter Konsum rein digitaler Inhalte: 42 Prozent der Befragten beziehen Filme und Musik als Stream oder Download, während digitale Bücher und Presseerzeugnisse von 19 Prozent genutzt werden. Auch die Reise- und Freizeitplanung ist ein wesentlicher Faktor, insbesondere durch die Buchung von Eintrittskarten (32 Prozent), Unterkünften (29 Prozent) und Transportmitteln (27 Prozent). Abgerundet wird dieses Profil durch die weite Verbreitung von Online-Banking (71 Prozent) und den gelegentlichen Verkauf eigener Waren durch knapp ein Drittel der Bevölkerung [320].

Das resultierende digitale Erbe unserer modernen Gesellschaft erweist sich als zunehmend komplex und unterliegt einer stetigen Evolution. Während digitales Erbe früher primär mit E-Mail-Konten assoziiert wurde, umfasst es heute neben sozialen Medien und Online-Banking auch gespeicherte Fotos, Videos und Nachrichten sowie virtuelle Währungen, Verhaltensdaten und sogar KI-generierte Avatare [214]. Trotz dieser Vielfalt unterschätzen viele Menschen die Anzahl ihrer digitalen Konten erheblich; es herrscht eine Illusion der Kontrolle [252]. Eine Untersuchung aus dem Jahr 2018 belegte bereits, dass Nutzer ihre Online-Konten im Median auf lediglich 15 schätzten, während objektive Scans ihrer E-Mail-Postfächer tatsächlich 80 Konten nachwiesen [167]. Da diese Fehlwahrnehmung selbst im technikaffinen, akademischen Umfeld auftrat, gilt sie als Ausdruck begrenzter Rationalität – eine kognitive Kapazitätsgrenze, die über alle Bildungsschichten hinweg besteht.

Im Jahr 2026 ist diese Kluft historisch groß: Rund 95 Prozent der Deutschen glauben, insgesamt weniger als 10 Online-Konten zu besitzen [29]. Die objektive Realität zeigt jedoch eine Belastung von durchschnittlich 170

Passwörtern pro Person [260]. Methodisch basieren diese Realitätswerte auf der Auswertung von Nutzerdaten bei Passwort-Manager-Anbietern. Da nicht jeder Mensch solche Hilfsmittel nutzt, verdeutlicht dieser Wert vor allem die extreme Komplexität für Personen, die ihren digitalen Alltag aktiv verwalten. Diese starke Unterschätzung führt dazu, dass heute nur noch circa 6 Prozent der tatsächlichen digitalen Präsenz bewusst wahrgenommen werden. Diese Wahrnehmungslücke lässt sich durch die Verfügbarkeitsheuristik erklären [248]: Menschen erinnern sich primär an die Dienste, die sie täglich oder wöchentlich nutzen, wie etwa E-Mail-Provider, soziale Netzwerke oder Online-Banking-Portale. Konten, die für einmalige Transaktionen – beispielsweise den Kauf eines speziellen Produkts in einem Nischen-Webshop, die Registrierung für eine zeitlich begrenzte Dienstleistung oder die Übernachtung im Ausland – erstellt wurden, verschwinden fast unmittelbar nach dem Zeitraum der Nutzung aus dem aktiven Gedächtnis. Dennoch bleiben diese Konten in den Datenbanken der Anbieter als aktive Identitäten bestehen und vergrößern die Angriffsfläche für potenzielle Datenleaks, ohne dass sich Nutzer dieser Gefahr bewusst sind [151]. Zusätzlich erfassen zehntausende Smartphone-Apps im Hintergrund das Standort- und Surfverhalten der Nutzer und speichern diese Daten zur weiteren Verwertung bei externen Datenhändlern. Diese lückenlosen Bewegungsprofile offenbaren weit mehr als Konsumgewohnheiten, sie gewähren tiefe Einblicke in intime Lebensumstände und gesundheitliche Routinen. Die Aufdeckung solcher privater Rückzugsorte macht Individuen bereits zu Lebzeiten anfällig für Manipulation, soziale Diskreditierung oder Stalking [89].

Die langfristigen Folgen dieser Konten-Akkumulation zeigen sich in den Dimensionen der großen Plattformen. Im Ranking der größten sozialen Netzwerke und Messenger nach der Anzahl der Nutzer belegte Facebook im Februar 2025 mit rund 3,07 Milliarden monatlichen aktiven Nutzern den ersten Platz. Auf Platz zwei folgte mit etwa 2,53 Milliarden das zu Google gehörende Videoportal YouTube. Rang drei ging mit jeweils zwei Milliarden Nutzern weltweit an Instagram und den Messaging-Dienst WhatsApp [344]. Bis zum Jahr 2100 könnten so bis zu 4,9 Milliarden Profile Verstorbener auf Facebook existieren, wodurch die Plattform zu einem „digitalen Friedhof“ würde [20], [93], [263].

## 5.3 RISIKEN UND GEFAHREN

Das digitale Selbst überdauert den physischen Körper oft auf unbestimmte Zeit. Im Gegensatz zu physischen Gütern verwittern digitale Inhalte nicht. Social-Media-Profile, ruhende Cloud-Speicher oder E-Mail-Konten verbleiben auf Servern, sofern sie nicht aktiv gelöscht werden [93] oder automatisierten Löschroutinen der Anbieter zum Opfer fallen, die zunehmend inaktive Konten nach Zeiträumen von sechs Monaten bis zwei Jahren entfernen. Forschende aus den Bereichen der digitalen Kultur und der Mensch-Computer-Interaktion bezeichnen diese dauerhafte Präsenz als „Informationsleichen“ – digitale Konten und Daten Verstorbener, die ohne Aufsicht auf Servern verbleiben [93], [261], [262].

Diese ewige Präsenz birgt Sicherheitsrisiken, da Informationsleichen aus Sicht der Cybersecurity als „Zombie-Accounts“ die Angriffsfläche massiv erhöhen können. Konkret werden so Benutzerkonten bezeichnet, die nach einem Jobwechsel oder dem Verlust der Zugangsdaten – oder dem Tod des Nutzers – nicht konsequent gelöscht oder deaktiviert wurden und so als herrenlose Zugänge in Systemen verbleiben. Da diese „ruhenden Identitäten“ oft über schwache oder veraltete Passwörter verfügen und nicht aktiv überwacht werden, dienen sie Angreifern als Eintrittstore, um unbemerkt in Netzwerke einzudringen [209], [214], [262], [353].

### Nekro-Ökonomie

In der aktuellen Debatte wird vor der Entstehung einer sogenannten „Nekro-Ökonomie“ [88] gewarnt, in der die Daten Verstorbener als wertvoller Rohstoff für die Werbewirtschaft und die KI-Industrie ausgebeutet werden, indem sie zum Training von Algorithmen – oder um Rückschlüsse auf lebende Angehörige zu ziehen – genutzt werden [6]. In diesem Kontext agieren große Tech-Konzerne wie Google, Meta und Apple faktisch als „digitale Bestatter“ [78], [214], [261], [262]. Sie kontrollieren das globale digitale Erbe und entscheiden durch Algorithmen und Nutzungsbedingungen darüber, wer erinnert oder gelöscht wird. Da diese Konzerne keine neutralen Archivare, sondern profitorientierte Unternehmen sind, droht bei Strategieänderungen oder Plattformschließungen ein massiver Verlust kollektiver menschlicher Geschichte [261]. Es entsteht somit ein Spannungsfeld zwischen dem individuellen Recht auf Privatsphäre und dem gesellschaftlichen Interesse an der Bewahrung historischer Daten. Daraus leitet sich die Forderung ab, digitale Überreste als kollektives Kulturgut zu betrachten und analog zu physischen Archiven unter besonderen Schutz zu stellen [261].

Diese nekro-ökonomische Logik der Datenverarbeitung beschränkt sich jedoch nicht nur auf die offiziellen Plattformbetreiber, sondern zeigt sich auch in der missbräuchlichen Aneignung durch Dritte. Profile mit hohem „digitalen Statuskapital“ (hoher Status, viele Follower) werden dabei zu einer wertvollen Ressource für Cyberkriminelle. Hacker „ernten“ den sozialen Status des Verstorbenen, um deren über Jahre aufgebaute Glaubwürdigkeit als Werkzeug für Desinformationskampagnen auszunutzen [251]. In dieser informellen Ebene der Nekro-Ökonomie wird die Identität Verstorbener zudem für die Selbstdarstellung anderer instrumentalisiert: Bei falschen Todesmeldungen beispielsweise nutzen Akteure die virale Dynamik der Nachricht, um das eigene Ansehen auf Kosten der Integrität der Betroffenen zu steigern [251]. Ohne autorisierte Nachlasskontakte verbreiten sich Gerüchte unkontrolliert, was das digitale Andenken dauerhaft beschädigen kann [304].

**Neue Dimensionen der Manipulation: KI und Social Engineering 2.0**

Die Integration von KI verleiht dem Identitätsmissbrauch eine neue Qualität. Sogenannte „neuronale Echos“ – KI-gestützte Simulationen (Griebots) – können das Online-Selbst eines Verstorbenen nahezu perfekt reproduzieren, indem sie Sprache, Tonfall, Argumentationsmuster und Reaktionsweisen so präzise nachahmen, dass sie für Dritte kaum noch von realer Kommunikation zu unterscheiden sind [78], [93]. Ohne Kennzeichnung drohen Täuschung und Integritätsverlust, da KI Worte generieren kann, die die reale Person nie geäußert hat [93]. Diese Technologie ermöglicht „Social Engineering 2.0“: Angreifer können Deepfake-Audio nutzen, um Vertrauen bei Angehörigen oder Geschäftspartnern zu erschleichen und betrügerische Handlungen zu legitimieren, sowie Deepfakes Verstorbener für politische oder finanzielle Manipulation einsetzen [93]. Darüber hinaus lassen sich durch die Kombination von Datenfragmenten mehrerer Individuen neue synthetische Identitäten erschaffen, bei denen aus den digitalen Spuren von zwei bis drei Verstorbenen eine scheinbar reale, jedoch unreale digitale ID konstruiert wird.

Neben diesen direkten Angriffen stellt die wachsende Digital Afterlife Industry ein neues Lieferketten-Risiko dar. Diese Branche lässt sich funktional in vier Hauptbereiche unterteilen: Informationsmanagement (z. B. Passwort-Tresore), posthume Nachrichtendienste, Online-Gedenkdienste sowie die technologisch fortgeschrittenen Re-Creation Services [78], [214], [262]. Ein Datenleck bei diesen Drittanbietern würde hochsensiblen private Daten wie Chat-Historien und Sprachproben

offenlegen und die Intimsphäre massiv gefährden [173]. Es besteht die Gefahr einer affektiven Ausbeutung, bei der sensible Trauerbekundungen kommerzieller Logik unterworfen werden [250]. Zudem könnten Firmen diese Daten für KI-Training oder Werbealgorithmen ausbeuten, was als Verletzung der Menschenwürde betrachtet wird [140], [173], [261], [262].

Wenn kein Nachlass geregelt ist, können private Informationen durch zukünftige Datenleaks an die Öffentlichkeit gelangen, ohne dass sich die betroffene Person noch wehren kann [261]. Studien belegen zudem eine wachsende Sensibilisierung für diese Problematik: So äußern bereits 61 Prozent der Verbraucher die Sorge, dass insbesondere die Identitäten Verstorbener anfällig für derartigen Missbrauch sind [209].

**Wirtschaftliche Folgerisiken**

Die finanziellen Folgen eines vernachlässigten digitalen Nachlasses sind groß, wenngleich sie statistisch schwer zu greifen sind. Angesichts durchschnittlicher Beerdigungskosten von rund 13.000 Euro [332] in Deutschland wird das zusätzliche finanzielle Risiko durch postmortalen Identitätsmissbrauch oft unterschätzt. Während die Bestattungskosten eine bekannte Größe darstellen, existieren zum digitalen Missbrauch bislang keine spezifischen Kennzahlen, da diese Fälle meist dezentral gemeldet und unter allgemeinem Betrug geführt werden. Legt man jedoch Zahlen zum Identitätsdiebstahl bei Lebenden zugrunde, liegt der durchschnittliche finanzielle Schaden in Deutschland bei etwa 1.366 Euro pro Fall [282]. Es ist davon auszugehen, dass dieser Wert bei Verstorbenen höher liegt, da der Missbrauch aufgrund der fehlenden Überwachung der Konten oft deutlich länger unentdeckt bleibt.

Dass dieses Phänomen, das sogenannte „Ghosting“, in den USA mit jährlich über 1,1 Millionen Fällen wesentlich verbreiteter scheint [135], lässt sich auf die dortige zentrale Meldestelle für Verbraucherbetrug und die Systematik der Social Security Number (SSN) zurückführen, die oft als alleiniger Identitätsnachweis ausreicht. Für den deutschen Kontext ergibt sich die Gefahr jedoch primär aus der bereits in den vorangegangenen Abschnitten beschriebenen technologischen Verschiebung: Während hiesige Sicherheitsstandards wie das Video-Ident-Verfahren lange als Hürde galten, ermöglichen es KI-gestützte Deepfakes zunehmend, biometrische Identifikationsprozesse zu unterwandern.

