Unternehmen in Deutschland auf ihrem Weg zur digitalen Souveränität

Welche Rolle spielt digitale Souveränität und mit welchen Maßnahmen ist sie zu erreichen?

techconsult TECHNOLOGY MARKET ANALYSTS | EIN UNTERNEHMEN DER heise group | IONOS

Informationen zur Studie

Erstellt durch

techconsult
TECHNOLOGY MARKET ANALYSTS
EIN UNTERNEHMEN DER heise group

Kontakt

techconsult GmbH
E-Mail: info@techconsult.de
Tel.: +49 561 8109 0
Fax: +49 561 8109 101
Web: www.techconsult.de

Veröffentlichungsdatum

03/2024

In Zusammenarbeit mit

IONOS

Sonstige Informationen

Aus Gründen der besseren Lesbarkeit wird bei Personenbezeichnungen und personenbezogenen Hauptwörtern in dieser Studie die männliche Form verwendet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter. Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.

Aufgrund von Rundungsanpassungen summieren sich einige Summen möglicherweise nicht zu 100%.

Inhaltsverzeichnis

Executive Summary

Digitale Souveränität ist eine wesentliche Voraussetzung, um die Erreichung wichtiger Unternehmensziele zu gewährleisten. Sie umfasst die unabhängige Selbstbestimmung in Bezug auf die Nutzung und Gestaltung digitaler Systeme, der darin erzeugten und gespeicherten Daten sowie der damit abgebildeten Prozesse. Viel stärker als bei traditionellen IT-Dienstleistungen besteht bei Cloud-Dienstleistungen in den Unternehmen noch eine große Abhängigkeit von globalen Dienstleistern. Die Nutzung einer IT- Infrastruktur von einem europäischen Cloudanbieter ist für die Unternehmen ein wichtiger Schritt zum Erreichen digitaler Souveränität.

Zum Stand der digitalen Souveränität in Unternehmen in Deutschland ab 50 Mitarbeitenden hat techconsult im Auftrag von IONOS die vorliegende Studie durchgeführt. 226 Entscheidungsträger*innen, Manager*innen und Administrator*innen aus dem IT-Bereich geben Auskunft zur Bedeutung der digitalen Souveränität für ihr Unternehmen. Im Fokus der Studie stehen Maßnahmen und Handlungsoptionen in den Bereichen Hardware, Software und Daten.

Digitale Souveränität spielt eine wichtige Rolle

Zu den Kernergebnissen zählt, dass zentrale Aspekte digitaler Souveränität für die Unternehmen eine wichtige Rolle spielen. So geben die befragten IT-Entscheider unter anderem an, dass selbstbestimmtes Handeln, die Kontrolle über Datenzugriffe und -flüsse sowie die Vermeidung von strategischen Abhängigkeiten einen hohen Stellenwert für sie einnehmen.

Reduzierung von Abhängigkeiten

Trotz der hohen Bedeutung von digitaler Souveränität, weisen über 50 Prozent der befragten Unternehmen im Bereich des Cloud-Computings aktuell starke Abhängigkeiten von Nicht-EU-Dienstleistern auf. Das betrifft alle wichtigen Cloud-Segmente. 78 Prozent der Unternehmen mit Abhängigkeiten von Nicht-EU-Anbietern verfolgen jedoch das Ziel, unabhängiger zu werden. Zu den Maßnahmen, die in diesem Zusammenhang als wichtig erachtet werden, zählen unter anderem Multi-Cloud-Strategien sowie der Rückgriff auf europäische Anbieter, die keiner Drittstaatenjurisdiktion unterliegen.

Maßnahmen seitens Politik und Gesellschaft

Die Verwirklichung digitaler Souveränität ist ein Prozess, mit dem sich die Unternehmen kontinuierlich befassen müssen. Aus Sicht der Unternehmen sind auch Politik und Gesellschaft gefragt, in ihrem jeweiligen Verantwortungsbereich einen Beitrag zu leisten, um die digitale Souveränität nachhaltig zu stärken. Zu den geforderten Maßnahmen zählen:

- **Stärkung der Widerstandsfähigkeit gegenüber Cyber-Bedrohungen (48 Prozent)**
- **Digitale Bildung und Vermittlung von IT-Skills im Schulunterricht (46 Prozent)**
- **Gütesiegel zu Sicherheitseigenschaften von IT-Produkten und -Services (35 Prozent)**
- **Stärkung regionaler Lieferketten (33 Prozent)**
- **Förderung innovativer Technologien und Produktionsmethoden (29 Prozent)**

Anforderungen an Cloud-Dienstleister

Darüber hinaus zeigen die Ergebnisse, dass Unternehmen sehr konkrete Erwartungen an ihre Cloud-Dienstleister haben. Hierzu gehören beispielsweise jeweils mit einem Anteil von 82 Prozent transparente Zugriffsrechte auf Daten und die Zugangs- und Rechtekontrolle. 80 Prozent der Unternehmen wünschen sich die volle Kontrolle über ihre eigenen Daten. Sicherheitszertifizierungen und EU-DSGVO-Konformität machen die Top 5-Anforderungen komplett.

Einleitung

Die digitale Souveränität ist in der vernetzten und digitalisierten Welt zu einem zentralen Begriff geworden. Dieser bezieht sich auf „die Fähigkeit zur unabhängigen Selbstbestimmung in Bezug auf die Nutzung und Gestaltung digitaler Systeme selbst, der darin erzeugten und gespeicherten Daten sowie der damit abgebildeten Prozesse“ (* Zitat lt. Bundeswirtschaftsministerium). Für Unternehmen bedeutet dies, ihre eigenen digitalen Ressourcen zur Stärkung ihrer Resilienz autonom zu kontrollieren, zu schützen und zu gestalten. Viele Unternehmen sind in einem weltweiten Netzwerk von Lieferanten, Kunden und Partnern eingebunden. Dieser enge Austausch schafft Chancen für wirtschaftliches Wachstum, birgt jedoch gleichzeitig Risiken durch Abhängigkeiten von externen Faktoren.

Die jüngsten Ereignisse und geopolitischen Spannungen machen deutlich, welche nachteiligen Konsequenzen mit übermäßigen wirtschaftlichen Abhängigkeiten einhergehen können. Das betrifft auch den Bereich der Informationstechnologie. In Zukunft wird es kein Unternehmen geben, das auf Cloud-Computing-Technologien verzichten kann. Doch trotz aller Vorteile birgt die Nutzung von Cloud-Services auch Risiken durch eine zu starke Abhängigkeit von globalen Nicht-EU-Dienstleistern.

Mit der schnell zunehmenden Vernetzung von IT und Wirtschaft erhält die digitale Souveränität höchste Relevanz und rückt immer stärker in den Fokus der Unternehmen und Organisationen.

Der Weg zur digitalen Souveränität ist kein einfacher. Er ist ein Prozess, der kontinuierlich erfolgen muss und von den Unternehmen eine ganzheitliche Herangehensweise erfordert. Beginnend mit einer Bestandsaufnahme bestehender Abhängigkeiten zu Nicht-EU-Anbietern und einer Analyse darüber, wo Abhängigkeiten möglicherweise reduziert werden können, schließt der Prozess zur Souveränität die Einhaltung strikter Datenschutzstandards, die Vermeidung von Abhängigkeiten von einzelnen Anbietern, den Schutz sensibler Daten vor unautorisiertem Zugriff, die Kontrolle über IT-Infrastrukturen und die Schaffung flexibler sowie widerstandsfähiger digitaler Systeme mit ein.

Die Studie „Unternehmen in Deutschland auf ihrem Weg zur digitalen Souveränität“ wurde in Zusammenarbeit mit IONOS konzipiert und von tech**consult** durchgeführt. Anlass für die Studie war es, der zentralen Frage nachzugehen, welche Bedeutung digitale Souveränität für Unternehmen und Organisationen aktuell hat. 226 Unternehmen in Deutschland ab 50 Mitarbeitenden wurden zur Souveränität befragt und lieferten unter anderem Antworten auf folgende Fragen: Vor welchen Herausforderungen stehen die Unternehmen? Welche Ansätze ergreifen sie auf dem Weg zur digitalen Souveränität und welche Maßnahmen werden von Politik und Gesellschaft erwartet?

