Datensouveräne Cybersicherheit für das KI-Zeitalter

Cybersicherheit modernisieren und gleichzeitig digitale Souveränität bewahren

Connecting your world.

paloalto NETWORKS

Inhaltsverzeichnis

1. Zusammenfassung

Europas digitale Landschaft befindet sich in einem tiefgreifenden Wandel. Unternehmen treiben die Einführung von Cloud-Technologien voran, integrieren Künstliche Intelligenz (KI) in ihre Geschäftsprozesse und agieren in zunehmend vernetzten digitalen Ökosystemen. Cybersicherheit ist dabei längst nicht mehr nur eine technische Aufgabe. Sie hat sich zu einem strategischen Erfolgsfaktor entwickelt – sowohl für die Resilienz von Unternehmen als auch für den Umgang mit geopolitischen Risiken.

Geopolitische Spannungen und staatlich unterstützte Cyberangriffe verändern die Bedrohungslandschaft grundlegend. Cyberangriffe richten sich zunehmend gegen kritische Infrastrukturen, Lieferketten und industrielle Ökosysteme. Gleichzeitig entstehen durch die wachsende Abhängigkeit von global betriebenen Technologieplattformen neue Risiken – insbesondere im Hinblick auf Rechtsräume, Kontrolle und Abhängigkeiten.

Auch regulatorische Entwicklungen – darunter die NIS2-Richtlinie, der Digital Operational Resilience Act (DORA), der Cyber Resilience Act (CRA) sowie der EU AI Act – treiben diesen Wandel voran. Diese Regelwerke gehen über reine Compliance-Anforderungen hinaus: Sie verpflichten Unternehmen, ein hohes Maß an Kontrolle, Transparenz und Resilienz über ihre gesamte digitale Wertschöpfung sowie innerhalb ihrer Drittanbieter- und Partnerökosysteme nachzuweisen.

Diese Entwicklungen machen die digitale Souveränität zu einer zentralen Priorität für Chief Information Security Officers (CISOs).

Digitale Souveränität geht jedoch weit über die reine Datenresidenz hinaus. Sie beschreibt die Fähigkeit einer Organisation, die Kontrolle, Transparenz und Resilienz über ihre Daten, Geschäftsprozesse, Technologieabhängigkeiten und rechtlichen Rahmenbedingungen zu wahren – insbesondere in cloudbasierten Umgebungen.

Daraus ergibt sich für CISOs eine zentrale Herausforderung: Wie lassen sich moderne Cyber Security Funktionen im Cloud-Maßstab nutzen und gleichzeitig die souveräne Kontrolle über kritische Systeme und Betriebsprozesse sicherstellen?

Dieses Whitepaper stellt Sovereign Security als praxistauglichen Ansatz zur Bewältigung dieser Herausforderung vor. Es zeigt auf, wie sich folgende Anforderungen miteinander verbinden lassen:

- geopolitische Risiken und ihre Auswirkungen auf die Bedrohungslandschaft,
- den zunehmenden regulatorischen Druck und die daraus resultierenden Anforderungen an Governance,
- die operativen Anforderungen einer modernen Cyberabwehr.

Es zeigt auf, wie sich digitale Souveränität von einem politischen und regulatorischen Leitbild zu einer operativen Fähigkeit weiterentwickeln muss – verankert in der Sicherheitsarchitektur, der Cloud-Strategie und den täglichen Abläufen der Cyberabwehr.

Letztlich geht es bei Sovereign Security nicht darum, Innovationen einzuschränken. Vielmehr befähigt dieser Ansatz Unternehmen, mit vertrauenswürdiger Kontrolle zu agieren, Abhängigkeitsrisiken zu reduzieren und auch unter geopolitischem Druck resilient und handlungsfähig zu bleiben..

Unternehmen, die digitale Souveränität konsequent in ihre Cyber Security Strategie integrieren, sind besser darauf vorbereitet, regulatorische Komplexität zu bewältigen, externe Abhängigkeiten gezielt zu steuern und auch in einem zunehmend unsicheren globalen Umfeld einen sicheren und resilienten Geschäftsbetrieb aufrechtzuerhalten.

2. Souveränität in einer sich wandelnden Cyberlandschaft

Europas digitale Wirtschaft ist zunehmend von Cloud-Infrastrukturen, vernetzten Ökosystemen, KI-gestützten Prozessen und digitalen Echtzeitdiensten abhängig. Diese Transformation hat Innovationen beschleunigt und die betriebliche Effizienz erheblich gesteigert. Gleichzeitig hat sie Europas Anfälligkeit gegenüber geopolitisch motivierten Cyberrisiken deutlich erhöht.