Die ökonomische Logik hinter diesem Missbrauch wird auf den Marktplätzen des Darknets sichtbar, wo sogenannte „Fullz“-Pakete – komplette Identitätssätze bestehend aus Name, SSN, Geburtsdatum und Adresse – für 20 bis 100 USD gehandelt werden [326]. Datensätze von Verstorbenen, sogenannte „Dead Fullz“, sind bereits für 1 bis 3 USD erhältlich und dienen oft als Basis für die Eröffnung von Bankkonten zur Geldwäsche [308]. Neben kriminellen Missbrauch führt die sogenannte „Subscription Creep“ zu einem schleichenden Vermögensverlust [41], denn Verträge für Streaming, Cloud-Speicher oder Software-Lizenzen enden nicht automatisch mit dem Tod. Ohne aktive Vorsorge fließen so über Monate hinweg Gelder aus dem Erbe an Dienstleister ab. Besonders gravierend ist das Risiko zudem bei digitalen Vermögenswerten: Schätzungen zufolge sind bereits 11 bis 18 Prozent des gesamten Bitcoin-Bestands aufgrund fehlender Zugriffsschlüssel – auch durch Todesfälle – dauerhaft verloren [249]. Das digitale Erbe wird so ohne Verwaltung entweder zur Beute für Kriminelle oder verliert durch automatisierte Abbuchungen sowie unzugängliche Assets sukzessive an Wert.

**5.4 RECHTLICHE UND TECHNISCHE HERAUSFORDERUNGEN**

In der modernen Rechtsprechung und Techniksoziologie markiert der Übergang zum digitalen Zeitalter eine Zäsur für das Erbrecht. Fast jede verstorbene Person hinterlässt heute digitale Spuren – manche auch als Teil eines geheimen Onlinelebens: E-Mails, Chatverläufe auf Smartphones sowie Konten bei Bezahldiensten wie PayPal oder Internethandelsplattformen [269]. Digitale Vermögenswerte lassen sich durch vier Eckpfeiler charakterisieren: Erstens existieren sie ausschließlich digital und werden zweitens lokal, in der Cloud oder auf einer Blockchain gespeichert. Drittens besitzen sie einen finanziellen oder emotionalen Wert und zeichnen sich viertens durch „Quasi-Eigentumsrechte“ für die Nutzenden aus. Dies umfasst sowohl materielle Werte wie Kryptowährungen und Non-fungible Token (NFT)-Kunstwerke als auch immaterielle Inhalte [206], [262]. Über den monetären Aspekt hinaus können dabei auch Verhaltens- oder Gesundheitsdaten eine tiefe emotionale Bedeutung erlangen – etwa das Wissen um die Musik, die ein geliebter Mensch an seinem Todestag hörte [252].

Trotz dieser Bedeutung hinkt das Rechtssystem der Entwicklung hinterher. Die Entstehung digitalen Eigentums hat eine Revolution der Rechtsobjekte ausgelöst, doch der unklare Status stellt das Erbrecht vor mas-

sive Herausforderungen [353]. Digitale Vermögenswerte können rechtlich nicht vollständig als klassische Eigentumsobjekte charakterisiert werden, da sie im Gegensatz zu physischen Gütern zwingend auf technische Ausrüstung und externe Dienstleister angewiesen sind [353]. Dieser Umstand vertieft ein bestehendes Schutzvakuum: Während die EU-Datenschutz-Grundverordnung (DSGVO) gemäß Erwägungsgrund 27 verstorbene Personen explizit von ihrem Geltungsbereich ausnimmt, navigieren Familien und Unternehmen durch unklares Terrain. Diese Unsicherheit entsteht vor allem dadurch, dass der Zugriff auf Konten oft an den Nutzungsbedingungen der Plattformbetreiber scheitert, die den Zugang für Dritte vertraglich ausschließen. Zudem handelt es sich bei digitalen Inhalten meist um geteilte Daten: Da private Nachrichten Verstorbener untrennbar mit der Privatsphäre lebender Kommunikationspartner verknüpft sind, kollidiert das Auskunftsinteresse der Hinterbliebenen direkt mit dem fortbestehenden Datenschutzrecht dieser Dritten. Ohne spezifische nationale Gesetzgebung bleibt somit ungeklärt, wie das Erbrecht gegenüber diesen technischen und datenschutzrechtlichen Barrieren durchgesetzt werden kann [78], [93], [269].

**Internationale Rechtslage und nationale Unterschiede**

Frankreich agiert hierbei als Vorreiter: Das Gesetz für eine digitale Republik von 2016 schafft ein explizites Recht, verbindliche Anweisungen für den Verbleib personenbezogener Daten nach dem Tod zu hinterlassen [78]. Erben können dort Konten schließen oder Daten einsehen, sofern dies notwendig ist, wenngleich fehlende allgemeine Richtlinien die praktische Umsetzung noch erschweren [93].

Deutschland hingegen gehört zu den *ipso iure*-Nachfolgesystemen, in denen der Nachlass gemäß § 1942 BGB automatisch mit dem Tod auf die Erben übergeht. Ein Grundsatzurteil des Bundesgerichtshofs (BGH) vom Juli 2018 stellte klar, dass Verträge für digitale Konten vererbbar sind. Im Fall einer verstorbenen 15-Jährigen erzwangen die Eltern den Zugang zum Facebook-Konto. Der BGH entschied gemäß § 1922 BGB, dass Erben universell in alle Rechte und Pflichten eintreten. Zwar hat der BGH mit seinem Grundsatzurteil eine funktionale Gleichstellung geschaffen, indem er digitale Inhalte analog zu physischen Briefen behandelte und so den Zugang für die Erben ermöglichte [93], [349], [353]. Dennoch bleibt die systematische Hürde von § 90 BGB bestehen: Da Daten rechtlich nicht als Sachen zum Anfassen gelten, erben Hinterbliebene kein direktes



Eigentum, sondern lediglich die Position im Nutzungsvertrag mit dem Provider, also das Recht auf Zugang [206], [353].

### Plattformen als digitale Gatekeeper

Trotz rechtlicher Erfolge scheitert der digitale Nachlass in der Praxis oft an der technischen Umsetzung. Plattformen wie Facebook oder Google kontrollieren als „digitale Gatekeeper“ durch ihre spezifische Architektur – die sogenannten Affordanzen –, wer Zugang erhält und wie an eine Person erinnert wird [6], [78], [80], [173], [214], [248], [304]. Affordanzen bezeichnen dabei die Handlungsmöglichkeiten, die eine Plattform bietet oder verweigert. Dieses Machtungleichgewicht führt dazu, dass private Konzerne durch technische Erlaubnisse oder Verbote über die posthume Identität entscheiden, oft ohne die tatsächlichen Wünsche der Betroffenen zu kennen [80], [261], [304]. Dies entzieht sowohl den Verstorbenen als auch den Angehörigen die Kontrolle.

Das Feld des digitalen Nachlass ist geprägt von einer auffälligen Abwesenheit staatlicher Regulierung, wodurch digitale Dienstanbieter eine enorme Machtposition einnehmen [6]. Möglicherweise lässt sich dieser Mangel an verbindlichen Regeln durch das gesellschaftliche Unbehagen erklären, das die Auseinandersetzung mit dem Lebensende auslöst [229]. Hinzu kommt eine gravierende Wissenslücke: Etwa 85 Prozent der Facebook-Nutzer sind sich der auf Facebook verfügbaren Funktion für Nachlasskontakte überhaupt nicht bewusst [93]. Da einheitliche Standards und Schnittstellen fehlen, greifen Nutzer häufig auf riskante Workarounds wie die Passwortweitergabe zurück. Dies verstößt jedoch nicht nur gegen die Nutzungsbedingungen der Anbieter, sondern wird durch moderne Sicherheitsmechanismen wie Biometrie oder Multi-Faktor-Authentifizierung (MFA) technisch zunehmend verunmöglicht [323].

### Das ethische Dilemma: Digital Dead Body Management

Zentral bleibt der Konflikt zwischen dem Schutz der Privatsphäre der verstorbenen Person und den Eigentumsinteressen der Erben [214], [353]. In diesem Zusammenhang wurde das Konzept des „Digital Dead Body Management“ entwickelt, welches die Verwaltung digitaler Überreste adressiert und fordert, den Toten „Restrechte auf Würde und Respekt“ einzuräumen [20]. Dabei gilt es, den Schutz des digitalen Privatgeheimnisses (den postmortalen Datenschutz) gegen das Bedürfnis der Hinterbliebenen nach Aufarbeitung, Abschluss

und Heilung abzuwägen [20], [140], [173]. Da digitale Spuren von E-Mails bis hin zu Cloud-Fotos einen hohen emotionalen und spirituellen Wert besitzen, werden sie als wesentlicher Teil der Privatsphäre eingestuft [353].

Gleichzeitig sind diese Daten fragile historische Quellen. Da sie auf privaten Plattformen liegen, die kommerziellen Interessen folgen, ist ihre Bewahrung als kollektives Erbe ungewiss [20], [80]. Es stellt sich zudem die Frage, ob das Vertragsrecht Erbenden den vollen Zugriff und die Möglichkeit zur weiteren Nutzung von Social-Media-Konten gewähren sollte. Die Interessen der Erben decken sich nicht zwangsläufig mit denen der Plattformen, der Gesellschaft oder den mutmaßlichen Wünschen der Verstorbenen [229].

Letztlich zeigt sich, dass die Nachlassregelung derzeit oft an der technischen Realisierbarkeit und einem mangelnden Bewusstsein für Identitätsschutz scheitert, während der Bereich postmortaler Identität – insbesondere im Kontext von KI – weitgehend unreguliert bleibt. In der aktuellen Debatte wird daher ein erweitertes Recht auf digitale Identität diskutiert: das Recht, die eigene Lebensgeschichte selbst zu gestalten. Bisher wurde Privatsphäre vor allem als Schutz vor Eingriffen anderer verstanden. Die neue Interpretation betont jedoch eine aktive Dimension, bei der es um die Freiheit geht, die eigene Identität im digitalen Raum so zu entwickeln, wie man selbst gesehen werden möchte. Als rechtliche Basis dienen hierfür zwei Säulen der EU-Grundrechtecharta, Artikel 7 (Schutz des Privatlebens) und Artikel 8 (Schutz personenbezogener Daten). Experten schlagen vor, diese Rechte enger zu verknüpfen, um ein umfassendes Recht auf digitale Identität zu schaffen [229].

## 5.5 GANZHEITLICHE LÖSUNGSSTRATEGIEN UND HANDLUNGSBEDARF FÜR DIE ZUKUNFT

### Was Individuen tun sollten: Planung und Hinterbliebenen-Support

Die Planung des digitalen Nachlasses ist heute ebenso wichtig wie ein klassisches Testament. In Deutschland gibt es kein digitales Sondererbrecht, stattdessen gehen digitale Inhalte und Verträge nach dem Prinzip der Gesamtrechtsnachfolge automatisch auf die Erben über [3], [214], [310]. Die folgenden Punkte dienen dabei als erste Orientierung und allgemeine Information. Sie erheben keinen Anspruch auf Vollständigkeit und müssen unter Berücksichtigung der jeweiligen individuellen Situation betrachtet werden.

### Für Vorsorgende: Den digitalen Nachlass planen [3], [22], [214], [245], [252], [288], [310]

Um Angehörigen langwierige Prozesse zu ersparen, sollten Privatpersonen rechtzeitig aktiv werden.

#### 1. Bestandsaufnahme und Inventar:

- Erstellen Sie eine Liste aller Online-Konten, E-Mail-Adressen und Cloud-Dienste.
- Dokumentieren Sie auch Abonnements (Streaming, Shopping) und Finanzkonten (Online-Banking, Kryptowährungen).
- Sichern Sie persönliche Daten wie Fotos regelmäßig lokal auf externen Datenträgern, um den Zugriff unabhängig von Plattformen zu gewährleisten.

#### 2. Festlegung von Vertraulichkeit:

- Legen Sie explizit fest, welche Inhalte (z. B. private Chats, Browser-Verläufe) nach Ihrem Tod ungelesen gelöscht werden sollen. Dies schützt Ihr postmortales Persönlichkeitsrecht und verhindert, dass Angehörige ungewollt auf sensible Informationen stoßen.

#### 3. Rechtliche Absicherung:

- Hinterlegen Sie eine spezielle „digitale Vollmacht“ oder regeln Sie den Nachlass in einem Testament.
- Bestimmen Sie eine Vertrauensperson als „digitalen Bevollmächtigten“. Sie können anweisen, dass bestimmte Datenbereiche ohne Sichtung durch Dritte vernichtet werden müssen.
- Eine notariell beurkundete Vollmacht bietet im Rechtsverkehr mit Providern die höchste Akzeptanz und Sicherheit.

#### 4. Zugangsmanagement:

- Nutzen Sie einen Passwort-Manager als zentrale Lösung.
- Stellen Sie sicher, dass Ihre Vertrauensperson Zugriff auf das Master-Passwort erhält (z. B. durch Hinterlegung beim Notar oder in einem Schließfach).
- Sorgen Sie dafür, dass Erben Zugriff auf Ihr Smartphone haben, um Codes der MFA empfangen zu können.

#### 5. Plattforminterne Lösungen:

- Konfigurieren Sie bereits zu Lebzeiten die Erbfall-Funktionen der großen Anbieter, wie den „Nachlasskontakt“ bei Apple und Meta oder den „Inaktiven Kontomanager“ bei Google.

### Für Angehörige und Erben [3], [22], [214], [245], [310]

Im Todesfall müssen Angehörige oft schnell handeln, um Kosten und Datenverlust zu vermeiden.

#### 1. Sichtung der Unterlagen:

- Suchen Sie nach dem Inventarverzeichnis, der Vollmacht oder dem Testament.
- Prüfen Sie Kontoauszüge auf laufende Abbuchungen für digitale Dienste.