Stellenwert von digitaler Souveränität für Unternehmen

Digitale Souveränität in ihren unterschiedlichen Ausprägungen spielt für die befragten Unternehmen eine wichtige Rolle. Die Antworten, welche Aspekte digitaler Souveränität einen hohen Stellenwert einnehmen, fallen dabei sehr vielfältig aus. In besonderer Weise bedeutet Souveränität für die IT-Entscheider selbstbestimmtes Handeln (79 Prozent). Nachdem in der heutigen digitalen Welt Daten für Unternehmen zu einem der wertvollsten Güter geworden sind, ist auch selbstbestimmtes Datenmanagement für die Betriebe zu einem entscheidenden Faktor geworden. Für einen ähnlich hohen Prozentsatz der Befragten sind die Datenhoheit und die Kontrolle über die generierten und gesammelten Daten ein wichtiger Bestandteil digitaler Souveränität.

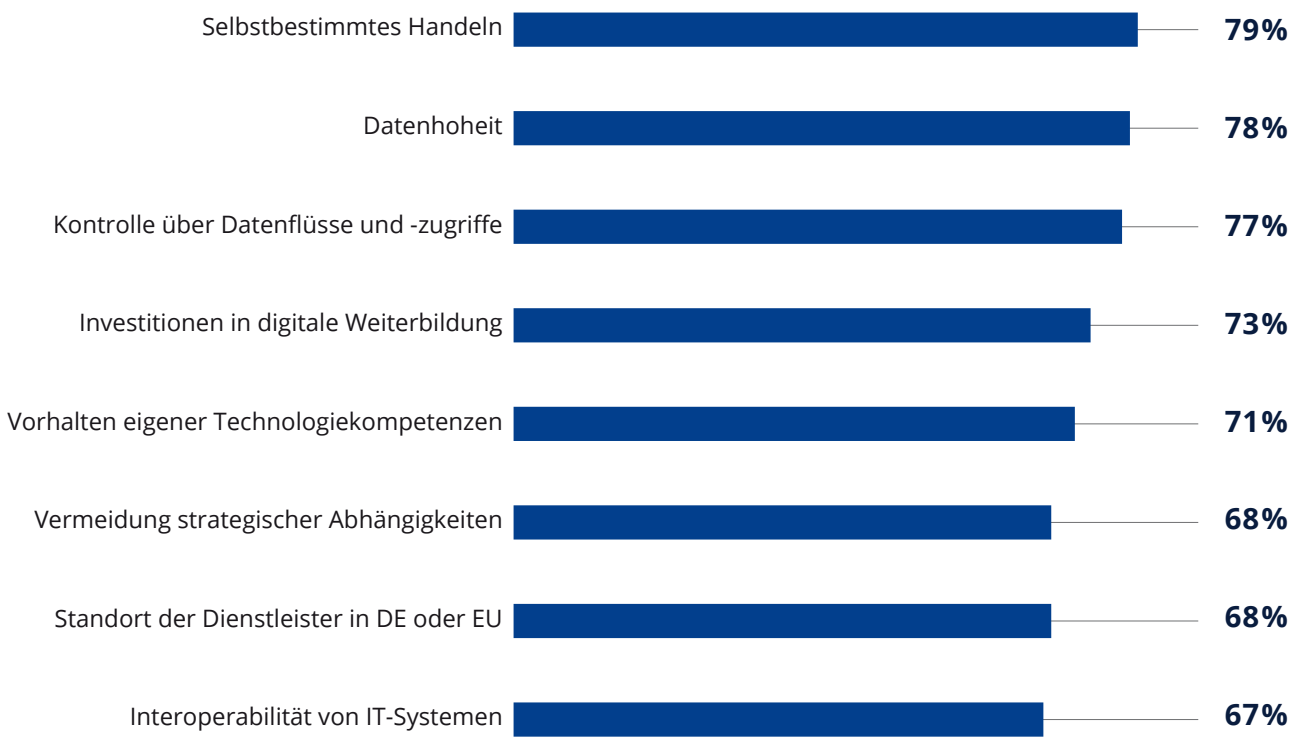
Durch die Kontrolle über ihre eigenen Daten können Unternehmen sicherstellen, dass sensible Informationen nicht in die falschen Hände gelangen. Sie können robustere Sicherheitsmaßnahmen implementieren und sich besser vor Cyberangriffen und Datenschutzverletzungen schützen.

Wichtig für 68 Prozent der befragten Unternehmen ist es, dass der Standort der Dienstleister von digitalen Technologien und Anwendungen in Deutschland oder der EU ist. Das wohl wichtigste Argument dafür dürfte die Datenschutz-Grundverordnung (DSGVO) sein, die gegenüber Anbietern aus nicht-EU-Staaten ein höheres Maß an Datenschutz und Sicherheit bietet.

Abbildung 1

Bitte geben Sie uns eine Einschätzung, welchen Stellenwert das Thema digitale Souveränität für Ihr Unternehmen derzeit hat.

Basis: 226 Unternehmen | Mehrfachauswahl möglich | Nennungen mit „Sehr großen Stellenwert“ und „Großen Stellenwert“



Gleich groß ist der Anteil an Unternehmen (68 Prozent), die in der Vermeidung einer technologischen und strategischen Abhängigkeit von einzelnen Anbietern und Ländern einen wichtigen Aspekt der Souveränität sehen. Souveränes Handeln setzt die Unternehmen in der Lage, ihre Interessen zu schützen und ihre digitale Zukunft selbst zu gestalten. Voraussetzung dafür ist, ihre eigenen Stärken auszubauen und in Zukunftstechnologien und in die IT-Sicherheit zu investieren.

Künstliche Intelligenz (KI) gilt als eine der wichtigsten Zukunftstechnologien und ist eine Schlüsseltechnologie, die Potenzial für Wirtschaftswachstum und Produktivitätszuwächse mit sich bringt. Der Einsatz von KI macht Geschäftsprozesse effizienter, erhöht die Leistungsfähigkeit und birgt Potenziale neuer Geschäftsmodelle. Investitionen in Forschung und Entwicklung helfen Unternehmen, ihre eigenen KI-Kompetenzen aufzubauen und weniger abhängig von externen Anbietern zu sein. Die aktive Beteiligung an der Regulierung im Kontext der KI stellt sicher, dass die Maßnahmen sowohl Innovation fördern als auch ethische Standards gewährleisten.

Das Vorhalten eigener Technologiekompetenzen und Produktionskapazitäten im eigenen Wirtschaftsraum ist im Kontext der Souveränität ein ebenso wichtiger Faktor, dem 71 Prozent der Unternehmen eine große Bedeutung beimessen. Dieser Faktor macht sie unabhängiger und resilienter gegenüber externen Einflüssen, wie zum Beispiel politischen Konflikten und Lieferkettenunterbrechungen.

Abhängigkeit von Nicht-EU-Dienstleistern

Obwohl der Vermeidung strategischer Abhängigkeiten von den Unternehmen eine hohe Bedeutung beigemessen wird, weisen über die Hälfte der befragten Unternehmen starke Abhängigkeiten auf, insbesondere von Nicht-EU-Dienstleistern. Das betrifft sowohl alle wichtigen Cloud-Service-Modelle von Infrastruktur-as-a-Service (IaaS) über Software-as-a-Service (SaaS) und Plattform-as-a-Service (Paas) bis Data-as-a Service (DaaS) als auch KI-Anwendungen.

Rund ein Viertel schätzt seine Abhängigkeit von Nicht-EU-Dienstleitern zwar als gering ein, doch nur Minderheiten (Anteile unter 20 Prozent) können von sich behaupten, völlig unabhängig von Nicht-EU-Dienstleistern zu sein.