Cyberoperationen beschränken sich längst nicht mehr auf finanziell motivierte Angriffe. Sie werden zunehmend als Instrumente strategischer Einflussnahme, wirtschaftlichen Drucks und gezielter operativer Störungen eingesetzt.

Mehrere Trends treiben diesen Wandel voran:

- Kritische Sektoren wie Energie, Transport, Telekommunikation, Gesundheitswesen, Fertigung und Logistik sind aufgrund ihrer Bedeutung für nationale Widerstandsfähigkeit und wirtschaftliche Stabilität zu primären Cyber-Zielen geworden.
- Staatlich geförderte Bedrohungsakteure, die mit Russland, China, Norden verbunden sind Korea und Iran verfolgen weiterhin europäische Infrastruktur, Industriesysteme sowie geistiges Eigentum durch Spionage, Ransomware, Kompromittierung der Lieferkette und langfristiges Eigentum Persistenzkampagnen[1].
- Hybride Kriegsführungsstrategien verbinden zunehmend Cyberoperationen mit politischen, wirtschaftlichen und informationsbasierten Taktiken und verstärken so Störungen über den digitalen Bereich hinaus.

Gleichzeitig schafft Europas wachsende Abhängigkeit von global betriebenen Technologieökosystemen neue Risiken für die digitale Souveränität. Viele der führenden Cloud- und Cyber Security Plattformen werden außerhalb Europas entwickelt, betrieben oder kontrolliert[4].

Die Herausforderung geht jedoch weit über die Frage der Datenresidenz hinaus.

Organisationen müssen bewerten:

- wer die Infrastruktur betreibt und administriert
- wer Zugriff auf sensible Systeme und Daten hat
- wo Telemetrie- und Metadaten verarbeitet werden
- wie Verschlüsselungen verwaltet werden
- welchen Rechtsräumen die jeweiligen Dienste und Daten unterliegen

Dies ist insbesondere für Unternehmen in regulierten Branchen und Betreiber kritischer Infrastrukturen von entscheidender Bedeutung. In diesen Bereichen sind Betriebskontinuität, Data Governance und strategische Autonomie unmittelbar mit der Cyberresilienz verknüpft.

Mit den geopolitischen Veränderungen der globalen Technologielandschaft entwickelt sich Sovereign Security von einer reinen Compliance-Anforderung zu einer strategischen Priorität für Resilienz. Ziel ist es, externe Abhängigkeiten zu reduzieren und die vertrauenswürdige Kontrolle über kritische digitale Umgebungen nachhaltig zu stärken.

[1] CERT-EU: Threat Landscape Report 2025
[2] Eurostat 2026
[3] Eurostat 2025
[4] Fortune Business Insights 2026

Nach Angaben von Eurostat nutzten im Jahr 2025 rund 53 % der europäischen Unternehmen kostenpflichtige Cloud-Computing-Dienste. Gleichzeitig nimmt der Einsatz von Künstlicher Intelligenz (KI) in europäischen Unternehmen weiter zu. Dadurch wächst die Abhängigkeit von extern betriebenen Plattformen und cloudbasierten Verarbeitungsumgebungen weiter.

3. Von Compliance zur Kontrolle: Europas Cyberregulierung

Europas regulatorisches Umfeld befindet sich in einem tiefgreifenden Wandel. Cybersicherheit, operationelle Resilienz, Data Governance und digitale Verantwortung werden nicht länger als voneinander getrennte Compliance-Bereiche betrachtet. Stattdessen werden sie zunehmend aufeinander abgestimmt, um den Schutz kritischer Infrastrukturen zu stärken, systemische Risiken zu reduzieren und Europas digitale Souveränität nachhaltig zu festigen.