## 2. Identifikation und Kündigung:

- Melden Sie den Todesfall unter Vorlage der Sterbeurkunde (und ggf. des Erbscheins) bei den jeweiligen Diensteanbietern.
- Kündigen Sie laufende Verträge und Abonnements zeitnah, da diese im Rahmen der Erbfolge auf Sie übergegangen sind.

## 3. Umgang mit Profilen:

- Entscheiden Sie, ob Konten in sozialen Netzwerken gelöscht oder in einen „Gedenkzustand“ versetzt werden sollen. Beachten Sie dabei etwaige Löschanordnungen des Verstorbenen für sensible Datenbereiche, um dessen Privatsphäre zu wahren.
- Sichern Sie wichtige digitale Erinnerungen (Fotos, Nachrichten), bevor ein Konto endgültig gelöscht wird, da viele Anbieter nach der Löschung keine Daten mehr herausgeben.

## 4. Rechtliche Durchsetzung:

- Berufen Sie sich bei Bedarf auf das BGH-Urteil von 2018/2020, das Erben grundsätzlich den Zugriff auf die Konten Verstorbener zuspricht.

## Anforderungen an die professionelle rechtliche Gestaltung und Beratung

Über die private Planung hinaus ergeben sich für die rechtssichere Umsetzung durch Experten (wie Rechtsanwälte und Notare) spezifische Standards [3], [214], [310]:

- **Vermeidung von Sicherheitsrisiken:** Passwörter sollten niemals direkt in das Testament geschrieben werden, da dieses nach der Eröffnung beim Nachlassgericht öffentlich einsehbar sein kann.
- **Differenzierung der Vollmachten:** Verträge sollten präzise zwischen administrativen Befugnissen (z. B. Account-Löschung) und dem Zugriff auf höchstpersönliche Kommunikation (z. B. Privat-Chats) unterscheiden.

- **Wahrung des Persönlichkeitsrechts:** Eine professionelle Gestaltung beinhaltet die Abwägung zwischen dem Informationsinteresse der Erben und dem Schutz der Privatsphäre des Verstorbenen. Hierbei kann vereinbart werden, dass der Notar die Löschung sensibler Daten überwacht, bevor Dritte eine Einsichtsmöglichkeit erhalten.

- **Rechtliche Einordnung:** Die gesetzliche Erbfolge in Deutschland umfasst den digitalen Nachlass zwar bereits, eine explizite Regelung erleichtert die praktische Abwicklung gegenüber Providern jedoch.

- **Internationaler Kontext:** Für Konten bei US-Anbietern sollten Vollmachten so formuliert sein, dass sie auch internationale Zugriffsstandards erfüllen, um die Zusammenarbeit mit den Providern zu verbessern [22], [288].

## Was die Politik tun sollte: Regulatorische Weichenstellungen

Um die strukturelle Schutzlücke zwischen dem biologischen Lebensende und der digitalen Persistenz zu schließen, ist der Gesetzgeber gefordert, verlässliche Infrastrukturen zu schaffen.

- **Zentrales Nachlassregister:** Ein Schwerpunkt liegt auf der Einführung eines zentralen digitalen Nachlassregisters gemäß des Entwurfs § 1959a BGB-E, das Erben das Auffinden von Online-Konten analog zur klassischen Kontenabfrage ermöglicht [42]. Ergänzend wird eine gesetzliche Informationspflicht für Anbieter empfohlen, um Nutzer proaktiv über die Vererbbarkeit ihrer Daten aufzuklären [214].

- **Automatisierte Identitätsprüfung:** Zur Beschleunigung dieses Prozesses plant die Bundesregierung, die Identitätsprüfung der Erben über die Deutschland-ID zu automatisieren [55]. Die Bundesrechtsanwaltskammer mahnt hierbei strikte Datenschutzvorgaben an, um den Missbrauch sensibler Daten zu verhindern [42].

- **Postmortaler Datenschutz:** Es bedarf einer präzisen rechtlichen Differenzierung des Nachlasses in persönlichkeitsbasierte, eigentumsrechtsbasierte und zusammengesetzte Daten [353]. Nur so können Plattformen effektiv zur Bereitstellung von Schnittstellen verpflichtet werden, ohne das postmortale Persönlichkeitsrecht zu verletzen [6].

## Was Unternehmen tun sollten

Unternehmen sollten den digitalen Nachlass durch operativ handhabbare Maßnahmen adressieren:

- **Account-Hygiene:** Regelmäßige Überprüfung inaktiver Konten und automatisiertes De-Provisioning (Koppelung von HR-Offboarding an IT-Workflows) schützen „ruhende Identitäten“ vor Missbrauch [22], [93].

- **Transparenz in der Kommunikation:** Anbieter sollten in ihren AGB verständlich klären, was mit Accounts, Abos und Lizenzen im Todesfall geschieht, und Klauseln zur Vererbbarkeit deutlich kennzeichnen. Ein vereinfachter Zugang für Erben – etwa durch die Akzeptanz digitaler Nachweise statt postalischer Original-Urkunden – reduziert den Verwaltungsaufwand auf beiden Seiten [3], [214].

## Europäische Lösungen

In Europa entstehen wegweisende Ansätze für eine rechtssichere digitale Nachlassregelung. Die eIDAS-2.0-Verordnung verankert das Modell der Self-Sovereign Identity (SSI), das bis 2026/2027 zur Einführung digitaler Identitäts-Wallets (EUDI Wallets) führen soll [119], [38]. Dieses System ermöglicht intelligente Erbfolge („Smart Successions“): Über Mechanismen wie einen „Dead Man's Switch“ (eine Art digitalen Notfallschalter) können digitale Schlüssel nach einem verifizierten Todesnachweis automatisch und verschlüsselt an Erben übertragen werden [6], [113]. Ergänzt werden kann dies durch regulatorische Rahmenbedingungen wie die European Law Institute Model Rules für den Datenzugriff [124] oder das französische Modell, das bereits ein gesetzliches Recht auf „digitales Sterben“ vorsieht [78].

Zur praktischen Umsetzung gibt es eine Vielzahl europäischer Anbieter (Auszug/Beispiele):

- Organisatorische Plattformen: Die deutsche Lösung Userwill unterstützt bei der strukturierten Nachlassverwaltung (z. B. Kontenlöschung, Abo-Kündigung). Ähnliche Dienste bieten memoresa oder ex-medio an.
- Technische Tresore: SecureSafe (Schweiz) bietet eine hochsichere Infrastruktur für Passwörter und Dokumente. Eine integrierte Datenvererbung ermöglicht es, Informationen erst nach Ablauf einer einstellbaren Sperrfrist automatisch an Begünstigte freizugeben.

- Spezialisierte Hilfe: Digital Life Legacy (Niederlande) unterstützt beim Zugriff auf Daten Verstorbener, während Inheriti (Belgien) auf dezentrale Erbinformationen setzt.

## Ein lebenslanges Management

Der digitale Nachlass erfordert ein lebenslanges Identitätsmanagement, das über den Tod hinausgeht. Ohne klare Anweisungen drohen Hinterbliebenen komplexe Hürden und das Risiko von Identitätsdiebstahl. Daher stehen sowohl Einzelpersonen als auch Tech-Unternehmen in der Pflicht, verbindliche Standards für Privatsphäre und Zugang zu schaffen.

Frühzeitige Vorsorge ist dabei ein Akt der Fürsorge: Sie schützt das digitale Abbild vor dem Missbrauch als bloßer „Daten-Rohstoff“ und ermöglicht es, das eigene Narrativ als würdevolles Zeugnis einer Existenz aktiv zu gestalten, statt die Kontrolle Algorithmen zu überlassen.



# ANHANG

# AKTUELLER STATUS DER NIS-2-REGULIERUNG

## DIE NIS-2-RICHTLINIE

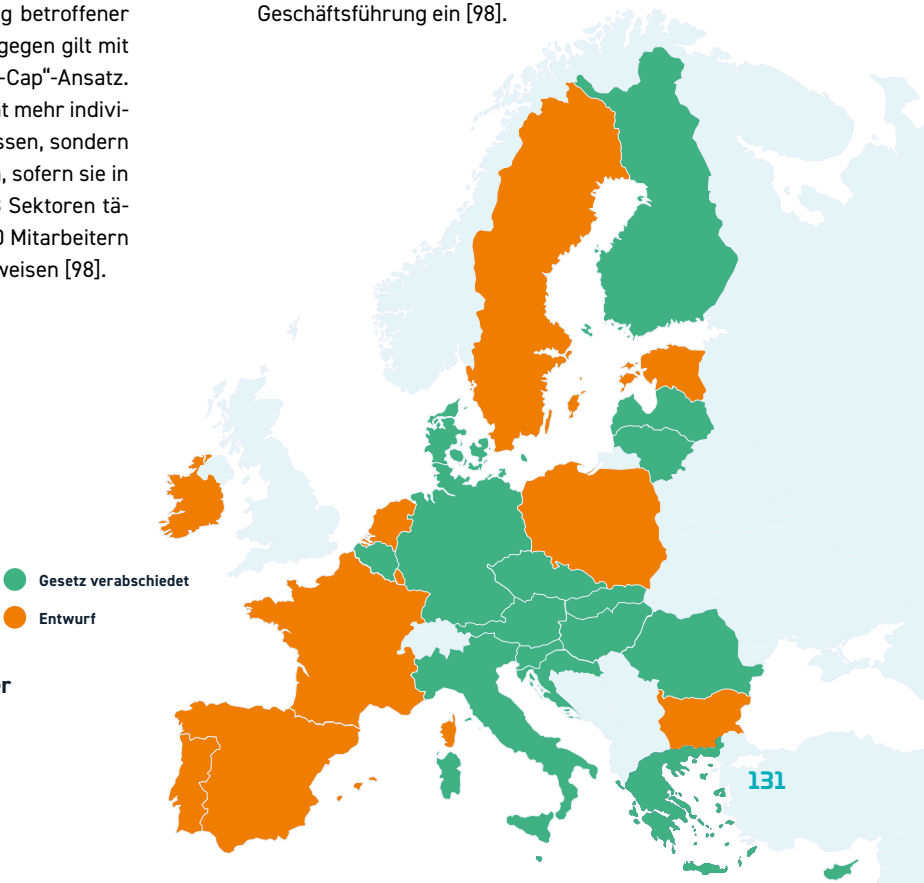
Die Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates (NIS-2) stellt die umfassende Überarbeitung der EU-Vorgaben zur Netz- und Informationssicherheit dar, um den stetig wachsenden Cyberbedrohungen für kritische Infrastrukturen zu begegnen [98], [120]. Ihre Entstehung basiert auf einer in der NIS-1-Richtlinie von 2016 verankerten Revisionsklausel. Diese verpflichtete die EU-Kommission dazu, die NIS-1-Richtlinie bis 2021 auf ihre Wirksamkeit zu prüfen [97]. Was als routinemäßiges Update geplant war, entwickelte sich aufgrund der massiven Zunahme von Ransomware-Angriffen und der durch die Pandemie beschleunigten Digitalisierung zu einer regulatorischen Generalüberholung, die im Januar 2023 offiziell in Kraft trat [120].

Im Vergleich zum Vorgänger markiert NIS-2 einen deutlichen Wandel in der Tiefe und Breite der Regulierung. NIS-1 definierte und adressierte lediglich sieben Sektoren als Kritische Infrastruktur (KRITIS) und ließ den Mitgliedstaaten bei der Identifizierung betroffener Unternehmen große Spielräume [97]. Hingegen gilt mit der neuen Richtlinie der sogenannte „Size-Cap“-Ansatz. Dieser führt dazu, dass Unternehmen nicht mehr individuell als „kritisch“ eingestuft werden müssen, sondern automatisch in den Geltungsbereich fallen, sofern sie in einem der nun EU-weiten festgelegten 18 Sektoren tätig sind und eine Größe von mindestens 50 Mitarbeitern oder 10 Millionen Euro Jahresumsatz aufweisen [98].

KRITIS sind Organisationen mit besonderer Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden [50]. Die NIS-2-Richtlinie unterscheidet zwischen zwei Hauptkategorien, was unmittelbare Auswirkungen auf die Intensität der staatlichen Aufsicht und die Höhe der Bußgelder hat. Es wird unterschieden zwischen wesentlichen und wichtigen Einrichtungen. KRITIS-Betreiber gelten im deutschen Gesetz automatisch als „Wesentliche Einrichtungen“ und unterliegen der proaktiven Aufsicht durch das BSI. Die Richtlinie legt hierbei einen EU-weiten Sanktionsrahmen fest: Bei Verstößen drohen wesentlichen Einrichtungen Bußgelder von bis zu 10 Mio. Euro oder 2 Prozent des weltweiten Umsatzes, während für wichtige Einrichtungen ein Sanktionsrahmen von bis zu 7 Mio. Euro oder 1,4 Prozent gilt [120]. Zudem definiert die Richtlinie in Artikel 21 einen verbindlichen Katalog an Risikomanagement-Maßnahmen (z. B. Backup-Konzepte, Lieferkettensicherheit) und führt eine verschärfte persönliche Haftung für die Geschäftsführung ein [98].

Quelle: [264]

**Abbildung 33: Umsetzungsstand Länder  
Anfang Februar 2026**





### Umsetzungsstand in Europa

Obwohl die offizielle Frist für die Umsetzung in nationales Recht am 17. Oktober 2024 ablief, zeigt sich ein heterogenes Bild. Bis November 2024 hatten erst vier Mitgliedstaaten die Richtlinie vollständig umgesetzt, weshalb die Europäische Kommission gegen 23 Staaten Vertragsverletzungsverfahren einleitete [117]. Mit Stand Februar 2026 haben 17 Mitgliedstaaten, darunter Deutschland, Belgien, Kroatien, Italien und die Slowakei, nationale Gesetze verabschiedet. In zehn weiteren Staaten, wie Frankreich und Estland, befinden sich die Gesetzentwürfe noch im Prozess, oft verzögert durch politische Entwicklungen [264].