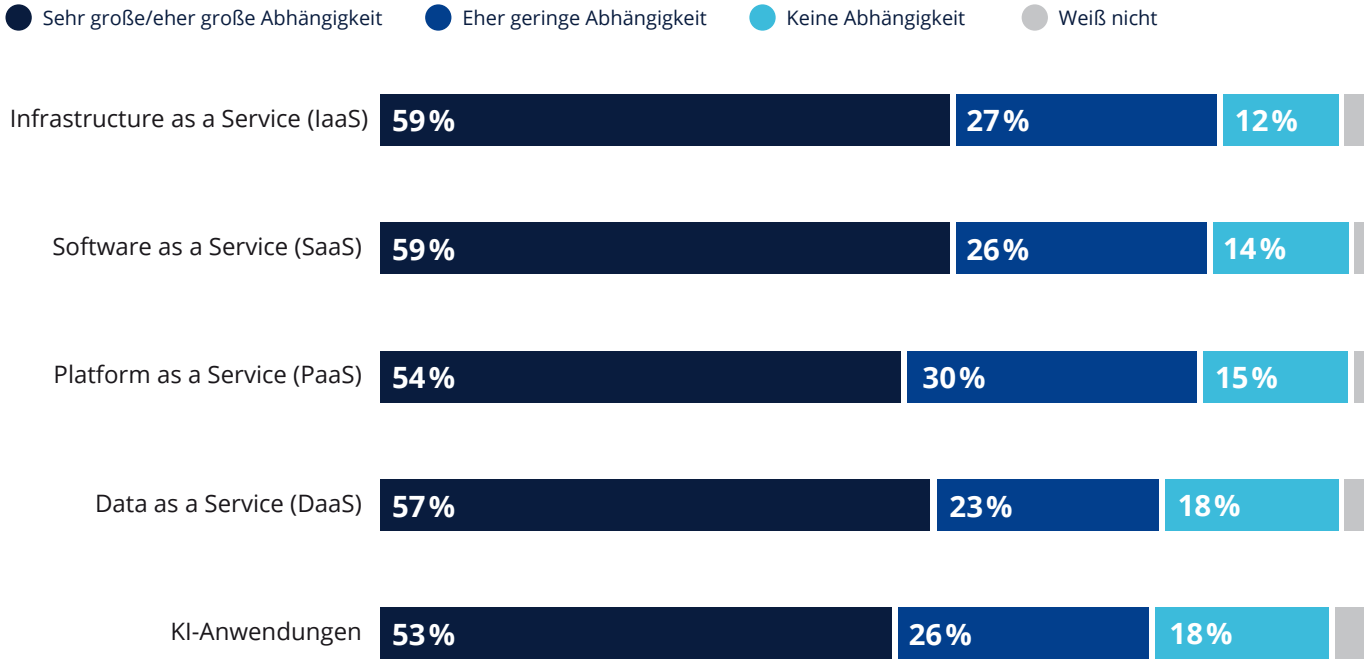
Größere Unternehmen ab 1.000 Mitarbeitenden konnten ihre Abhängigkeit von Nicht-EU- Dienstleistern über alle Bereiche bereits deutlicher reduzieren als kleinere Unternehmen. Während der Wert für größere Abhängigkeiten bei der IT-Infrastruktur (IaaS) beispielsweise bei Unternehmen mit 50 bis 249 Mitarbeitenden bei 65 Prozent liegt, sind es bei Unternehmen mit 1.000 und mehr Beschäftigten 47 Prozent. In den Bereichen PaaS, SaaS, DaaS und bei den KI-Anwendungen sehen die Relationen relativ ähnlich aus.

Von den Unternehmen, die derzeit von Nicht-EU-Dienstleistern abhängig sind, haben sich 78 Prozent der IT-Verantwortlichen das Ziel gesetzt, ihre Abhängigkeit zu reduzieren.

Abbildung 2

Wie schätzen Sie Ihre derzeitige Abhängigkeit von NICHT-EU-Dienstleistern in Ihrem Unternehmen ein?

Basis: 226 Unternehmen



Welche Faktoren sind die Gründe für bestehende Abhängigkeiten?

Die Abhängigkeit von Nicht-EU-IT-Dienstleistern resultiert in erster Linie aus wirtschaftlichen Überlegungen. 43 Prozent der befragten Unternehmen sehen Kostenvorteile als einen relevanten Grund für bestehende Abhängigkeiten. Neben wirtschaftlichen Aspekten gibt es jedoch weitere Gründe, die zu einer umfassenden Nutzung nicht-europäischer Anbieter führen.

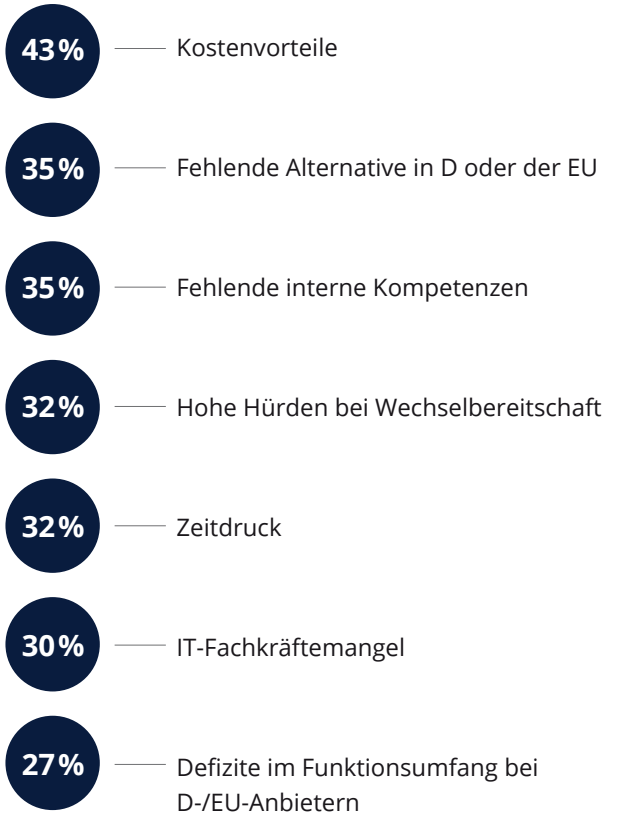
So fehlt es einem Drittel der Unternehmen an Alternativen in Deutschland beziehungsweise in Europa. Zeitdruck und Fachkräftemangel können in den Unternehmen dazu führen, dass der Marktüberblick fehlt und verfügbare Alternativen nicht gefunden werden. Insbesondere kleineren mittelständischen Unternehmen (41 Prozent) fehlt es an Kompetenzen, um alternative Angebote einzuholen, zu vergleichen und einen Wechsel des Dienstleisters vorzunehmen.

32 Prozent scheuen Hürden, die ein Anbieterwechsel möglicherweise mit sich bringen würde und halten lieber an bestehenden Vertragsverhältnissen fest. Für 27 Prozent der befragten Organisationen sind Defizite im Funktionsumfang bei europäischen Anbietern ein Grund dafür, dass die Entscheidung zugunsten eines globalen IT-Service Providers ausfällt.

Abbildung 3

Wo sehen Sie relevante Gründe für die Abhängigkeit von NICHT-EU-Dienstleistern?

Basis: 213 Unternehmen | Mehrfachauswahl möglich | Filter: Wenn Abhängigkeit besteht



Weitere Herausforderungen: Fachkräftemangel und IT-Security

Auf dem Weg zur digitalen Souveränität sehen sich die Unternehmen, neben zu starken Abhängigkeiten von einzelnen Anbietern, mit weiteren Herausforderungen konfrontiert. So stellt beispielsweise die Einhaltung von Datenschutz und Datensicherheit noch immer für jede zweite Organisation ein Problem dar. 25 Prozent der befragten Organisationen sind sich unsicher darüber, wer alles Zugriff auf ihre in der Cloud gespeicherten Daten hat. Im kleineren Mittelstand mit bis zu 249 Beschäftigen sind es sogar 34 Prozent. Die Unternehmen müssen sicherstellen, dass sie von der Erhebung bis zur Verarbeitung und Speicherung von Daten alle Anforderungen der Datenschutz-Grundverordnung (DSGVO) erfüllen. Ebenso wichtig ist die Einhaltung der Compliance, der gesetzlichen Regelungen, die für die Informationstechnologie des Unternehmens gelten. Mehr als jedem zweiten Unternehmen ab 1.000 Mitarbeitern bereitet das noch Sorge.

Auch die steigende Anzahl von Cyberangriffen stellt eine zunehmende Bedrohung für die Sicherheit von Unternehmensdaten dar. Seit Beginn des Ukraine-Kriegs hat sich die Bedrohungslage weiter verschärft. 36 Prozent der Unternehmen werden dadurch herausgefordert und haben Schwierigkeiten, ihre IT-Sicherheit zu gewährleisten. Besonders hoch ist der Anteil mit 49 Prozent in Unternehmen ab 1.000 Mitarbeitenden.

Ein Drittel der Unternehmen kämpft darüber hinaus mit personellen Engpässen in der IT. Ihnen fehlt es an Fachkräften für Informationstechnologie und Cybersicherheit. 30 Prozent der Unternehmen haben Schwierigkeiten, geeignete Weiterbildungsmaßnahmen zu konzipieren und umzusetzen, um die digitalen Kompetenzen bei Mitarbeitenden auszubauen.

Abbildung 4

Welche der genannten Herausforderungen trifft auf Ihr Unternehmen zu?