Ausweitung der EU-Regulierungsverpflichtungen

Eine wachsende Zahl europäischer Vorschriften beeinflusst inzwischen unmittelbar, wie Unternehmen ihre digitalen Umgebungen gestalten, betreiben und absichern. Für Unternehmen in regulierten Branchen schafft dieser Wandel eine neue operative Realität. Sicherheitsentscheidungen werden heute nicht mehr ausschließlich von technischen Anforderungen bestimmt. Ebenso maßgeblich sind Aspekte wie die Kontrolle über den anwendbaren

NIS2-Richtlinie

Die NIS2-Richtlinie erweitert die Cybersicherheitsanforderungen für wesentliche und wichtige Einrichtungen innerhalb der Europäischen Union. Sie führt strengere Vorgaben in den Bereichen Governance, Verantwortlichkeit der Unternehmensleitung, Meldung von Sicherheitsvorfällen, Management von Lieferkettenrisiken sowie operationelle Resilienz ein. Unternehmen müssen künftig eine deutlich höhere Transparenz über ihre Drittanbieter, Infrastrukturabhängigkeiten und ihre gesamte Cyberrisikolage nachweisen.

GDPR (General Data Protection Regulation)

Obwohl die Datenschutz-Grundverordnung (DSGVO) in erster Linie den Schutz personenbezogener Daten und die Wahrung der Privatsphäre regelt, prägt sie weiterhin maßgeblich den Umgang von Unternehmen mit Datenresidenz, Zugriffsrechten, grenzüberschreitenden Datenübermittlungen und Rechenschaftspflichten. Sie unterstreicht die Notwendigkeit, jederzeit eine klare Kontrolle darüber zu behalten, wer auf sensible Daten zugreifen darf und unter welchem Rechtsraum dieser Zugriff erfolgt.

EU AI Act

Der EU AI Act führt Governance-Anforderungen für die Entwicklung und den Einsatz von KI-Systemen ein – insbesondere für Anwendungen mit hohem Risiko. Mit der zunehmenden Integration von KI-Funktionen in Unternehmensumgebungen und Cloud-Plattformen müssen Unternehmen Transparenz, Verantwortlichkeit, ein wirksames Risikomanagement sowie eine robuste Data Governance sicherstellen.

DORA (Digital Operational Resilience Act)

DORA schafft eine Rahmen für die operationelle Resilienz im europäischen Finanzsektor. Im Mittelpunkt stehen das Management von IKT-Risiken, Resilienztests, das Management von Sicherheitsvorfällen, die Überwachung von Drittanbieterrisiken sowie die Sicherstellung der Betriebskontinuität. Ein besonderer Schwerpunkt liegt auf Konzentrationsrisiken, die sich aus der Abhängigkeit von externen Technologie- und Cloud-Dienstleistern ergeben. Finanzinstitute sind daher verpflichtet, eine stärkere Kontrolle über ihre Abhängigkeiten sicherzustellen.

CRA (Cyber Resilience Act)

Der Cyber Resilience Act (CRA) führt verbindliche Cybersicherheitsanforderungen für Produkte mit digitalen Komponenten über deren gesamten Lebenszyklus hinweg ein. Dazu gehören die sichere Entwicklung, das Management von Schwachstellen, die Bereitstellung von Sicherheitsupdates sowie die Verantwortung der Hersteller für die Sicherheit ihrer Produkte. Die Verordnung ist Teil einer umfassenderen europäischen Initiative, das grundlegende Sicherheitsniveau in vernetzten Ökosystemen und entlang digitaler Lieferketten nachhaltig zu erhöhen.

Regulatorische Komplexität auf nationaler Ebene

In addition to EU-wide legislation, individual countries continue to enforce national cybersecurity frameworks and sector-specific requirements. Organizations operating across multiple jurisdictions must account for expectations from national authorities and regulators.

Dadurch entsteht eine vielschichtige Compliance-Landschaft, in der Unternehmen sowohl harmonisierte EU-Vorgaben als auch nationale und sektorspezifische Anforderungen gleichzeitig erfüllen müssen.

4. Souveränität in Europas kritischer Infrastruktur

Gesundheitsökosysteme

Das Gesundheitswesen ist zunehmend durch Telemedizin-Plattformen, KI-gestützte Diagnostik, elektronische Patientenakten und vernetzte Versorgungsstrukturen geprägt. Gleichzeitig müssen Gesundheitseinrichtungen hochsensible Daten schützen und strenge regulatorische Vorgaben sowie hohe Anforderungen an Governance und Betriebssicherheit erfüllen. Sovereign Cloud Security unterstützt sie dabei, ihre IT-Infrastruktur zu modernisieren und gleichzeitig die operative Kontrolle sowie eine wirksame Steuerung von Zugriffsrechten sicherzustellen.