### UMSETZUNG IN DEUTSCHLAND: DAS NIS-2-UMSETZUNGSGESETZ

In Deutschland wurde die NIS-2-Richtlinie durch das „Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung“ (NIS2UmsuCG) in nationales Recht überführt [159]. Als Mantelgesetz stellt es eine umfassende Modernisierung des deutschen IT-Sicherheitsrechts. NIS-2 enthält „Artikel“, die wiederum bestehende Gesetze ändern, wie das „Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen“ (BSI-Gesetz – BSI-G).

Ob ein Unternehmen nach deutscher Gesetzgebung betroffen ist, richtet sich nach drei Faktoren [159]:

- **Sektorzugehörigkeit:** Das Unternehmen ist in einem kritischen Bereich tätig (z. B. Energie, Gesundheit oder Transport).
- **Größe:** Es werden mindestens 50 Mitarbeiter beschäftigt oder ein Jahresumsatz von über 10 Mio. € erzielt.
- **Sonderfälle:** Bestimmte Anbieter fallen größenunabhängig immer in den Geltungsbereich, da ihre Dienste als systemkritisch eingestuft werden.

Die Umsetzung bringt erhebliche Herausforderungen für den Privatsektor mit sich, da Schätzungen zufolge allein in Deutschland über 41.000 Unternehmen betroffen sein werden [114].

### Kernpflichten

Unternehmen, die als „besonders wichtige“ oder „wichtige“ Einrichtungen in den Anwendungsbereich der NIS2-Richtlinie fallen, sind gesetzlich verpflichtet, sich in einem Portal des BSI (BSI-Portal)) online zu registrieren. Dabei müssen Stammdaten zum Unternehmen, Kontaktpersonen für IT-Sicherheitsvorfälle sowie die Zuordnung zu den jeweiligen Sektoren und Teilsektoren hinterlegt werden. Ziel ist es, dass das BSI im Falle von großflächigen Cyberangriffen oder kritischen Schwachstellen die betroffenen Unternehmen unmittelbar warnen und unterstützen kann [159].

Risikomanagementmaßnahmen gemäß § 30 BSI-G. Unternehmen müssen angemessene technische und organisatorische Maßnahmen ergreifen, die dem "Stand der Technik" entsprechen. Der Gesetzgeber nennt hier explizit [158]:

- Konzepte für Risikoanalyse und Informationssicherheit.
- Bewältigung von Sicherheitsvorfällen (Incident Management).
- Aufrechterhaltung des Betriebs (Business Continuity Management), z. B. durch Backups und Krisenpläne.
- Sicherheit in der Lieferkette (Überprüfung der Zulieferer).
- Schulungen und Sensibilisierungsmaßnahmen.
- Kryptografie und Verschlüsselung.
- Multi-Faktor-Authentifizierung (MFA) als Standard für den Zugriff.

Verschärfte Meldepflichten gemäß § 32 BSI-G. Bei erheblichen Sicherheitsvorfällen gilt ein strenger Zeitplan [158]:

- **24 Stunden:** Frühwarnung nach Kenntnisnahme.
- **72 Stunden:** Erste umfassende Bewertung des Vorfalls.
- **30 Tage:** Abschlussbericht mit detaillierter Ursachenanalyse.

### Rolle der Geschäftsführung und Haftungsfragen

Ein wesentliches Element des deutschen Umsetzungsgesetzes ist die direkte Verantwortung der Leitungsorgane. Geschäftsführer und Vorstände können die Cybersicherheit nicht an die IT-Abteilung delegieren. Verletzt die Geschäftsleitung ihre Pflichten schuldhaft (Vorsatz oder Fahrlässigkeit), haftet sie der Einrichtung gegenüber persönlich für den entstandenen Schaden (§ 38 Abs. 2 BSI-G).

Die Kernpflichten der Geschäftsführung sind:

- **Implementierungspflicht:** Die Geschäftsleitung muss die Risikomanagementmaßnahmen (nach § 30 BSI-G) umsetzen.
- **Überwachungspflicht:** Sie muss die Umsetzung dieser Maßnahmen kontinuierlich überwachen.
- **Fortbildungspflicht:** Jedes Mitglied der Geschäftsleitung ist gesetzlich verpflichtet, regelmäßig an Schulungen teilzunehmen (§ 38 Abs. 3 BSI-G) [158].

### Cybersecurity Act 2 (CSA 2): Fokus auf Zertifizierung und Souveränität

Seit dem Inkrafttreten der NIS-2 Richtlinie am 16. Januar 2023 hat sich die Bedrohungslage durch Ransomware, staatlich gelenkte Spionage und hybride Angriffe weiter verschärft. Während NIS-2 Unternehmen vorschreibt, dass sie sich schützen müssen, blieb oft unklar, welche technischen Produkte dafür sicher genug sind. Um diese Lücke zu schließen, legte die Europäische Kommission am 20. Januar 2026 den Entwurf für den Cybersecurity Act 2 (CSA2) vor [121]. Der ursprüngliche Cybersecurity Act von 2019 (Verordnung EU 2019/881) bildete zwar den theoretischen Rahmen für EU-weite Sicherheitszertifikate, scheiterte in der Praxis

jedoch oft an der Freiwilligkeit der Maßnahmen [287]. Besonders deutlich wurde dies beim EUCS (European Cybersecurity Certification Scheme for Cloud Services). Dieses einheitliche Sicherheitsniveau für Cloud-Dienste wurde jahrelang durch Debatten über „Souveränitätsanforderungen“ blockiert – konkret ging es um die Frage, wie europäische Daten vor dem Zugriff ausländischer Behörden geschützt werden können.

Der CSA2-Entwurf löst den jahrelangen Stillstand bei der Zertifizierung auf, indem er eine strikte Trennung zwischen technischen Sicherheitskriterien und geopolitischen Erwägungen vornimmt [121]:

- **Technik:** Das europäische Cloud-Zertifizierungsschema EUCS wird als rein technisches Zertifikat unter dem CSA2 finalisiert.
- **Geopolitik:** Für die Bewertung von Hochrisiko-Anbietern in der Lieferkette – also die Frage nach der Vertrauenswürdigkeit von Herstellern aus Drittstaaten – wird ein separates Instrument eingeführt.

### Die wichtigsten Neuerungen des CSA2

Ein zentrales Element der Reform ist der Wechsel von der Freiwilligkeit zur Pflicht. Die EU-Kommission kann nun für kritische Informations- und Kommunikationstechnik (IKT-Komponenten) verbindliche Zertifikate vorschreiben. Für Unternehmen bietet dies handfeste Vorteile und klare Konsequenzen [121]:

- **Konformitätsvermutung:** Wer zertifizierte Produkte nutzt, hat gegenüber Aufsichtsbehörden automatisch den Nachweis erbracht, dass er die strengen Risikomanagement-Anforderungen der NIS-2-Richtlinie erfüllt.
- **Harmonisierung:** Der CSA2 übernimmt zentrale Definitionen (wie etwa zu Sicherheitsvorfällen oder Netzsystemen) direkt aus der NIS-2. Dies geschieht im Sinne des REFIT-Programms (dem EU-Programm zur Gewährleistung der Effizienz und Leistungsfähigkeit der Rechtsetzung), um die Umsetzung für Unternehmen zu vereinfachen.
- **Drakonische Sanktionen:** Bei Verstößen gegen die neuen Vorgaben zur Lieferkettensicherheit erhöht der Entwurf den maximalen Bußgeldrahmen auf bis zu 7 Prozent des weltweiten Jahresumsatzes.

## Operative Schlagkraft durch ENISA

Die ENISA (die Agentur der Europäischen Union für Cybersicherheit) wird weiter zur „Schaltzentrale“ des europäischen Cyberschutzes ausgebaut. Sie unterstützt die Mitgliedstaaten operativ und übernimmt koordinierende Aufgaben [121]:

- **Aufbau von Krisenteams:** Sie unterstützt den Aufschichtsbau von CSIRTs (Computer Security Incident Response Teams), staatlichen Eingreiftruppen für IT-Sicherheitsvorfälle.
- **Zentrale Datenbanken:** Sie führt eine europäische Schwachstellen-Datenbank und stellt das Sekretariat für das Krisennetzwerk EU-CyCLONe (das europäische Verbindungsnetzwerk für Cyberkrisenorganisationen).
- **European Cyber Shield:** Flankiert wird dies durch ein Netzwerk aus KI-gestützten Sicherheitszentren, sogenannten Security Operations Centres (SOCs), die Bedrohungen EU-weit in Echtzeit erkennen sollen.

## Digital-Omnibus-Paket

Im November 2025 hat die Europäische Kommission das Digital-Omnibus-Paket (COM(2025) 837) vorgelegt, um die Überschneidungen zwischen verschiedenen EU-Gesetzen wie NIS-2, DSGVO, AI Act und DORA zu bereinigen [118].

Ein Kernstück der Reform im Bereich Cybersicherheit ist das angestrebte Prinzip „Report once, share many“: Über einen Single Entry Point (SEP) bei der ENISA sollen Unternehmen Cybervorfälle künftig zentral melden, statt verschiedene Behörden einzeln informieren zu müssen. Dies könnte geschätzt 5 Milliarden Euro an Verwaltungskosten einsparen [118]. Flankierend dazu sollen die DSGVO-Meldefristen bei Nutzung des SEP von 72 auf 96 Stunden verlängert und die Schwelle für Meldepflichten auf Fälle mit „hohem Risiko“ angehoben werden, um die Flut an Bagatellmeldungen einzudämmen [118].

Besondere Entlastung erhofft sich der Mittelstand durch die geplante Einführung der Kategorie der „Small Mid-Caps“ (SMCs) – Unternehmen mit bis zu 750 Mitarbeitern. Diese sollen unter NIS-2 künftig nur noch reaktiv statt proaktiv beaufsichtigt werden, was für rund 22.500 europäische Betriebe eine erhebliche Reduzierung der Compliance-Last bedeuten würde [118].

## HANDLUNGSBEDARF FÜR UNTERNEHMEN (STAND MÄRZ 2026)

Das Jahr 2026 markiert einen historischen Höchststand der administrativen Last. Die grundlegende Hoffnung jedoch ist, dass diese kurzfristige Belastung langfristig zu einem resilienten digitalen Binnenmarkt führt, der durch Vertrauen und Sicherheit zum globalen Wettbewerbsvorteil wird.

Es ergeben sich folgende Handlungsfelder:

1. **Registrierung prüfen:** Einrichtungen müssen sich spätestens drei Monate, nachdem sie erstmals oder erneut NIS-2-betroffen sind, im BSI-Portal registrieren.
2. **Lieferketten-Check:** Eine Inventur kritischer Hard- und Software ist essenziell. Unter dem CSA2 werden Anbieter nun separat auf geopolitische Risiken geprüft, was künftig zum Ausschluss bestimmter Hersteller führen kann.
3. **Management-Haftung:** Geschäftsführer müssen ihre gesetzliche Fortbildungspflicht jetzt dokumentieren, um persönliche Haftungsrisiken zu minimieren.
4. **Prozesse anpassen:** Interne Meldewege sollten auf die europäischen Standardformate (SEP) umgestellt werden.

# ÜBER DIE SCHWARZ GRUPPE UND SCHWARZ DIGITS

Die Schwarz Gruppe ist eine international führende Handelsgruppe mit rund 14.200 Filialen und rund 595.000 Mitarbeitern. Im Geschäftsjahr 2024 erwirtschafteten die Unternehmen der Schwarz Gruppe einen Gesamtumsatz von 175,4 Milliarden Euro. Mit ihrem einzigartigen Ökosystem decken sie den gesamten Wertschöpfungskreis ab: von der Produktion über den Handel bis hin zu Recycling und Digitalisierung. Sie schaffen Lösungen, die das Leben heute und in Zukunft nachhaltiger, gesünder und sicherer machen – sie handeln voraus.

Lidl und Kaufland bilden die Säulen im Lebensmittel-einzelhandel und sind ein fester Bestandteil im Alltag von Kunden in 32 Ländern. Viele Eigenmarkenprodukte und nachhaltige Verpackungen kommen direkt von der Schwarz Produktion. Der Umweltdienstleister PreZero fördert mit seinem Wertstoffmanagement eine funktionierende Kreislaufwirtschaft und investiert so in eine saubere Zukunft. Schwarz Digits bietet als IT- und Digitalsparte überzeugende digitale Produkte und Services an, die den hohen deutschen Datenschutzstandards entsprechen und garantiert so größtmögliche digitale Souveränität. Als partnerschaftliche Dienstleister unterstützen Schwarz Corporate Solutions die Unternehmen der Schwarz Gruppe bei allen Themen über Verwaltung, Personal bis hin zu operativen Tätigkeiten.

Schwarz Digits ist die IT- und Digitalsparte der Schwarz Gruppe. Sie bietet überzeugende digitale Produkte und Services an, die den hohen deutschen Datenschutzstandards entsprechen. Damit garantiert Schwarz Digits größtmögliche digitale Souveränität. Mit diesem Anspruch stellt Schwarz Digits die IT-Infrastruktur und Lösungen für das umfangreiche Ökosystem der Unternehmen der Schwarz Gruppe bereit und entwickelt dieses zukunftsfähig weiter. Zu den souveränen Kernleistungen von Schwarz Digits gehören Cloud, Cyber Security, Data und AI, Communication und Workspace. Schwarz Digits schafft optimale Bedingungen für die Entwicklung richtungsweisender Innovationen für Endkunden, Unternehmen und Organisationen der öffentlichen Hand.