Basis: 226 Unternehmen | Mehrfachauswahl möglich

- Datenschutz- und Datensicherheit **49%**
- Zunehmende Cyberangriffe **36%**
- Einhaltung der IT-Compliance **34%**
- Fehlende Fachkräfte im IT-Bereich **32%**
- Ausbau digitaler Kompetenzen **30%**
- Schnittstellenoffenheit/API-Vielfalt **26%**
- Unsicherheiten über Datenzugriffe **25%**
- Fehlende Flexibilität innerhalb IT **21%**
- Vermeidung eines Vendor Lock In **18%**

In Zeiten der zunehmenden Vernetzung können auch offene Schnittstellen vorteilhaft sein. Sie erleichtern die Integration neuer Ressourcen und Dienste, was Unternehmen die Möglichkeit gibt, ihre Systeme flexibel zu erweitern, um mit wachsenden Anforderungen Schritt zu halten. Neben den Vorteilen müssen die Unternehmen jedoch auch die damit verbundenen Risiken berücksichtigen. 26 Prozent der Befragten sehen in der Vielfalt von Programmierschnittstellen eine Herausforderung. Die Verwaltung einer Vielzahl von APIs (Application Programming Interfaces) ist komplex und kann zeitaufwendig sein, vor allem wenn die APIs nicht gut dokumentiert oder standardisiert sind. Darüber hinaus ist mit offenen Schnittstellen das Risiko von Sicherheitslücken verbunden.

Handlungsoptionen zum Erreichen digitaler Souveränität

Strukturelle Maßnahmen

Die Gewährleistung digitaler Souveränität erfordert eine umfassende Strategie, die auch Maßnahmen der IT-Infrastruktur betreffen.

Ein Multi-Cloud-Ansatz ist Teil einer Strategie, um die Souveränität zu stärken und wird von drei Viertel der befragten Unternehmen genannt. Eine solche Strategie verhindert nicht nur einseitige Abhängigkeiten von einzelnen Anbietern, die Nutzung unterschiedlicher Cloud-Anbieter bietet den Unternehmen zudem Flexibilität, Redundanz und Ausfallsicherheit.

Eine weitere Maßnahme sehen die IT-Verantwortlichen darin, die Abhängigkeit von proprietärer Hardware zu reduzieren (82 Prozent). Hardwaresysteme, die auf geschlossenen Systemen und patentierten Technologien basieren, führen zu Abhängigkeiten, die die Autonomie beeinträchtigen.

84 Prozent der Unternehmen sind überzeugt, dass vertragliche Regelungen zu Server- bzw. Datenstandorten, Zugriffsrechten und Sicherheitsmaßnahmen die Grundlage für eine sichere und souveräne Zusammenarbeit legen.

Einen wichtigen Schritt zur Stärkung der digitalen Souveränität sehen die befragten Unternehmen auch im Rückgriff auf europäische Anbieter oder solche, die keiner Drittstaatenjurisdiktion unterliegen. Kommen Anbieter zum Einsatz, die ausschließlich europäischem Recht unterliegen, fördert es das Vertrauen. Und werden eigene Fachkräfte durch das Know-how vertrauensvoller Partner unterstützt, können die Unternehmen eine robuste digitale Infrastruktur schaffen, die Sicherheit bietet und den Herausforderungen gewachsen ist.

Abbildung 5

Inwiefern unterstützen die folgenden Maßnahmen Ihr Unternehmen auf Ihrem Weg zur digitalen Souveränität?

Basis: 226 Unternehmen | Mehrfachauswahl möglich

	Unterstützend	Wenig unterstützend	Nicht unterstützend
Vertragliche Regelungen zu Datenstandorten, Zugriffsrechten und Sicherheitsmaßnahmen	**84%**	**13%**	**2%**
Reduzierung des Einsatzes von proprietärer Hardware	**82%**	**17%**	**1%**
Rückgriff auf europäische Anbieter bzw. Anbieter, die keiner Drittstaatenjurisdiktion unterliegen	**76%**	**19%**	**5%**
Einsatz von zertifizierten Netzwerkkomponenten, die frei von Backdoor-Funktionen sind	**76%**	**20%**	**4%**
Selbstständiges Wiederherstellen der Prozesse oder mit Hilfe von vertrauenswürdigen Partnern	**75%**	**19%**	**6%**
Nutzung von redundanten Netzwerkverbindungen	**75%**	**20%**	**5%**
Nutzung unterschiedlicher Private- oder Public-Cloud-Anbieter für unsere Daten und Dienste	**72%**	**22%**	**6%**

Ansätze im Bereich der Software

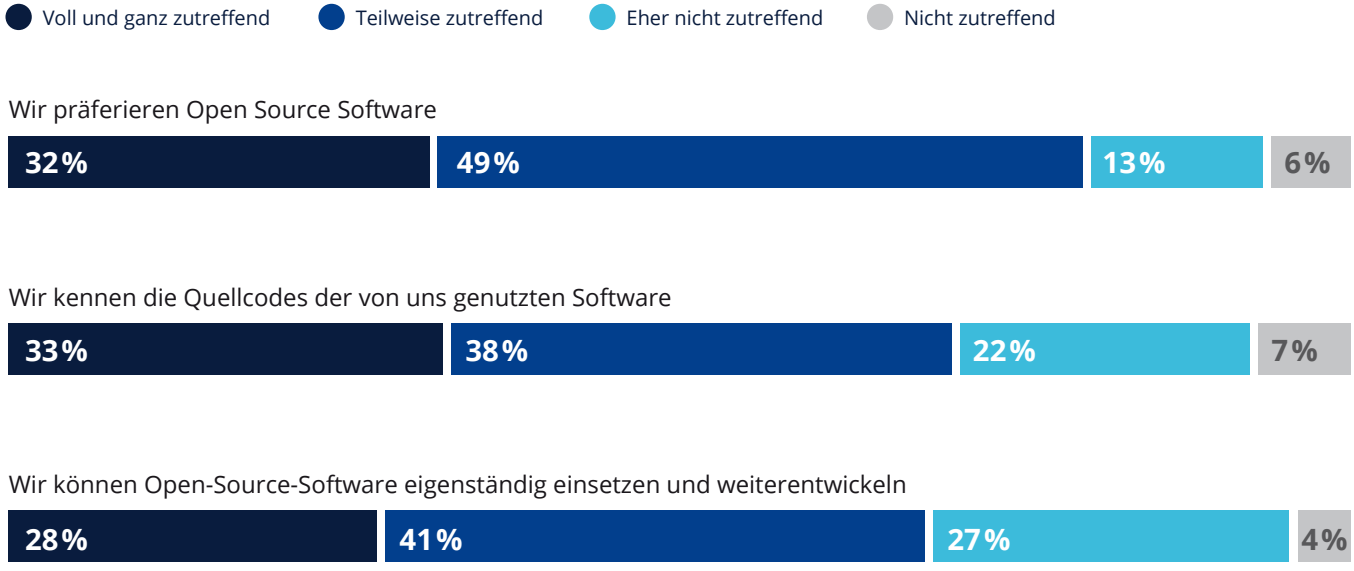
Im Bereich der Software lassen sich Abhängigkeiten von einzelnen Anbietern beispielsweise durch den Einsatz von Open-Source-Anwendungen reduzieren. Lösungen, bei denen der Quellcode eingesehen und genutzt werden kann, ermöglichen Interoperabilität zwischen verschiedenen Softwarelösungen. Darüber hinaus tragen Open-Source-Lösungen zur Unabhängigkeit bei, denn die Software kann von eigenen Entwicklern selbstständig an die unternehmensinternen Bedürfnisse angepasst werden. Dies reduziert die Risiken von Lieferantenabhängigkeit und ermöglicht eine größere Kontrolle über die Software. 32 Prozent der befragten Unternehmen präferieren Open-Source-Software. Allerdings zeigen sich 49 Prozent auch zurückhaltend und stimmen nur teilweise zu.

Neben den Vorteilen wie Skalierbarkeit und Kosteneffizienz, sind auch potenzielle Nachteile zu berücksichtigen. Eine Open-Source-Lösung bietet beispielsweise nicht immer die Sicherheit eines proprietären Systems, es fehlt der klassische Support. Die Erkennung und Korrektur von Fehlern und das Schließen von Sicherheitslücken sind nicht zwingend gesichert. Einen Mehrwert können Unternehmen dann erzielen, wenn sie in der Lage sind, eigenständig Open-Source-basierte Software einzusetzen und für ihre Zwecke weiterzuentwickeln. Für 28 Prozent der befragten Unternehmen trifft das zu, für weitere 41 Prozent zumindest teilweise.

Abbildung 6

Inwieweit treffen derzeit folgende Aussagen zum Einsatz von Open-Source-Software auf Ihr Unternehmen zu?