## Folge dem Schmetterling



Unser Schmetterling symbolisiert eine große Vision: die digitale Transformation. In unserem Podcast *Tech, KI & Schmetterlinge* entschlüsseln wir, wie Technologie unsere Welt verändert.

Tauchen Sie auf schwarz-digits.de tiefer in unseren digitalen Kosmos ein:

- **Spannung:** Tech-Insights mit VIP-Gästen im Podcast.
- **Wissen:** Exklusive Whitepaper zur digitalen Souveränität.
- **Sicherheit:** Alle Cyber Security Reports & aktuelle Umfragewerte im Überblick.



# DEFINITIONEN UND ABKÜRZUNGSVERZEICHNIS

## DEFINITIONEN

|                                           |                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Advanced Persistent Threat (APT)          | Langfristig angelegte Cyberangriffe, meist durch staatliche Akteure oder deren Umfeld. Ziel ist nicht schnelle Zerstörung, sondern dauerhafter, verdeckter Zugriff auf Informationen, Systeme oder Entscheidungsprozesse.                                                                                                                 |
| Adversary-in-the-Middle (AiTM)            | Angriffsmethode, bei der Angreifer den Anmeldeprozess unbemerkt „zwischenschalten“. Dadurch können sie nicht nur Passwörter, sondern auch aktive Sitzungen übernehmen – selbst wenn Multifaktor-Authentifizierung genutzt wird.                                                                                                           |
| API-Token                                 | Digitale Schlüssel, mit denen Anwendungen automatisiert auf Systeme zugreifen. Ihre Kompromittierung ist besonders kritisch, da sie oft weitreichende Rechte besitzen.                                                                                                                                                                    |
| Business Email Compromise (BEC)           | Gezielte Betrugsform, bei der Angreifer sich als Führungskräfte, Geschäftspartner oder Dienstleister ausgeben, um Zahlungen oder sensible Informationen zu erschleichen.                                                                                                                                                                  |
| Common Vulnerabilities and Exposure (CVE) | Ein eindeutiges Identifikations- und Benennungssystem für bekannte Sicherheitslücken in Software, das von einer unabhängigen Organisation vergeben wird.                                                                                                                                                                                  |
| Credential Stuffing                       | Angriff, bei dem gestohlene Zugangsdaten automatisiert bei vielen Diensten ausprobiert werden. Funktioniert besonders gut, weil Passwörter oft mehrfach verwendet werden.                                                                                                                                                                 |
| Cyberresilienz                            | Fähigkeit einer Organisation, Cyberangriffe zu verhindern, zu bewältigen und sich schnell zu erholen – technisch, organisatorisch und strategisch.                                                                                                                                                                                        |
| DevSecOps                                 | „DevSecOps“ (Kofferwort entstanden aus Development, Security und Operations) ist ein Ansatz, der die Sicherheit (Security) von Anwendungen bereits frühzeitig im Entwicklungsprozess (Development) berücksichtigt, indem Sicherheitsmaßnahmen in die Arbeitsabläufe von Entwicklern und IT-Betriebs-Teams (Operations) integriert werden. |
| Exploit                                   | Technischer Mechanismus zur Ausnutzung einer Schwachstelle. Viele Angriffe nutzen bekannte Exploits, weil Gegenmaßnahmen nicht rechtzeitig umgesetzt werden.                                                                                                                                                                              |
| Identitäts- und Zugriffsmanagement (IAM)  | Gesamtheit der Prozesse und Systeme zur Verwaltung von Benutzerkonten, Rollen und Zugriffsrechten. Heute eine zentrale Sicherheitsdisziplin.                                                                                                                                                                                              |
| Initial Access Broker                     | Kriminelle Akteure, die kompromittierte Zugänge verkaufen. Sie sind ein zentrales Bindeglied zwischen Datendiebstahl und Ransomware.                                                                                                                                                                                                      |
| Managed Service Provider (MSP)            | Externe IT-Dienstleister, die Systeme für viele Kunden betreiben. Ihre privilegierten Zugänge machen sie zu attraktiven Angriffszielen.                                                                                                                                                                                                   |
| Multi-Faktor-Authentifizierung (MFA)      | Anmeldung mit mehr als einem Faktor (z. B. Passwort + Code), was die Sicherheit verstärkt.                                                                                                                                                                                                                                                |
| Passkey                                   | Passwortloses Anmeldeverfahren auf Basis kryptografischer Schlüssel. Reduziert Risiken durch Phishing und Passwortdiebstahl und gilt als zukünftiger Standard für privilegierte Zugänge.                                                                                                                                                  |
| Passwort-Spraying                         | Angriff, bei dem ein häufiges Passwort bei vielen Konten getestet wird.                                                                                                                                                                                                                                                                   |
| Patch-Management                          | Strukturierter Prozess des Identifizierens, Testens, Bereitstellens und Überwachens von Software-Updates (Patches) für Betriebssysteme und Anwendungen, um bekannte Schwachstellen zu schließen.                                                                                                                                          |
| Phishing                                  | Täuschungsangriff, bei dem Nutzer zur Preisgabe von Zugangsdaten verleitet werden. Durch KI zunehmend glaubwürdig und zielgerichtet.                                                                                                                                                                                                      |

|                                  |                                                                                                                                                                                                    |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Prompt Injection                 | Angriff auf KI-Sprachmodelle, bei dem durch manipulierte Eingabebefehle Sicherheitsmechanismen umgangen werden, um schadhafte Anweisungen auszuführen.                                             |
| Ransomware                       | Erpressungssoftware, die Systeme sperrt und/oder Daten stiehlt.                                                                                                                                    |
| Ransomware-as-a-Service (RaaS)   | Plattformmodell, bei dem verschiedene Akteure arbeitsteilig Ransomware-Kampagnen durchführen – ähnlich einem Franchise-System.                                                                     |
| Security Operations Center (SOC) | Organisationseinheit, die IT-Sicherheitsereignisse überwacht, bewertet und auf Vorfälle reagiert.                                                                                                  |
| Shadow-IT                        | Nicht offiziell genehmigte IT- oder Cloud-Nutzung durch Fachabteilungen. Erhöht Risiken, da Sicherheitskontrollen umgangen werden.                                                                 |
| Single Sign-on (SSO)             | Authentifizierungsverfahren, das Nutzern den Zugriff auf mehrere Anwendungen und Websites mit nur einem einzigen Satz von Anmeldedaten ermöglicht.                                                 |
| Session Hijacking                | Angriff, bei dem aktive Anmeldesitzungen übernommen werden, etwa durch das Abfangen von Zugriffstokens. Dadurch können Angreifer Sicherheitsmechanismen wie MFA umgehen.                           |
| Social Engineering               | Ausnutzung menschlicher „Schwächen“ wie Angst, Neugier oder Gehorsam, um zur Preisgabe sensibler Informationen, Umgehung von Schutzmaßnahmen oder Installation schädlicher Programme zu verleiten. |

ABKÜRZUNGSVERZEICHNIS

|           |                                                                               |        |                                                                                                 |
|-----------|-------------------------------------------------------------------------------|--------|-------------------------------------------------------------------------------------------------|
| ANN       | Artificial Neural Network                                                     | GRC    | Governance, Risikomanagement und Compliance                                                     |
| ANSSI     | Französischen Agentur für Sicherheit der Informationssysteme                  | IaaS   | Infrastructure-as-a-Service                                                                     |
| API       | Application Programming Interface (Programmierschnittstelle)                  | IAM    | Identity and Access Management                                                                  |
| APT       | Advanced Persistent Threat (staatlich gesteuerte, langfristige Cyberangriffe) | IO     | Information Operations                                                                          |
| BDSG      | Bundesdatenschutzgesetz                                                       | IoT    | Internet of Things                                                                              |
| BJA       | Bundeskriminalamt                                                             | IR     | Incident Response                                                                               |
| BMF       | Bundesministerium der Finanzen                                                | KRITIS | Kritische Infrastruktur(en)                                                                     |
| BMDs      | Bundesministerium für Digitales und Staatsmodernisierung                      | LLM    | Large Language Model, großes Sprachmodell                                                       |
| BRAK      | Bundesrechtsanwaltskammer                                                     | MFA    | Multifaktor-Authentifizierung                                                                   |
| BSI       | Bundesamt für Sicherheit in der Informationstechnik                           | MSP    | Managed Service Provider (externer IT-Dienstleister)                                            |
| C5        | BSI Cloud Computing Compliance Criteria Catalogue                             | MSS    | Managed Security Services                                                                       |
| CADA      | Cloud and AI Development Act                                                  | NIS    | Network and Information Security Directive (EU-Richtlinie zur Netz- und Informationssicherheit) |
| CATI      | Computer Assisted Telephone Interview                                         | NIST   | National Institute of Standards and Technology                                                  |
| CISA      | Cybersecurity and Infrastructure Security Agency                              | OSS    | Open Source Software                                                                            |
| CISO      | Chief Information Security Officer                                            | OT     | Operational Technology (Betriebstechnologie)                                                    |
| CISPE     | Cloud Infrastructure Service Providers in Europe                              | PaaS   | Platform-as-a-Service                                                                           |
| CLOUD Act | US Clarifying Lawful Overseas Use of Data Act                                 | RaaS   | Ransomware-as-a-Service                                                                         |
| CPU       | Central Processing Unit                                                       | SaaS   | Software-as-a-Service                                                                           |
| CRA       | Cyber Resilience Act                                                          | SBOM   | Software Bill of Materials                                                                      |
| DARPA     | Defense Advanced Research Projects Agency                                     | SEAL   | Sovereignty Effective Assurance Level                                                           |
| DDoS      | Distributed Denial-of-Service (Überlastungsangriff auf IT-Dienste)            | SOC    | Security Operations Centre                                                                      |
| DG DIGIT  | Generaldirektion Digitale Dienste der Europäischen Kommission                 | SSI    | Self-Sovereign Identity                                                                         |
| DORA      | EU Digital Operational Resilience Act                                         | STR    | Short Tandem Repeats                                                                            |
| DSB       | Datenschutzbeauftragter                                                       | TFLOPS | TeraFLOPS                                                                                       |
| DsiN      | Deutschland sicher im Netz e. V.                                              | USD    | US-Dollar                                                                                       |
| DSGVO     | Datenschutz-Grundverordnung                                                   | VPN    | Virtuelles privates Netzwerk                                                                    |
| ENISA     | European Network and Information Security Agency                              | WEF    | World Economic Forum                                                                            |
| FLOP      | False Load Output Prediction                                                  | WAF    | Web Application Firewall                                                                        |
| GAI       | Generative AI                                                                 | ZenDiS | Zentrum für Digitale Souveränität                                                               |
|           |                                                                               | ZIT    | Zentralstelle zur Bekämpfung der Internetkriminalität                                           |



# LITERATURVERZEICHNIS

[1] Acome, E. et al. (2018) Hydraulically amplified self-healing electrostatic actuators with muscle-like performance, Science, 359(6371), pp. 61-65.

[2] AliAkbarpour, H. et al. (2024) Emerging Trends and Applications of Neuromorphic Dynamic Vision Sensors: A Survey, IEEE Sensors Reviews, vol. 1, pp. 14-63.

[3] Allianz (2026) Den digitalen Nachlass regeln: Das Wichtigste in Kürze.

[4] Allianz (2026) Risk Barometer.

[5] Alto Intelligence (2026) From European Airspace to Venezuela: Pink Slime Media and Pre-Positioned Narrative Infrastructure.

[6] Ammicht, Q. et al. (2024) Ethik, Recht und Sicherheit des digitalen Weiterlebens. Forschungsergebnisse und Gestaltungsvorschläge zum Umgang mit Avataren und Chatbots von Verstorbenen.

[7] Anti-Phishing Working Group, Inc (2025) Phishing Activity Trends Report 2nd Quarter 2025.

[8] ArmyInform (2026) Record ePoints: Ukrainian drone operators eliminated over 33,000 Russians in a month.

[9] Asimov, I. (1942) Runaround, Astounding Science Fiction, March. New York: Street & Smith.

[10] ATHENE Cybernation Deutschland (2025) Sicherheit der IT der Länder.

[11] ATHENE Cybernation Deutschland (2025) Sicherheit der IT der Universitäten.

[12] Bai, Y. et al. (2025) Swarm navigation of cyborg-insects in unknown obstructed soft terrain, Nat Commun 16, 221.

[13] Baker, S. (2025) Ukrainian robotics company says autonomy in defense is overhyped – but it’s also past the point of no return, Business Insider.

[14] Barlow, J. P. (1996) Declaration of Independence for Cyberspace.

[15] Bartelson, J. (1995) A genealogy of sovereignty (Vol. 39) Cambridge University Press.

[16] Baums, A. & Kilian, M. (2025) Better Stack (Part 1): 10 Theses to Demystify the Debate on Digital Sovereignty and the Euro Stack. GovTech Intelligence Hub.

[17] BBC (2020) Kanye West gives Kim Kardashian birthday hologram of dead father.

[18] BCG (2025) Europe’s Race to Tech Readiness.

[19] Belli, L. & Jiang, M. (2024) Digital Sovereignty in the BRICS Countries: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance. Cambridge University Press.

[20] Bergtora Sandvik, K. (2020) Digital Dead Body Management: Time to Think it Through. Journal of Human Rights Practice, 12(2020), 428-443.