Basis: 226 Unternehmen



Wichtige Erkenntnisse ergeben sich auch zum Einsatz von Software im Allgemeinen:

Nur 36 Prozent geben an, sie seien sich vollumfänglich über die Risiken der eingesetzten Software bewusst. Dazu gehören Kenntnisse über Datenschutz- und Sicherheitsrisiken sowie Informationen über die Abhängigkeit von proprietärer Software und deren Risiken.

Ein signifikanter Anteil (43 Prozent) fühlt sich nicht ausreichend darüber informiert und ein Fünftel kennt die Risiken kaum beziehungsweise gar nicht.

Die plattformunabhängige Migration ermöglicht es Organisationen, flexibel auf sich ändernde Anforderungen, Kostenstrukturen oder entstehende Sicherheitsbedenken zu reagieren.

37 Prozent der IT-Entscheider sind in der Lage, ihre Cloud-Lösungen plattformunabhängig einzusetzen, auf weitere 44 Prozent trifft dies zumindest teilweise zu.

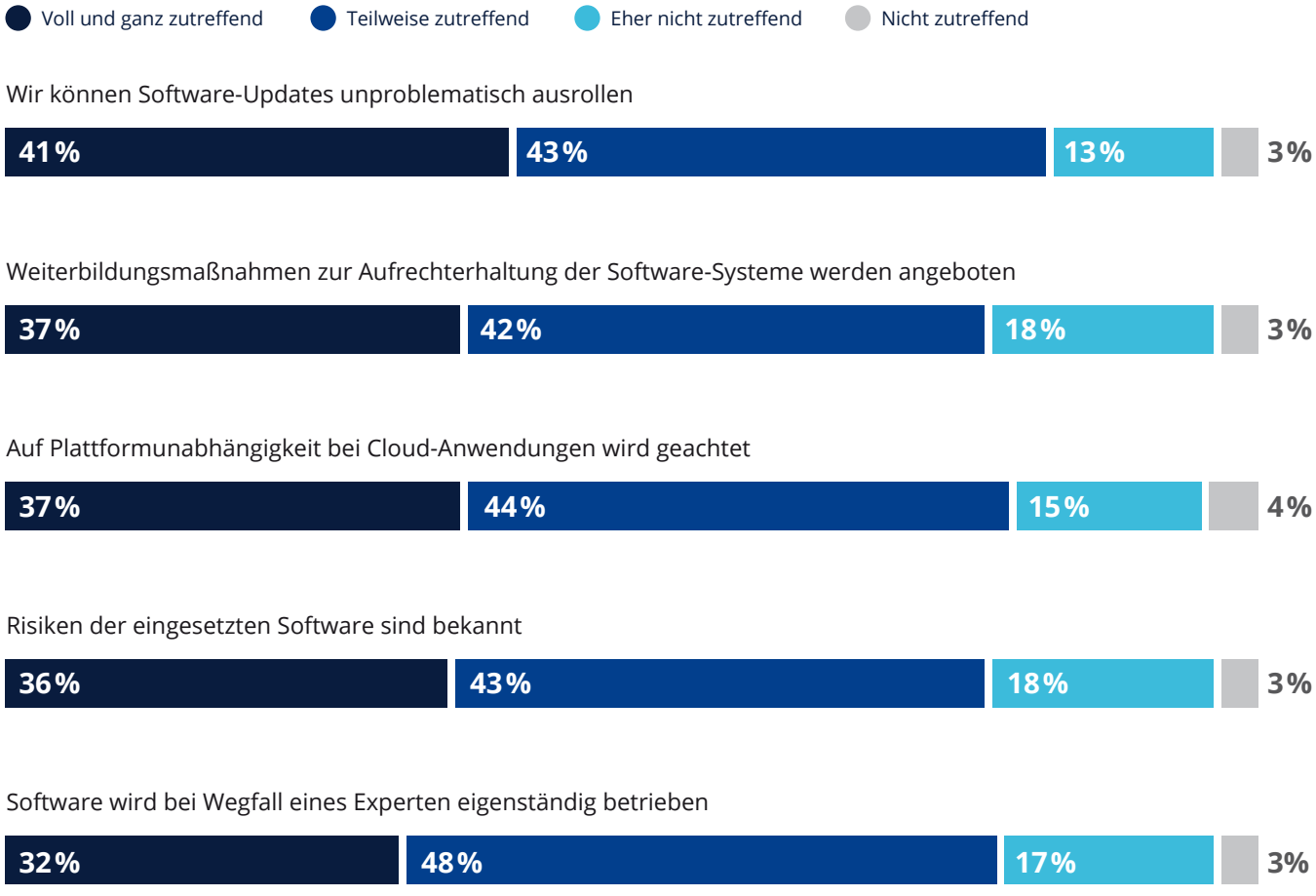
Vier von zehn Unternehmen geben an, Software-Updates unproblematisch ausrollen zu können. So können sie schneller auf Sicherheitslücken, Fehlerbehebungen oder neue Funktionen reagieren. 43 Prozent stimmen dem zumindest teilweise zu.

Darüber hinaus ist auch die Qualifikation der Beschäftigten ein zentraler Schlüssel für mehr digitale Souveränität, um beispielsweise Software-Anwendungen auch dann betreiben zu können, wenn externe Experten nicht zur Verfügung stehen. Durch regelmäßige Weiterbildung können sich Mitarbeitende schneller an neue Technologien oder Trends anpassen. Das steigert ihre Leistungsfähigkeit und damit auch die Wettbewerbsfähigkeit des Unternehmens. 21 Prozent der IT-Verantwortlichen geben jedoch an, dass in ihrem Unternehmen auch Software zum Einsatz kommt, für die keine eigenen Weiterbildungsangebote existieren.

Abbildung 7

Inwieweit treffen derzeit folgende Aspekte zum Softwareeinsatz im Allgemeinen auf Ihr Unternehmen zu?

Basis: 226 Unternehmen



Maßnahmen zum Schutz der Daten

Der Schutz und die Sicherheit von Daten sind elementare Güter in der digitalen Gesellschaft und eine wichtige Voraussetzung für digitale Souveränität. Um die Datensicherheit zu gewährleisten, ist eine Kontrolle über die eigene Netzwerkinfrastruktur unverzichtbar. 74 Prozent der befragten Unternehmen setzen Maßnahmen wie ein kontinuierliches Netzwerk-Monitoring, die Implementierung von Sicherheitsaudits, starke Authentifizierung und Zugriffskontrollen um. Auf diese Weise schützen sie ihre Netzwerkinfrastruktur vor Zugriffen und Manipulationen Unbefugter. 79 Prozent der Unternehmen verbessern die Sicherheit ihrer Daten und minimieren das Risiko von Sicherheitsvorfällen, indem sie ihre Mitarbeitenden zum sicheren Umgang mit Daten sensibilisieren und qualifizieren.

Alle genannten Maßnahmen tragen dazu bei, die Autonomie der Unternehmen zu stärken und die Kontrolle über Ihre eigenen Daten zu behalten.

Die Erstellung von regelmäßigen Backups (73 Prozent) und die Zusammenarbeit mit Cloud-Anbietern, die die Vorgaben der DSGVO vollumfänglich erfüllen (70 Prozent), sind weitere wichtige Aspekte, die zur Souveränität beitragen und von vielen Unternehmen umgesetzt werden. Gleiches gilt für den verschlüsselten Datenaustausch (67 Prozent).

Abbildung 8

Inwieweit treffen die Aussagen auf Ihr Unternehmen zu?

Basis: 226 Unternehmen

	Zutreffend	Teilweise zutreffend	Nicht zutreffend
Sensibilisierung und Qualifizierung der Mitarbeitenden zum sicheren Umgang mit Daten	**79%**	**18%**	**3%**
Bewusste Entscheidung für rollenbasierte Zugriffsrechte	**74%**	**18%**	**8%**
Sicherstellung, dass Dritte keinen Zugang zur Netzwerkinfrastruktur haben	**74%**	**18%**	**8%**
Regelmäßige Backups von gespeicherten Daten	**73%**	**19%**	**8%**
Zusammenarbeit mit Cloud-Anbietern, die die Vorgaben der DSGVO vollumfänglich erfüllen	**70%**	**23%**	**7%**
Generell verschlüsselter Datenaustausch	**67%**	**24%**	**9%**

Die Rolle der Cloud-Anbieter

Anforderungen der Nutzer

Die Unternehmen haben sehr konkrete Vorstellungen davon, was ihr Cloud-Dienstleister leisten soll. Besonders wichtig ist den IT-Verantwortlichen die Transparenz über Zugriffsrechte sowie die Zugangs- und Rechtekontrolle (IAM), beide Aspekte wurden jeweils von 82 Prozent genannt. Für 80 Prozent der Unternehmen ist die Zusicherung der Datenhoheit relevant. Denn nur so haben sie die volle Kontrolle über ihre eigenen Daten.

Drei Viertel der Unternehmen ist es wichtig, dass ihre Daten ausschließlich auf europäischem Gebiet verarbeitet und gespeichert werden. Eine wichtige Rolle spielt jedoch nicht nur der Ort der Datenverarbeitung, sondern auch das Thema Compliance. In diesem Zusammenhang achten 77 Prozent der Unternehmen sehr stark auf die Einhaltung der Vorgaben, die für eine sichere und erfolgreiche Unternehmensführung notwendig sind.

Für 79 Prozent der befragten Unternehmen ist es darüber hinaus von hoher Relevanz, dass Sicherheitszertifizierungen vorhanden sind und europäisches Recht (DSGVO/GDPR) eingehalten wird. Drei Viertel sehen zudem in der Interoperabilität mit anderen Cloud-Diensten eine wichtige Anforderung. Bieten IT-Dienstleister eine kompatible technische Plattform, wird die nahtlose Zusammenarbeit zwischen verschiedenen Systemen und Anwendungen erleichtert. Das fördert die Effizienz, verbessert die Produktivität und ermöglicht es Unternehmen, flexibel auf neue Anforderungen zu reagieren.

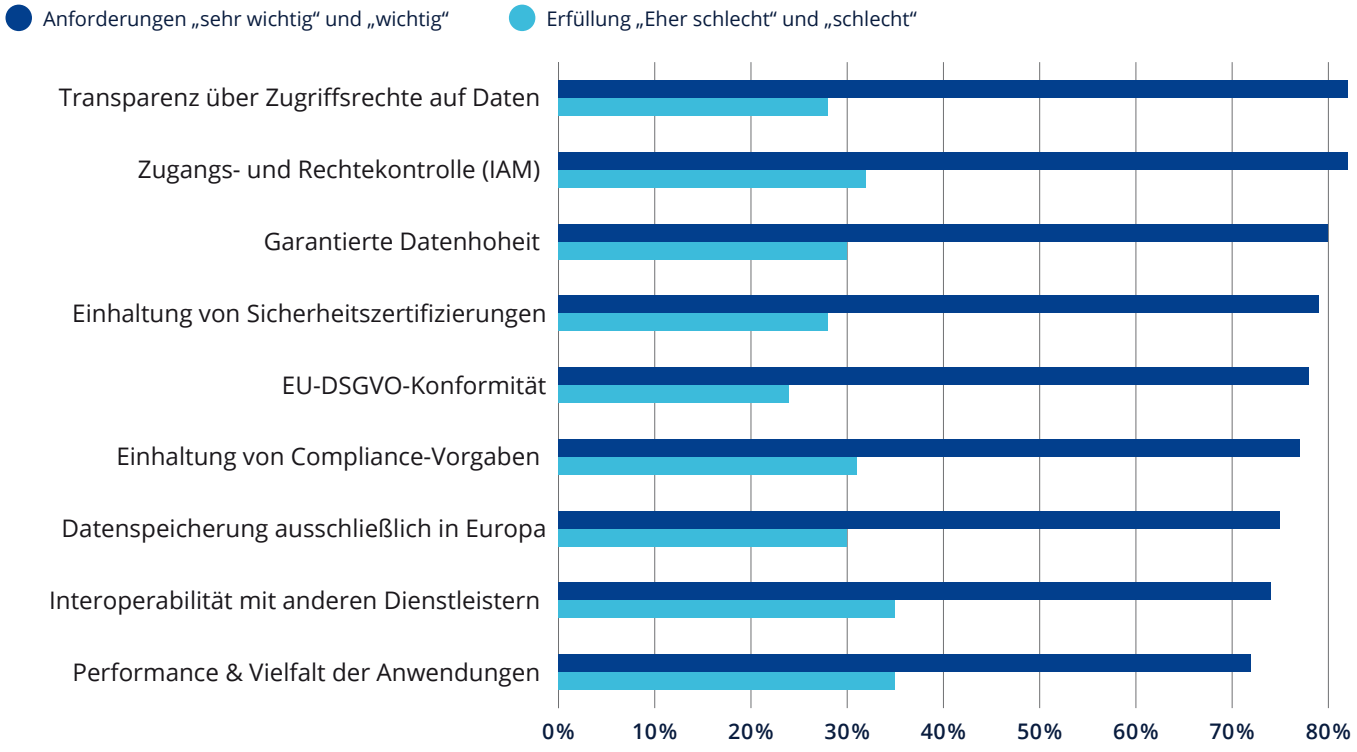
Kritikpunkte

Fragt man die Anwender nach ihrer bisherigen Einschätzung zu ihrem Cloud-Dienstleister, offenbart sich Verbesserungspotenzial. Nicht alle Anforderungen werden zur vollen Zufriedenheit der Unternehmen erfüllt.

Abbildung 9

Wie erfüllen die von Ihnen eingesetzten Cloud-Dienstleister diese Aspekte?

Basis: 226 Unternehmen



Fehlende Interoperabilität und ein Mangel an Performance sind mit jeweils 35 Prozent die am häufigsten genannten Kritikpunkte, die Unternehmen an ihre Cloud-Dienstleister richten. Defizite gibt es auch bei der Zugangs- und Rechtekontrolle (32 Prozent) sowie bei der Einhaltung der Compliance-Vorgaben (31 Prozent). Obwohl die Unternehmen durch geltendes Recht dazu verpflichtet sind, sicherzustellen, dass Daten nur bei Anbietern verarbeitet werden, die DSGVO-konform sind, scheinen 24 Prozent nicht von der Erfüllung dieser Anforderungen durch ihren Anbieter überzeugt zu sein. Ein Widerspruch, der schnellstens aufgelöst werden sollte. Hinzu kommt der Wunsch nach Transparenz über die Zugriffsrechte auf Daten. Auch diesbezüglich werden die Erwartungen der Anwender nicht vollständig erfüllt.

Wichtige Zertifizierungen

Zertifizierungen, die die Qualität, Sicherheit, Kompetenz und Verlässlichkeit eines Unternehmens bewerten, spielen für Unternehmen und Organisationen eine wichtige Rolle. Die internationale Norm für Informationssicherheitsmanagementsysteme (ISMS), ISO/IEC 27001, legt die Anforderungen für die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines dokumentierten ISMS fest.

Die Norm zielt darauf ab, sicherzustellen, dass Dienstleister angemessene Sicherheitskontrollen implementieren, um die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen nicht zu gefährden.

Unbedingt notwendig ist die Zertifizierung für 48 Prozent der befragten Unternehmen, wünschenswert ist sie für 44 Prozent. Doch nur 62 Prozent geben an, dass ihr Dienstleister über dieses Zertifikat verfügt. Ebenso groß ist der Anteil für den Kriterienkatalog C5, einem IT-Sicherheitskonzept des Bundesamtes für Sicherheit in der Informationstechnik (BSI) für die umfassende Sicherheitsbewertung von Cloud-Diensten. C5 steht für „Cloud Computing Compliance Criteria Catalogue“ und definiert Mindestanforderungen zur Informationssicherheit, Datensicherheit, Compliance und dem Sicherheitsmanagement, die nicht unterschritten werden dürfen. Der Katalog umfasst 125 Kriterien in 17 Themengebieten wie zum Beispiel der Zugangskontrolle, der Business Continuity, des Backups oder des Lieferantenmanagements. Das C5 Testat ist für 46 Prozent der befragten Unternehmen ein „Must-have“, weitere 43 Prozent befürworten es, doch nur 62 Prozent ihrer Dienstleister verfügen darüber. Je größer das Unternehmen, umso eher erfolgt die Zusammenarbeit mit Dienstleistern, die über entsprechende Zertifizierungen verfügen.

Abbildung 10

Welche Zertifizierungen sind Ihnen bei der Wahl eines IT-Dienstleisters wichtig und über welche verfügt Ihr Dienstleister?