[21] BfV (2026) Cyberangriffe. Gefahren, Risiken und Schutz vor staatlich gesteuerten Attacken.

[22] Biersdorfer, J. D. (2025) How to Prepare for Your Digital Afterlife.

[23] Bitkom (2025) Cyberkriminalität – Bevölkerungsumfrage zu Wahrnehmung, Erfahrungen und Schutzverhalten.

[24] Bitkom (2025) Digitales Erbe: Was passiert mit Online-Zugängen nach dem Tod?

[25] Bitkom (2025) Europas Weg in die digitale Souveränität.

[26] Bitkom (2026) Digitalwirtschaft bleibt Stabilitätsanker: 245 Milliarden Euro Umsatz in 2026.

[27] Bitkom (2025) Wirtschaftsschutz 2025.

[28] Bitkom (2025) Wirtschaft setzt verstärkt auf Cloud – Forderungen nach europäischen Anbietern nehmen zu.

[29] Bitdefender (2024) 2024 Consumer Cybersecurity Assessment Report.

[30] BKA (2025) Bundeslagebild Cybercrime 2024.

[31] BKA (2025) Darknet-Handelsplattform „Archetyp Market“ abgeschaltet.

[32] BKA (2025) Endgame 2.0: Weitere 20 Haftbefehle in der bislang weltweit größten Cyber-Polizeioperation.

[33] BKA (2025) International abgestimmtes Vorgehen gegen die hacktivistische Gruppierung „NoName057(16)“.

[34] BKA (2025) Strafverfolgungsbehörden schalten die zwei weltweit größten Cybercrime-Foren mit rund zehn Millionen registrierten Nutzern ab.

[35] Blair-Frasier (2025) The 2025 Security Benchmark Report.

[36] BMDS (2025) Deutschland-Stack.

[37] BMDS (2025) Gipfel zur Europäischen Digitalen Souveränität.

[38] BMDS (2026) Bund startet Sandbox für EUDI-Wallet.

[39] BMF (2024) Entwurf zum Bundeshaushaltsplan 2024 Einzelplan 14.

[40] BNP Media (2025) The Security Benchmark Report.

[41] Bologna, C. (2025) This Sneaky Spending Habit Might Cost You More Money Than You Think.

[42] BRAK (2025) Digitale Nachlassermittlung: BRAK fordert strengere Datenschutzregeln.

[43] Brave1 (2026) Defense Tech Cluster Market.

[44] Brewster, T. (2026) Microsoft Gave FBI Keys To Unlock Encrypted Data, Exposing Major Privacy Flaw, Forbes.

[45] Bria, F., Timmers, P., & Gernone, F. (2025) EuroStack – A European alternative for digital sovereignty. EuroStack.

[46] BSI (2019) BSI – Kriterienkatalog C5.

[47] BSI (2025) Befragung zur Cybersicherheit.

[48] BSI (2025) Die Lage der IT-Sicherheit in Deutschland 2025.

[49] BSI (2025) Entscheidungsbaum der NIS-2-Betroffenheitsprüfung des BSI.

[50] BSI (2025) Kritische Infrastrukturen (KRITIS).

[51] BSI (2025) KRITIS in Zahlen.

[52] Buchholz, L. (2025) Digitale Souveränität in Deutschland: Eine Analyse der Cloud-Angebote von Superscalern und Hyperscalern für Behörden, focus on IT.

[53] Calderaro, A. & Blumfelde, S. (2022) Artificial intelligence and EU security: the false promise of digital sovereignty. European Security.

[54] Cao, L. (2024) Humanoid Robots and Humanoid AI: Review, Perspectives and Directions, arXiv preprint arXiv:2405.15775.

[55] CDU, CSU und SPD (2025) Verantwortung für Deutschland. Koalitionsvertrag zwischen CDU, CSU und SPD.

[56] Chander, A. & Sun, H. (Eds.) (2023) Data sovereignty: From the digital silk road to the return of the state. Oxford University Press.

[57] Chang, E. et al. (2024) Bird-inspired reflexive morphing enables rudderless flight, Sci. Robot.9, eado4535(2024).

[58] Check Point (2025) 40,000 phishing emails disguised as SharePoint and e-signing services: A new wave of finance-themed scams.

[59] Check Point (2025) AI 2030: The coming era of autonomous cyber crime.

[60] Check Point (2025) Check Point Blog.

[61] Check Point (2025) Global cyber attacks increase in November 2025 driven by ransomware surge and GenAI risks.

[62] Check Point (2025) Global cyber threats September 2025: Attack volumes ease slightly but GenAI risks intensify as ransomware surges.

[63] Check Point (2025) Latin America 2025 Mid-Year Cyber Snapshot Reveals 39% Surge in Attacks as AI Threats Escalate Regional Risk.

[64] Check Point (2025) Microsoft dominates phishing impersonations in Q3 2025.

[65] Check Point (2025) Phishing campaign leverages trusted Google Cloud automation capabilities to evade detection.

[66] Check Point (2025) The rise of AI-powered threats and other mobile risks highlight why it's time to rethink your security architecture.

[67] Check Point (2025) The State of Cyber Security 2025.

[68] Check Point (2025) The state of ransomware in Q3 2025.

[69] CISA (2025) CISA, NSA and Cyber Centre Warn Critical Infrastructure of BRICKSTORM Malware Used by People's Republic of China State-Sponsored Actors.

[70] CISA (2025) CISA Unveils Guide to Combat Bulletproof Hosting Cybercrime.

[71] CISA (2025) Forging National Resilience for an Era of Disruption.

[72] CISA (2025) FY2025-2026 CISA International Strategic Plan.

[73] CISA (2025) Key Cyber Initiatives from CISA: KEV Catalog, CPGs, and PRNI.

[74] CISA (2025) News.

[75] CISA (2025) United in Cyber Defense: A Model for Operational Collaboration.

[76] CISPE (2025) CISPE Cloud Catalogue.

[77] CISPE (2025) No Such Thing as "75% Sovereign".

[78] CNIL (2025) Our Data After Us. From Digital Death to Immortality, Uses and Issues of Post Mortem Data. IP Report N°10, Innovation & Foresight Division.

[79] Couture, S. & Toupin, S. (2019) What does the notion of "sovereignty" mean when referring to the digital? New media & society, 21(10).

[80] Corralero Medina, L. (2025) The Digital Afterlife: Ethical implications of memorial accounts on socio-technological platforms.

[81] CSO Online (2025) Cyberangriff auf Arla Deutschland.

[82] CSO Online (2025) Diese Unternehmen hat es schon erwischt.

[83] CSO Online (2025) Vodafone von Hackerangriff auf Dienstleister betroffen.

[84] Cyber Monitoring Centre (2025) Cyber Monitoring Centre Statement on the Jaguar Land Rover Cyber Incident – October 2025.

[85] CyberProof (2025) 2025 Global Threat Intelligence Report 2025 – Mapping Threats and Trends.

[86] CyberProof (2025) Mid-Year Cyber Threat Landscape Report – H1 2025 Analysis August 2025.

[87] Cyfirma (2026) Tracking Ransomware Dec 2025.

[88] Czieśla, F. (2022) Von der Biopolitik zur Nekro-Ökonomie. Für eine genealogische Kritik der politischen Ökonomie des Todes. Bielefeld: transcript.

[89] Dachwitz, I. & Meineck, S. (2025) New data set reveals 40,000 behind location tracking.

[90] Daily News Egypt (2025) Egypt's ICT minister stresses need for Arab cooperation on cyber threats.

[91] Danby, P. (2022) Human brain cells in a dish learn to play Pong, UCL News.

[92] DARPA (2025) DARPA program sets distance record for power beaming.

[93] Del Valle, I. (2025) AI After Death: Digital Identity, Neural Echoes, and Post-Mortem Decision Rights.

[94] Deutsche Verwaltungswolke (2025) Reifegradmodell.

[95] Digital SME Alliance (2025) New Tech Sovereignty Catalogue Announced to Map Europe's Digital Potential.

[96] Diletta, D. M. et al. (2025) Open but Not Powerless: Towards a Common Understanding of EU Digital Sovereignty, EU Joint Research Center, European Commission.

[97] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

[98] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

[99] Doaré, R. et al. (2014) Robotson the Battlefield: Contemporary Issues and Implications for the Future. Fort Leavenworth, KS: Combat Studies Institute Press.

[100] Dormmann, L. et al. (2021) Kompendium: Li-Ionen-Batterien, VDE.

[101] Draghi Bericht (2024) Die Zukunft der europäischen Wettbewerbsfähigkeit, Teil A.

[102] Dressler, N. (2026) Neues BSI-Protal startet: Vorstände haften persönlich für IT-Sicherheit.

[103] DsiN (2025) Deutschland im Fokus von Cyberangriffen: Höchste Angriffszahlen in der EU.

[104] DsiN (2025) DsiN Sicherheitsindex 2025.

[105] DsiN (2025) Pressemitteilungen.

[106] Du, J. et al. (2024) Global Automation Humanoid Robot: The AI accelerant. Goldman Sachs.

[107] Eiben, A. & Smith, J. (2015) From evolutionary computation to the evolution of things, *Nature* 521, 476–482.

[108] Elias, J. (2026) Exaggeration per record.

[109] EngineAI Official Website (2025).

[110] ENISA (2025) ENISA Threat Landscape 2025.

[111] ENISA (2025) NIS Investments 2025.

[112] Etienne-Cummings, R. & Van der Spiegel, J. (1996) Neuromorphic vision sensors, *Sensors and Actuators A: Physical*, 56(1-2), pp. 19-29.

[113] European Commission (o. J.) Verifiable Credentials Framework.

[114] European Commission (2020) Commission Staff Working Document.

[115] Europäische Kommission (2025) Cyberresilienzgesetz.

[116] Europäische Kommission (2025) International Criminal Court switches to open source with openDesk.

[117] Europäische Kommission (2025) Vertragsverletzungsverfahren: Kommission leitet in vier Fällen rechtliche Schritte gegen Deutschland ein.

[118] Europäische Kommission (2026) Ein agiles digitales Regelwerk für die EU.

[119] Europäische Kommission (2026) Europäische digitale Identität.

[120] Europäische Kommission (2026) NIS2-Richtlinie: Sicherung von Netz- und Informationssystemen.

[121] Europäische Kommission (2026) Vorschlag für eine Verordnung zum EU-Rechtsakt zur Cybersicherheit.

[122] Europäische Kommission DG DIGIT (2025) Cloud Sovereignty Framework. Europäische Kommission. Seiten 1-6. Brüssel, Belgien.

[123] Europäischer Rat, Rat der Europäischen Union (2026) Cybersicherheit in der EU: Strategie und wichtigste Maßnahmen.

[124] European Law Institute (2025) ELI Guiding Principles and Model Rules on Digital Assistants for Consumer Contracts.

[125] European Parliament (2024) Public Procurement Act. In "A new plan for Europe's sustainable prosperity and competitiveness", Legislative Train Schedule.

[126] European Parliamentary Research Service (2025) Cloud and AI Development Act.

[127] Europol (2025) Europol and partners shut down "Cryptomixer".

[128] Europol (2025) Global operation targets NoName057(16) pro-Russian cybercrime network.

[129] Europol (2025) Internet Organised Crime Threat Assessment, IOCTA 2025.

[130] Europol (2025) Key figure behind major Russian-speaking cybercrime forum targeted in Ukraine.

[131] Europol (2025) Key figures behind Phobos and 8Base ransomware arrested in international cybercrime crackdown.

[132] Europol (2025) Newsroom.

[133] EuroStack Industry Alliance (2025) Regulation of Strategic Digital Procurement.

[134] EY (2025) Datenklastudie 2025. Virtuelle Gefahr – realer Schaden.

[135] Federal Trade Commission (2025) Data Book 2024.

[136] Figure AI (2025) F.02 Contributed to the Production of 30,000 Cars at BMW.

[137] FinalSpark (2024) Biocomputing.

[138] Flashpoint (2025) Flashpoint 2025 Global Threat Intelligence Report.

[139] Flashpoint (2025) Flashpoint's Global Threat Intelligence Index: 2025 Midyear Edition.

[140] Floridi, L. (2016) On human dignity as a foundation for the right to privacy. *Philos Technol* 29:307–312.

[141] Floridi, L. (2020) The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. *Philosophy & Technology*.

[142] Förster, M. (2025) Microsofts Souveränitäts-Debakel: Zwischen „blumiger Werbung“ und „keine Panik“. heise.

[143] Förster, M. (2025) Scharfe Kritik am EU-Rahmenwerk für Cloud-Souveränität.

[144] Forbes (2025) Billions Of Passwords Have Leaked — Hack Attacks Are Ongoing, Act Now.

[145] Fortinet (2025) Bericht zum Stand der Betriebstechnologie (OT) und Cybersecurity 2025.

[146] Fortinet (2025) CISO Predictions 2026.

[147] Fortinet (2025) Data Security Report 2025.

[148] Fortinet (2025) Global Threat Landscape Report 2025.

[149] Fortinet (2025) Insider Risk Report 2025.

[150] Fox, P., Schnitzer, M. & Privitera, D. (2025) KI-Rechenzentren in Deutschland. Aktuelle Kapazität, künftiger Bedarf. KIRA Center.

[151] Francis, J. (2025) The Hidden Dangers of Forgotten Accounts.

[152] Fraunhofer (2025) Berührungsloses Patientenmonitoring: EKG per Radar. Press Release, May 2025.

[153] Fraunhofer IPA (2019) If Machines Could Smell ...

[154] Fraunhofer ISS (2026) Neuromorphes Computing.