Basis: 226 Unternehmen

	Must have	Nice to have	Unwichtig	Verfügbarkeit beim Dienstleister
ISO 9001 (Internationale Norm für Qualitätsmanagement)	53%	37%	10%	67%
ISO/IEC 27001 (Internationale Norm für IT-Informationssicherheit)	48%	44%	8%	62%
Kriterienkatalog des Bundesamtes für Sicherheit in der Informationstechnik C5	46%	43%	11%	62%
ISO/IEC 22301 (Internationale Norm für Business Continuity Management)	35%	49%	16%	53%

Welchen Beitrag können Gesellschaft und Politik leisten?

Aus Sicht der IT-Verantwortlichen sind zur Stärkung der digitalen Souveränität nicht nur die Unternehmen und ihre IT-Dienstleister in der Verantwortung, sondern auch Politik und Gesellschaft müssen in ihrem Verantwortungsbereich Maßnahmen ergreifen, um die digitale Souveränität nachhaltig zu stärken.

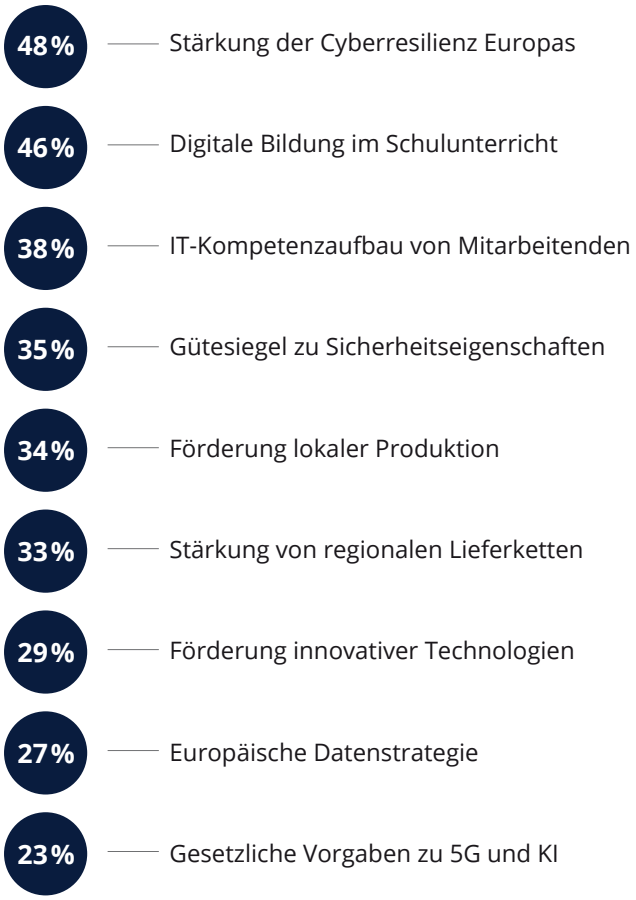
Knapp jedes zweite Unternehmen ist der Meinung, dass die Cyberresilienz Europas im Kontext digitaler Souveränität eine wichtige Rolle spielt und weiter gestärkt werden muss. Die europäischen Staaten müssen in der Lage sein, ihre IT-Infrastrukturen zu schützen und resilienter gegenüber Cyberangriffen zu machen, um auch in Krisenzeiten widerstandsfähig zu sein. Die Abhöraffäre bei der deutschen Luftwaffe ist das jüngste Beispiel dafür, wie angreifbar die Informations- bzw. Telekommunikationstechnik für Spionageattacken ist. Gleichermaßen macht sie auch deutlich, wie notwendig die Sensibilisierung der Mitarbeitenden für das Thema Sicherheit ist. 46 Prozent der Befragten sind der Ansicht, dass die Förderung von digitaler Bildung und die Vermittlung von IT-Skills bereits in den Schulunterricht integriert sein muss, damit schon frühzeitig der Grundstein für eine Generation gelegt wird, die fähig ist, die Herausforderungen und Chancen der digitalen Zukunft selbstbestimmt anzugehen. Insbesondere größeren Unternehmen ab 1.000 Beschäftigten ist darüber hinaus die Einführung von Gütesiegeln zu Sicherheitseigenschaften von IT-Produkten und -Services wichtig. Auch im Hinblick auf die lokale Produktion von Schlüsselprodukten und -komponenten fordert fast jedes zweite große Unternehmen (47 Prozent) ein Umdenken.

Für Befragte aller Unternehmensgrößen ist eine gemeinsame europäische Datenstrategie und die Schaffung eines europäischen Datenökosystems relevant. Denn in einer zunehmend digitalisierten Welt, in der Daten eine Schlüsselrolle spielen, ist es entscheidend, dass Europa eine strategische Vision für den Umgang mit Daten entwickelt, um seine digitale Souveränität und damit gleichzeitig die digitale Souveränität Deutschlands zu stärken. Eine weitere zu erwartende Maßnahme sind gesetzliche Vorgaben und Prüfkriterien beispielsweise für 5G- und KI-Technologien (23 Prozent). Sie schützen vor unerwünschter Einflussnahme und garantieren die Sicherheit sowie Vertrauenswürdigkeit dieser Technologien. Klare gesetzliche Rahmenbedingungen gewährleisten die Kontrolle über die Technologien und deren Entwicklung. Gleichzeitig wird durch die Einhaltung der Vorgaben das Vertrauen der Unternehmen in diese Technologien gestärkt.

Abbildung 11

Welche Maßnahmen erwarten Sie von Politik und Gesellschaft, um die digitale Souveränität zu gewährleisten und zu stärken?

Basis: 226 Unternehmen | Mehrfachauswahl möglich



Fazit

Digitale Souveränität wird in einer zunehmend digitalen Welt mit vielfältigen geostrategischen Herausforderungen immer wichtiger. Sie ist eine wesentliche Voraussetzung dafür, dass Unternehmen wirtschaftlich erfolgreich agieren und die Sicherheit und Kontrolle über ihre digitalen Ressourcen gewährleisten können.

Ein zentrales Ergebnis dieser Studie ist, dass die digitale Souveränität für Unternehmen eine hohe Relevanz hat und in deren Bewusstsein verankert ist. Das Erreichen digitaler Souveränität ist ein Prozess, mit dem sich die Unternehmen permanent auseinandersetzen müssen. Obwohl viele Unternehmen den Weg zur digitalen Souveränität bestreiten und Maßnahmen zur Erreichung dieses Ziels in die Praxis umsetzen, besteht in vielen Fällen noch weiterer Handlungsbedarf. Das betrifft alle drei betrachteten Fokusbereiche dieser Studie, die Software, die Daten und die Hardware.

Sehr hoch ist aktuell auch noch die Abhängigkeit der Unternehmen von Nicht-EU-Dienstleistern. Ein Großteil der Organisationen zielt jedoch darauf ab, die Abhängigkeit von globalen Dienstleistern zu reduzieren.

Ein Teil der Unternehmen hat bereits vielfältige Maßnahmen auf den Weg gebracht: Die Reduzierung von proprietären Systemen, die Wahl von offenen Standards, verschlüsselter Datenaustausch, die Zusammenarbeit mit DSGVO-konformen Dienstleistern und der Aufbau interner IT-Kompetenzen durch die Schulung von Mitarbeitenden sind nur einige genannte Schritte auf dem Weg zur digitalen Souveränität. Hinzu kommt eine bewusste Auswahl von Cloud-Diensten und der Rückgriff auf europäische bzw. deutsche Anbieter.

Auch der Multi-Cloud-Ansatz rückt immer stärker in den Fokus der Unternehmen. Kein Unternehmen wird sich in Zukunft der Cloud entziehen können. Wenn es wettbewerbsfähig sein möchte, muss es auf flexible, skalierbare und resiliente Cloud-Lösungen setzen. Dabei sollten Unternehmen und Organisationen immer sorgfältig prüfen, wie sie Cloud-Technologien nutzen und welche Dienstleister ihren spezifischen Anforderungen am besten entsprechen. Bei der Wahl des Cloud-Anbieters sollten nicht nur die Faktoren Kosten und Funktionalität eine Rolle spielen, sondern auch die Stärkung der digitalen Souveränität.

Bevor sich ein Unternehmen für die Zusammenarbeit mit einem IT-Service-Provider entscheidet, ist es hilfreich zu prüfen, ob der ausgewählte IT-Dienstleister die gewünschten Anforderungen im Kontext der digitalen Souveränität erfüllt.

IN FÜNF SCHRITTEN ZUR DIGITALEN SOUVERÄNITÄT

Ausgehend von den Ergebnissen dieser Studie sind zum Erreichen digitaler Souveränität folgende fünf Schritte wichtig und empfehlenswert. Da es sich um einen fortlaufenden Prozess handelt, sind diese Schritte regelmäßig zu überprüfen.

Bestandsaufnahme und Entwicklung einer Strategie

- Identifizierung aller verwendeten digitalen Ressourcen und Technologien
- Analyse und Bewertung von Abhängigkeiten
- Definition von klaren Zielen zum Erreichen der digitalen Souveränität und Entwicklung einer Strategie, die den Schutz, die Kontrolle und den verantwortungsvollen Umgang mit digitalen Ressourcen festlegt

Stärkung der Unabhängigkeit

- Reduzierung von Abhängigkeiten von Nicht-EU-Anbietern
- Reduzierung von proprietären Systemen und Einsatz von Open-Source-Technologien, um mehr Kontrolle zu erhalten

Gewährleistung von Datensicherheit und Datenschutz

- Einhaltung der DSGVO und anderen einschlägigen europäischen Vorschriften und Standards
- Implementierung von robusten Sicherheitsmaßnahmen, einschließlich Firewalls, Verschlüsselung und Zugriffskontrollen

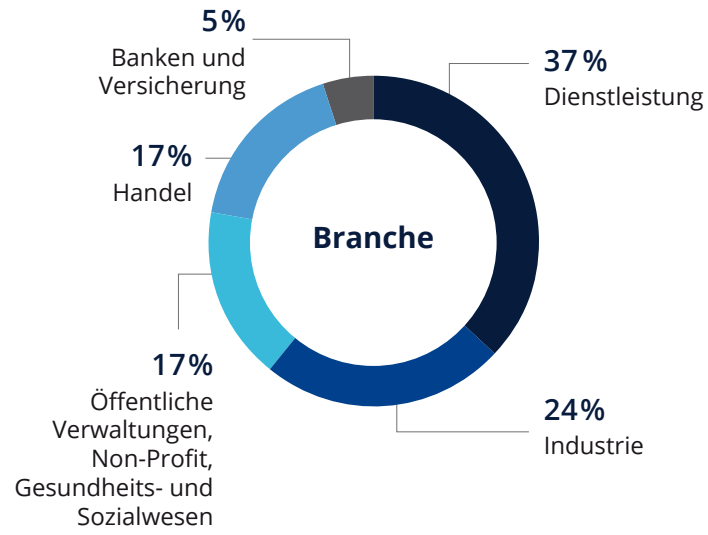
Schulungen und Sensibilisierung von Mitarbeitenden

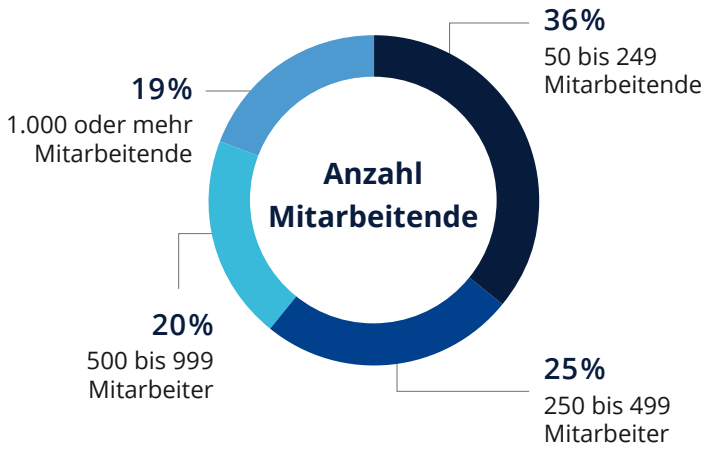
- Sensibilisierung der Beschäftigten für die Bedeutung der digitalen Souveränität und regelmäßige Schulungen von Mitarbeitenden
- Sicherstellung der Einhaltung aller geltenden Gesetze, Vorschriften und Standards im Zusammenhang mit digitaler Souveränität

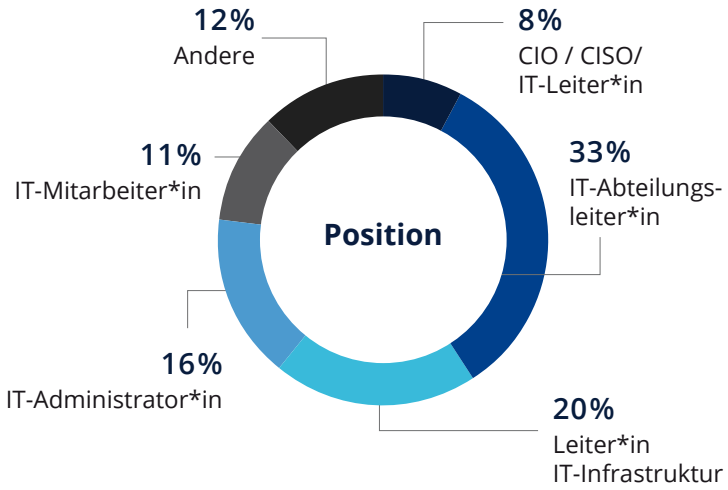
Überprüfung, Anpassung sowie Vorbereitung und Management möglicher Krisen

- Regelmäßige Überprüfungen des Sicherheitsmanagements für die IT-Infrastruktur, um Schwachstellen zu identifizieren und zu beheben
- Kontinuierliche Anpassung der Strategie an Veränderungen in der Technologie- und Bedrohungslandschaft und Entwicklung von Notfallplänen für den Fall von Cyberangriffen, Datenverlusten oder anderen digitalen Schadensereignissen

Studiendesign und Stichprobe







Die Studie „Unternehmen in Deutschland auf ihrem Weg zur digitalen Souveränität“ wurde von der techconsult GmbH im Auftrag von IONOS konzipiert und durchgeführt. 226 Unternehmen in Deutschland aller Branchen ab 50 Mitarbeitenden wurden zur Bedeutung von digitaler Souveränität und deren Umsetzung befragt. Die Befragung erfolgte über einen Online-Fragebogen. Ansprechpartner*innen waren in erster Linie IT-Leiter*innen, Leiter*innen der IT-Infrastruktur und IT-Administratoren*innen.

Weitere Informationen

Kontakt

Verena Bunk
Analyst

Telefon: +49 561 8109 144
E-Mail: verena.bunk@techconsult.de

techconsult GmbH
Baunsbergstr. 37
D-34131 Kassel

Telefon: +49 561 8109 0
Fax.: +49 561 8109 101
Web: www.techconsult.de

Über techconsult GmbH

Seit über 30 Jahren ist tech**consult** – als Research- und Analystenhaus – ein verlässlicher Partner für Anbieter und Nachfrager digitaler Technologien und Services. Mehr als 35.000 Interviews/Jahr mit Entscheidern, auf der Business- und Technologieebene, Lösungsanwendern sowie Technologie- und Serviceanbietern, bilden die neutrale Grundlage unserer Beratungs- und Projektaktivitäten.

So werden Nachfrager in ihrer digitalen Standortbestimmung und strategischen Planung ebenso unterstützt, wie in konkreten Sourcing-Prozessen, um fundierte Entscheidungen auf Basis datengestützter Fakten zu treffen. In der Entwicklung und Umsetzung individueller Go-to-Market-Strategien profitieren Anbieter sowohl strategisch als auch taktisch von der marktorientierten Unterstützung unserer Analysten und des tc-Partnernetzwerks.

IONOS

Kontakt

IONOS SE
Elgendorfer Str. 57
56410 Montabaur

www.ionos.de

Über IONOS

IONOS ist der führende europäische Digitalisierungs-Partner für kleine und mittlere Unternehmen (KMU). IONOS hat sechs Millionen Kundinnen und Kunden und ist mit einer weltweit verfügbaren Plattform in 18 Märkten in Europa und Nordamerika aktiv. Mit seinen Web Presence & Productivity-Angeboten agiert das Unternehmen als “One-Stop-Shop“ für alle Digitalisierungs-Bedürfnisse von Domains und Webhosting über klassische Website-Builder und Do-It-Yourself-Lösungen, von E-Commerce bis zu Online-Marketing-Tools. Darüber hinaus bietet IONOS Cloud-Lösungen für Firmen, die im Zuge der Weiterentwicklung ihres Geschäfts in die Cloud wechseln möchten.

Germany IONOS Cloud Kontakt
Tel: +49 30 57700 850
Mail: info@cloud.ionos.de

Impressum

techconsult GmbH
Baunsbergstraße 37
34131 Kassel

E-Mail: info@techconsult.de

Telefon: +49 561 8109 0
Telefax: +49 561 8109 101
Web: www.techconsult.de

techconsult TECHNOLOGY MARKET ANALYSTS | EIN UNTERNEHMEN DER heise group | IONOS