[155] Friedman, C. R. et al. (2025) Leveraging a Strategic Public-Private Partnership to Launch an Airport-Based Pathogen Monitoring Program to Detect Emerging Health Threats, *Emerg Infect Dis.* 2025 May; 31(13):35-38.

[156] Gao Y. et al. (2025) A neuromorphic robotic electronic skin with active pain and injury perception, *Proc. Natl. Acad. Sci. U.S.A.* 122 (52) e2520922122.

[157] G DATA Cyberdefense (2025) Cybersicherheit in Zahlen.

[158] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen (BSI-Gesetz – BSIg).

[159] Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung.

[160] Gineikyte-Kanclere, V., Eggert, M. & Skiotyte, G. (2025) European Software and Cyber Dependencies, Study Requested by the ITRE Committee, European Parliament.

[161] Glasze, G. et al (2023) Contested spatialities of digital sovereignty, *Geopolitics*.

[162] Google Threat Intelligence Group (2025): APT24's Pivot to Multi-Vector Attacks.

[163] Google Threat Intelligence Group (2025) GTIG AI Threat Tracker: Advances in Threat Actor Usage of AI Tools.

[164] Gravert, S. D. et al. (2024) Low-voltage electrohydraulic actuators for untethered robotics, *Sci Adv.* 2024 Jan 5;10(1):ead9319.

[165] Group-IB (2025) Trends in der High-Tech Kriminalität 2025.

[166] Hamerly, R. et al. (2019) Large-Scale Optical Neural Networks Based on Photoelectric Multiplication, *Physical Review X*, 9(2), 021032.

[167] Hanamsagar, A. et al. (2018) Leveraging Semantic Transformation to Investigate Password Habits and Their Causes.

[168] Hardman, D. et al. (2025) Multimodal information structuring with single-layer soft skins and high-density electrical impedance tomography, *Sci. Robot.* 10,eadq2303.

[169] Hawkins, Z. H., Lehdonvirta, V., & Wu, B. (2025) AI Compute Sovereignty: Infrastructure Control Across Territories, Cloud Providers, and Accelerators. *Cloud Providers, and Accelerators*.

[170] Heise Online (2025) Schleswig-Holstein: Fast 80 Prozent der Microsoft-Lizenzen gekündigt.

[171] Hoang, V. D. et al. (2024) Autonomous Overhead Powerline Recharging for Uninterrupted Drone Operations, 2024 IEEE International Conference on Robotics and Automation (ICRA).

[172] Hölzl, V. (2025) USA verhängen Sanktionen gegen IStGH-Chefankläger Khan. ZEIT.

[173] Hollanek, T., & Nowaczyk-Basińska, K. (2024) Griefbots, Deadbots, Postmortem Avatars: On Responsible Applications of Generative AI in the Digital Afterlife Industry. *Philosophy & Technology*, 37(63).

[174] Hornetsecurity (2025) Cybersecurity Report 2025.

[175] Hornetsecurity (2025) Monthly Threat Reports 2025.

[176] Hornetsecurity (2025) Monthly Threat Report Mai 2025.

[177] Hornetsecurity (2025) Monthly Threat Report Juni 2025.

[178] Hornetsecurity (2025) Monthly Threat Report Juli 2025.

[179] Horneysecurity (2025) Monthly Threat Report Oktober 2025.

[180] Hornetsecurity (2025) Monthly Threat Report November 2025.

[181] Hornetsecurity (2025) Monthly Threat Report Dezember 2025.

[182] Howard, D. et al. (2019) Evolving embodied intelligence from materials to machines, *Nat Mach Intell* 1, 12–19.



[183] Hsu, J. (2015) Robot Funerals Reflect Our Humanity.

[184] IANS (2026) The CISO Pay Gap: Inside Cybersecurity's massive compensation divide.

[185] IBM Security (2025) Cost of a Data Breach 2025.

[186] ICSSD (2020) 4th International Conference on Science and Sustainable Development: Industry and Robotics. Conference Proceedings.

[187] Informatik.ch (2025) Gehirn auf dem Chip: Wie 800.000 Neuronen einen Computer antreiben.

[188] Inside the Rise of AI-Powered Pharmaceutical Scams.

[189] Intel 471 (2025) Cybercrime takedowns: trust, partnerships and focus.

[190] Intel 471 (2025) DanaBot malware disrupted, threat actors named.

[191] Intel 471 (2025) How initial access offers power intrusions and ransomware.

[192] Intel 471 (2025) Intel 471 Blog.

[193] Intel 471 (2025) Law enforcement hammered cybercrime in 2024. Is it working?

[194] Intel 471 (2025) "Pig-Butchering" Scams: The Dark Side of Social Engineering and Why Terminology Matters.

[195] Intel 471 (2025) UK 2025 Threat Landscape: "Rampant Cyber Crime".

[196] International Federation of Robotics (2025) Absatz von Industrierobotern nach ausgewählten Ländern weltweit in den Jahren 2023 und 2024. Statista.

[197] International Federation of Robotics (2024) Manufacturing industry-related robot density in selected regions worldwide in 2022 (in units per 10,000 employees). Statista.

[198] Interpol (2025) African authorities dismantle massive cybercrime and fraud networks, recover millions.

[199] ISACA (2025) State of Cybersecurity 2025 report.

[200] ISC2 Research (2025) 2025 ISC2 Cybersecurity Workforce Study.

[201] it-daily (2025) Analyse aktueller Cyberangriffe im Nahen Osten.

[202] Jerusalem Post (2025) China unveils "robotic wolves" leading frontline in amphibious assault exercise.

[203] Jerusalem Post (2025) "First robotics war": Defense Ministry shows how robotic systems used in Israel-Hamas War.

[204] Joint Cybersecurity Advisory (2025) Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System.

[205] Jordan, J. M. (2019) The Czech Play That Gave Us the Word Robot.

[206] Juhász, Á. (2024) Inheriting Digital Assets – A Glimpse Into the Future, Juridical Tribune – Review of Comparative and International Law 14, no. 4: 547-563.

[207] Kaloudis, M. (2021) Sovereignty in the Digital Age – How Can We Measure Digital Sovereignty and Support the EU's Action Plan? New Global Studies, 16(3).

[208] Kashchenko, M. (2025) Robot rescues Ukrainian soldier trapped 33 days behind Russian lines, navigating minefields and mortar strikes, CNBC News.

[209] Kaspersky (2024) Digital Afterlife: 61% Worry About Online Legacy of the Deceased. Press Release, Aug 21, 2024.

[210] Königssohn, K.-K. (2025) White House protection included, Mimer.

[211] Kompetenzzentrum Öffentliche IT (2017) Digitaler Nachlass.

[212] KPMG (2025) Passkeys: Sicherheit ohne Passwort.

[213] Kreml. S. (2025) Gutachten: US-Behörden haben weitreichenden Zugriff auf europäische Cloud-Daten. heise.

[214] Kubis, M. et al. (2019) Der digitale Nachlass. Eine Untersuchung aus rechtlicher und technischer Sicht.

[215] Kumar, A. et al. (2021) RMA: Rapid Motor Adaptation for Legged Robots, Preprint 2107.04034.

[216] Kunz, E. M. et al. (2025) Inner speech in motor cortex and implications for speech neuroprostheses, Cell, 188(17).

[217] Lambach, D. & Oppermann, K. (2023) Narratives of digital sovereignty in German political discourse. Governance.

[218] Larsson, O. (2025) DNA as a power tool in hybrid warfare, Swedish Defence University.

[219] LastPass (2022) Psychology of Passwords.

[220] Lee, B. et al. (2023) A principal odor map unifies diverse tasks in olfactory perception, Science381, 999-1006(2023).

[221] Li, C. et al. (2025) An overview of machine unlearning High-confidence computing.

[222] Lin, Q. et al. (2025) Cyborg insect factory: automatic assembly for insect-computer hybrid robot via vision-guided robotic arm manipulation of custom bipolar electrodes, Nat Commun 16, 6073 (2025).

[223] Li, S. et al. (2025) Advanced Brain-on-a-Chip for Wetware Computing: A Review, Advanced Science, 12, e08120.

[224] Li, Y. et al. (2025) MCOD: The First Challenging Benchmark for Multispectral Camouflaged Object Detection, Proceedings of the 33rd ACM International Conference on Multimedia (MM '25).

[225] Li, Z. et al. (2025) Humanoid Locomotion and Manipulation: Current Progress and Challenges in Control, Planning, and Learning, arXiv preprint arXiv:2501.02116.

[226] Lundblad, N. (2025) Digital Sovereignty: Can Europe afford it. CEPA.

[227] Mackay, N. (2025) Germany's defense procurement crisis: it's time for strategic overhaul, CCM Institute Insights.

[228] Mahmoud, O. A. et al. (2025) Advancements and Applications of STR Kits in Forensic DNA Profiling: A Comprehensive Review, Baghdad Journal of Biochemistry and Applied Biological Sciences. 6. 1-17.

[229] Mak, C. (2023) Data After Life: The Protection of Users' Development of their Digital Identity, VerfBlog, 2023/5/24.

[230] Mandiant (2025) Adversarial Misuse of Generative AI.

[231] Mandiant (2025) BitM Up! Session Stealing in Seconds Using the Browser-in-the-Middle Technique.

[232] Mandiant (2025) Deception in Depth: PRC-Nexus Espionage Campaign Hijacks Web Traffic to Target Diplomats.

[233] Mandiant (2025) M-Trends 2025 Report.

[234] Mandiant (2025) Phishing Campaigns Targeting Higher Education Institutions.

[235] Mandiant (2025) Preparing for Threats to Come: Cybersecurity Forecast 2026.

[236] Mandiant (2025) Threat Intelligence.

[237] Mandiant (2025) What's in an ASP? Creative Phishing Attack on Prominent Academics and Critics of Russia.

[238] Marco Polo The Global AI Talent Tracker (2023).

[239] Marsh (2025) Cyber catalyst report: Guiding priorities in cyber investments.

[240] Max, K. et al. (2025) Synthetic biology meets neuromorphic computing: towards a bio-inspired olfactory perception system, Neuromorphic Computing and Engineering 5 034010.

[241] Max-Planck-Gesellschaft Synthetische Biologie und Sicherheit (2026)

[242] McNulty, D. et al. (2022) A review of Li-ion batteries for autonomous mobile robots: Perspectives and outlook for the future, Journal of Power Sources, Volume 545, 2022, 231943.

[243] Mehar, V. et al. (2025) Receiver-Side Power Control of a 200-kW Three-Phase DWPT System for Heavy-Duty Vehicles, 2025 IEEE Transportation Electrification Conference & Expo (ITEC).

[244] Merkel, A., Frederiksen, M., Marin, S. & Kallas, K. (2021) Letter to European Commission President Ursula von der Leyen.

[245] Meyer, H. (2023) Digital legacy: how to organise your online life for after you die.

[246] Microsoft (2025) Microsoft Digital Defense Report 2025.

[247] Ministerium für Kultus, Jugend und Sport Baden-Württemberg (2025) Digitaler Arbeitsplatz für Lehrkräfte wird nun mit openDesk umgesetzt.

[248] Nagy, P., & Neff, G. (2015) Imagined Affordance: Reconstructing a Keyword for Theory. Sage Journals, 1(2).

[249] Nair, V. (2025) How many Bitcoin are lost?

[250] Nansen, B. et al. (2017) Social Media in the Funeral Industry: On the Digitization of Grief, Journal of Broadcasting & Electronic Media, 61(1), pp. 73–89.

[251] Nansen, B. et al. (2019) "Death by Twitter": Understanding false death announcements on social media and the performance of platform cultural capital. First Monday, 24(12).

[252] Nansen, B. (2025) Most of us will leave behind a large digital legacy when we die.

[253] NASA (2024) OTPS SBSP Report Final.

[254] National Security Bureau. R.O.C. (2025) Analysis on China's Cyber Threats to Taiwan's Critical Infrastructure in 2025.

[255] Nextcloud (2025) Digital Sovereignty Index.

[256] Nextcloud (2025) Nextcloud enables secure, sovereign collaboration for Austria's Federal Ministry.

[257] Next:public (2025) Souveränitätsbarometer der öffentlichen IT.

[258] NIST (2025) National Vulnerability Database.

[259] NOKIA (2025) Threat Intelligence Report 2025.

[260] NordPass (2024) People have around 170 passwords on average, study shows.

[261] Öhman, C. (2024) The Afterlife of Data. What happens to your information when you die and why you should care. The University of Chicago Press, Chicago and London.

[262] Öhman, C. & Floridi, L. (2017) The Political Economy of Death in the Age of Information: A Critical Approach to the Digital Afterlife Industry. *Minds & Machines* 27, 639–662.

[263] Öhman, C., & Watson, D. (2021) Are the Dead Taking Over Instagram? A Follow-up to Öhman & Watson (2019). In: Cows, J., Morley, J. (eds) *The 2020 Yearbook of the Digital Ethics Lab*. Digital Ethics Lab Yearbook. Springer, Cham.

[264] OpenKRITIS (2026) NIS2 in EU Countries.

[265] Open Web Application Security Project (OWASP) (2025) OWASP Attack Surface Management Top 10.

[266] Paleja, A. (2021) US Military's Active Denial System is a 95 GHz Heat Ray, Interesting Engineering.

[267] Palo Alto Networks (2025) Bedrohungsbeschreibung: Eskalation des Cyberrisikos im Zusammenhang mit dem Iran.

[268] Pandey, M., et al. (2025) Advanced Materials for Biological Field-Effect Transistors (Bio-FETs) in Precision Healthcare and Biosensing, *Advanced Healthcare Materials*, 14(13), 2500400.

[269] Pape, A. (2023) Ethische Herausforderungen digitaler Nachlässe. Hannover: Hochschule Hannover.

[270] Pasquale, F. (2019) From Territorial to Functional Sovereignty: The Case of Amazon, LPE.

[271] Paulus, A. (2025) Europas Cybersicherheit hängt an den USA, SWP-Aktuell 2025/A 48.

[272] Pelrine, R. et al. (2000) High-Speed Electrically Actuated Elastomers with Strain Greater Than 100%, *Science*, 287(5454), pp. 836-839.

[273] PEO Soldier (2019) XM157 Next Generation Squad Weapons – Fire Control, Program Executive Office Soldier.

[274] PHF Science NZ (2025) Testing plane sewage at border can help detect disease.

[275] Pilch, R. et al. (2021) Scientific Risk Assessment of Genetic Weapon Systems, *CNS Occassional Paper #52* (2021).

[276] Plattner, C. & Seiller, F. (2025) Schneller zur digitalen Souveränität. Atlantik Brücke.

[277] Plattner, C. & Strubel, V. (2025) Joint Statement by ANSSI and BSI on Cloud Sovereignty Criteria.

[278] P. M. Wensing et al. (2017) Proprioceptive Actuator Design in the MIT Cheetah: Impact Mitigation and High-Bandwidth Physical Interaction for Dynamic Legged Robots, *IEEE Transactions on Robotics*, vol. 33, no. 3.

[279] Pohle, J. (2020) Digitale Souveränität Ein neues digitalpolitisches Schlüsselkonzept in Deutschland und Europa, Konrad Adenauer Stiftung.

[280] Pohle, J. & Thiel, T. (2020) Digital Sovereignty. *Internet Policy Review*.

[281] Prophesee.ai (2026).

[282] Ptock, J. (2020) Cybercrime: Zahlen und Statistiken für Deutschland.

[283] PwC US Group LLP (2025) 2026 Global Digital Trust Insights: C-suite playbook and findings – New world, new rules: Cybersecurity in an era of uncertainty.

[284] Qiang L. et al. (2020) A Review of Tactile Information: Perception and Action Through Touch, *Trans. Rob.* 36, 6 (Dec. 2020), 1619–1634.

[285] Qu, S. et al. (2025) Skynet Starter Kit: From Embodied AI Jailbreak to Remote Takeover of Humanoid Robots, 39C3.

[286] Rahman, M. M. et al. (2024) A comprehensive review of wireless power transfer methods, applications, and challenges, *Engineering Reports*, 6(10), e12951.

[287] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

[288] Roosevelt, R. & Hodder, C. (2025) The Ultimate Guide to Planning Your Digital Estate.

[289] Rothemund, P. et al. (2020) Miniaturized Circuitry for Capacitive Self-Sensing and Closed-Loop Control of Soft Electrostatic Transducers, *Soft Robotics*.

[290] Rouco, A. et al. (2025) Biometric Identification via Through-Wall Radar: A Survey on Vital Signs and Gait Analysis, *IEEE Access* 25(13).

[291] RPTU (2025) Dänemark: Bye-bye Microsoft?

[292] Rus, D. & Tolley, M. (2015) Design, fabrication and control of soft robots, *Nature*. 521. 467-75.

[293] Salary.com (2025) SVP of Information Security Salary in the United States.

[294] SAP (2024) Aktionärsstruktur & Basisdaten, SAP Investor Relations.

[295] ScamWatchHQ (2025) Egypt Scams 2025: The Nile's Digital Deception – When Currency Crisis, Youth Unemployment, and Religious Trust Create a Perfect Storm for Fraud.

[296] Scharre, P. (2018) *Army of None: Autonomous Weapons and the Future of War*, New York: W. W. Norton & Company.

[297] Schneider, M. (2025) Mistral starts processing personal data in USA and stops notifying of such changes. Open Terms Archive.

[298] Schoder, S. (2025) Physics-Informed Neural Networks for Modal Wave Field Predictions in 3D Room Acoustic, *Applied Sciences*, 15(2), 939.

[299] Schwarz Digits (2025) Cyber Security Report.

[300] Schwarz Digits (2025) Warum die Digitalisierung ein Umdenken in einer neu geordneten Welt erfordert.

[301] ScienceDirect (2024) Cognitive Architecture.

[302] Shao, S. et al. (2022) High Efficiency Wireless Power Transmission System That Uses HTS Transmitting and Copper Receiving Coils, *IEEE Transactions on Applied Superconductivity*, 32(4).

[303] Shaughnessey, I. M. (2024) The Ethics of Robots in War, *NCO Journal*, February 2024.

[304] Shaw, A. (2017) Encoding and decoding affordances: Stuart Hall and interactive media technologies. *Sage Journals*, 39(4), 592-602.

[305] Sherazi, H. H. R., Zorbas, D., & O'Flynn, B. (2022). A Comprehensive Survey on RF Energy Harvesting: Applications and Performance Determinants. *Sensors*, 22(8), 2990.

[306] Singh, S. et al. (2024) Powering the future: A survey of ambient RF-based communication systems for next-gen wireless networks, *IET Wireless Sensor Systems*, 14(6), 265-292.

[307] Smith, J. (2025) Meeting Abstracts, *Journal of The Electrochemical Society*, MA2025-02.

[308] SOCRadar (2022) "Fullz," "Dumps," and More: What do Hackers Sell on the Black Market?

[309] Soleimani, J. & Kurt, G. K. (2024) High-power radio frequency wireless energy transfer system: Comprehensive survey on design challenges, *IET Wireless Sensor Systems*, 14(6), 248-264.

[310] Sommer, D. & Lorenz, B. (2022) Der digitale Nachlass – Was passiert mit meinen Daten nach meinem Tod?

[311] Sophos (2025) The Human Cost of Vigilance: Addressing Cybersecurity Burnout in 2025.

[312] Sophos (2025) The Sophos Annual Threat Report: Cybercrime on Main Street 2025.

[313] Sophos (2025) The State of Ransomware 2025.

[314] StackIT (2025) Deutschlands Digitaler Aufbruch.

[315] Statista (2025) Estimated cost of cybercrime worldwide 2018-2029.

[316] Statista (2025) Ranking der größten Social Networks und Messenger nach der Anzahl der Nutzer im Februar 2025.

[317] Statista Market Insights (2025) Brand Shares (BETA), basierend auf Finanzberichterstattung der Key Player.

[318] Statista Market Insights (2025) Public Cloud – Durchschnittliche Ausgaben je Arbeitnehmer.

[319] Statista Market Insights (2025) Public Cloud – Umsatz.

[320] Statistisches Bundesamt (2025) Informations- und Kommunikationstechnologien privater Haushalte.

[321] Swiss Cyber Security (2025) Adidas meldet Datenleck nach Angriff auf Dienstleister.

[322] Taglione, C., et al. (2024) Polarimetric Imaging for Robot Perception: A Review, *Sensors*, 24(14), 4440.

[323] Taylor, J. (2024) Digital afterlife – how to deal with social media accounts when someone dies.

[324] Techround (2024) How The Rise Of Grief Tech Comforts The Broken Hearted.

[325] Terryn, S. et al. (2017) Self-healing soft pneumatic robots, *Sci. Robot.* 2,eaan4268(2017).

[326] Tester, P. (2025) What are Fullz? How Hackers & Fraudsters Obtain & Use Fullz.

[327] Thaihut (2026) Why China is testing humanoid robots at its border with Vietnam right now.

[328] Thales (2025) 2025 Thales Data Threat Report.

[329] The Rise of AI-Powered Threats and Other Mobile Risks Highlight Why It's Time to Rethink Your Security Architecture.

[330] The White House (2025) National Security Strategy of the United States of America November 2025.

[331] Tidy, J. (2024) Firm hacked after accidentally hiring North Korean cyber criminal.

[332] Todesfall-Checkliste.de. (2020) Durchschnittliche Kosten von Bestattungen in Deutschland (in Euro). Statista.

[333] Tom, G. et al. (2025) From Molecules to Mixtures: Learning Representations of Olfactory Mixture Similarity using Inductive Biases, Preprint 2501.16271.

[334] Tong, Y., et al. (2024) Advancements in Humanoid Robots: A Comprehensive Review and Future Prospects, IEEE/CAA Journal of Automatica Sinica, 11(2), pp. 301-328.

[335] Trend Micro (2025) Trend Micro State of AI Security Report, 1H 2025.

[336] Trend Micro (2026) The AI-Fication of Cyberthreats.

[337] TÜV Verband (2025) TÜV Cybersecurity Studie 2025.

[338] Tutika, R. et al. (2021) Self-healing liquid metal composite for reconfigurable and recyclable soft electronics, Commun Mater 2, 64 (2021).

[339] UNIDIR Security and Technoligy Programme (2026) Securing Cyberspace for Peace: Insights into Cyberthreats and International Security in 2025.

[340] Van Mulders, J., et al. (2022) Wireless Power Transfer: Systems, Circuits, Standards, and Use Cases, Sensors, 22(15), 5573.

[341] Verfassungsblog (2024) Gaza, Artificial Intelligence, and Kill Lists.

[342] Verizon Business (2025) 2025 Data Breach Investigations Report.

[343] Wang Y. & Weng G.-M. (2025) Nuclear batteries: Potential, challenges and the future. The Innovation Energy 2:100079.

[344] We Are Social, DataReportal, Meltwater (2025) Ranking der größten Social Networks und Messenger nach der Anzahl der Nutzer im Februar 2025 (in Millionen). Statista.

[345] WEF (2025) Cybercrime Atlas: Impact Report 2025.

[346] WEF (2026) Global Cybersecurity Outlook 2026.

[347] WEF (2026) The Global Risks Report 2026.

[348] Weizenbaum Institut (2024) Digitale Souveränität.

[349] Wen, S. (2024) The real battle for data privacy begins when you die.

[350] Wright, Q. (1936) The Causes of War and the Conditions of Peace, Journal of the Aeronautical Science Volume 3.

[351] Xie, Y. et al. (2025) Complex-valued matrix-vector multiplication using a scalable coherent photonic processor, Science Advances, 11(eads7475).

[352] Yaghmazadeh, O. (2024) Pulsed High-Power Radio Frequency Energy Can Cause Non-Thermal Harmful Effects on the BRAIN, IEEE Open Journal of Engineering in Medicine and Biology, vol. 5, pp. 50-53.

[353] Yang, Q. (2025) Principles for the Standardized Handling of Digital Property Inheritance. Humanities and Social Science Research, 8(3), p29.

[354] Yu, C. & Wang, P. (2022) Dexterous Manipulation for Multi-Fingered Robotic Hands With Reinforcement Learning: A Review, Frontiers in Neurorobotics.

[355] Yuan, W. et al. (2017) GelSight: High-Resolution Robot Tactile Sensors for Estimating Geometry and Force, Sensors, 17(12), 2762.

[356] Záboji, N. & Sachse, M. (2026) Frankreich wirft Teams, Zoom und Co. raus, Frankfurter Allgemeine Zeitung.

[357] ZEW (2024) Digitale Souveränität: Unternehmen sehen Abhängigkeit bei KI und Software.

[358] ZEW (2025) Digitale Souveränität: Herausforderungen aus Sicht der Unternehmen.

[359] Zhang, S. et al. (2021) A Robotic Electrochemical Biosensor Based on Kinetic Electronics Technique, IEEE Sensors, 2021, pp. 1-4.

[360] Zhang, R., et al. (2025) Characteristics and driving factors of power generation performance in microbial fuel cells: An analysis based on the CNKI database, Frontiers in Microbiology, 16, 1620539.

[361] Zhao, X. et al. (2025) Remote Vital Sign Monitoring Based Millimeter-Wave Sensing, IEEE Access, 24(12).

[362] Zhou, K. et al. (2023) Dimensional emotion recognition from camera-based PRV features, Volume 218.





Die hier vorgestellten Fälle sind lediglich ein Auszug und bei Weitem nicht vollständig.



## CULT OF THE DEAD COW SEIT 1984

2025

2025

## IMPRESSUM

### Herausgeber

Schwarz Digits KG  
Am Campus 1  
74177 Bad Friedrichshall  
Deutschland

Sitz: Neckarsulm (ab 01.05.2026 Bad Friedrichshall)  
Registergericht: Stuttgart HRA 737212  
USt-IdNr.: DE335467503

E-Mail: [info@schwarz-digits.de](mailto:info@schwarz-digits.de)  
Website: [www.schwarz-digits.de](http://www.schwarz-digits.de)  
LinkedIn: <https://www.linkedin.com/company/98943909>  
Youtube: <https://www.youtube.com/@SchwarzDigits>

Wissenschaftliche Leitung: Dr. Alexander Schellong

Autoren: Dr. Leonid Glanz, PD Dr. Robert Koch, Dr. Patricia Köpfer, Dr. Alexander Schellong, Sofie Schönborn

Design: André Renvert, Lukas Breitreutz (infotectures)

Die Zusammenfassung der bestehenden und geplanten Regulatorik im Cybersecurity Kontext stellt keine Rechtsberatung dar und erhebt keinen Anspruch der Vollständigkeit. Sie dient dazu den Lesern einen Überblick zu verschaffen.

Die Schwarz Digits KG wird vertreten durch die Ny-Stiftung mit Sitz in Dresden, Landesdirektion Sachsen, AZ 20-2245/589, die ihrerseits gemeinsam durch zwei gesamtvertretungsberechtigte Vorstände, u. a. Christian Müller und Rolf Schumann vertreten wird.