Die Initiative European Health Data Space (EHDS) unterstreicht die wachsende Bedeutung sicherer und vertrauenswürdiger Rahmenbedingungen für den Datenaustausch innerhalb des europäischen Gesundheitsökosystems[5].

Finanzdienstleistungen

Finanzinstitute stehen zunehmend unter Druck, ihre digitalen Services zu modernisieren und gleichzeitig ihre Resilienz zu stärken. Echtzeitzahlungen, digitales Banking, Open-Finance-Ökosysteme und KI-gestützte Prozesse erhöhen die Abhängigkeit von Cloud-Infrastrukturen und vernetzten digitalen Umgebungen.

Gleichzeitig erhöhen regulatorische Rahmenwerke wie der Digital Operational Resilience Act (DORA) die Anforderungen an die operationelle Resilienz und das Management von Drittanbieterrisiken erheblich.

Vor diesem Hintergrund werden operationelle Souveränität und externes Schlüsselmanagement zu strategischen Prioritäten für den Finanzsektor. Sie ermöglichen es Finanzinstituten, die Kontrolle über kritische Werte und Systeme zu stärken, Abhängigkeitsrisiken zu reduzieren und den steigenden regulatorischen sowie sicherheitsrelevanten Anforderungen gerecht zu werden.

Öffentlicher Sektor

Als Verantwortliche für den Schutz von Bürgerdaten, nationalen Infrastrukturen und essenziellen öffentlichen Dienstleistungen unterliegen öffentliche Einrichtungen in Europa besonders hohen Anforderungen an die digitale Souveränität. Entsprechend entwickelt sich Souveränität zunehmend von einer technischen Fragestellung zu einer zentralen Anforderung in Beschaffung, Governance und strategischer Steuerung.

Der ENISA Threat Landscape 2025 bestätigt diese Entwicklung und zählt die öffentliche Verwaltung weiterhin zu den am häufigsten von Cyberangriffen betroffenen Sektoren.6

[5] European Health Data Space Regulation
[6] ENISA Threat Landscape 2025

5. Souveränität als Grundlage für sichere Innovation

Europas Strategie zur digitalen Souveränität verfolgt nicht das Ziel, den Zugang zu globalen Technologieinnovationen einzuschränken. Große Unternehmen sind auch künftig auf leistungsfähige Cyber Security Plattformen, KI-Funktionen und Hyperscale-Cloud-Infrastrukturen angewiesen. Gleichzeitig setzt sich zunehmend die Erkenntnis durch, dass diese Technologien innerhalb von Governance-Modellen betrieben werden müssen, die den europäischen rechtlichen, operationellen und Resilienzanforderungen entsprechen.

Strategische Autonomie ohne Isolation

Europas Ansatz zur digitalen Souveränität zielt nicht darauf ab, Innovationen einzuschränken oder Technologieökosysteme voneinander abzuschotten. Vielmehr geht es darum, vertrauenswürdige digitale Umgebungen zu schaffen, in denen sich Cloud-Technologien, Künstliche Intelligenz (KI), Cybersicherheit und datengetriebene Innovationen auf der Grundlage klarer Governance-Strukturen und eindeutiger Verantwortlichkeiten sicher skalieren lassen. Da digitale Infrastrukturen zunehmend zur Grundlage wirtschaftlicher Stabilität, industrieller Wertschöpfung, öffentlicher Dienstleistungen und nationaler Resilienz werden, fördert Europa Rahmenwerke, die Kontrolle, Interoperabilität und Vertrauen innerhalb des digitalen Ökosystems stärken. Damit wird digitale Souveränität nicht nur zu einer Voraussetzung für Sicherheit, sondern auch zu einem strategischen Wegbereiter für Innovation.

Dies erhöht die Nachfrage nach Betriebsmodellen, die den Zugang zu führenden Technologien mit:
·Starke Kontrolle über Betriebsumgebungen
·Klare Zuständigkeitsverteilung
·Transparenz bei der Dienstleistungserbringung und Verwaltung
·Rechenschaftspflicht im Rahmen europäischer Regulierungsrahmen

Vor diesem Hintergrund entwickelt sich Sovereign Security zu einem zentralen Baustein der europäischen Digitalstrategie. Sie ermöglicht es Unternehmen, ihre Resilienz zu stärken, die Kontrolle über ihre digitalen Umgebungen zu bewahren und regulatorische Anforderungen zu erfüllen, ohne dabei Innovationen einzuschränken.

Digitale Ökosysteme in Europa gestalten

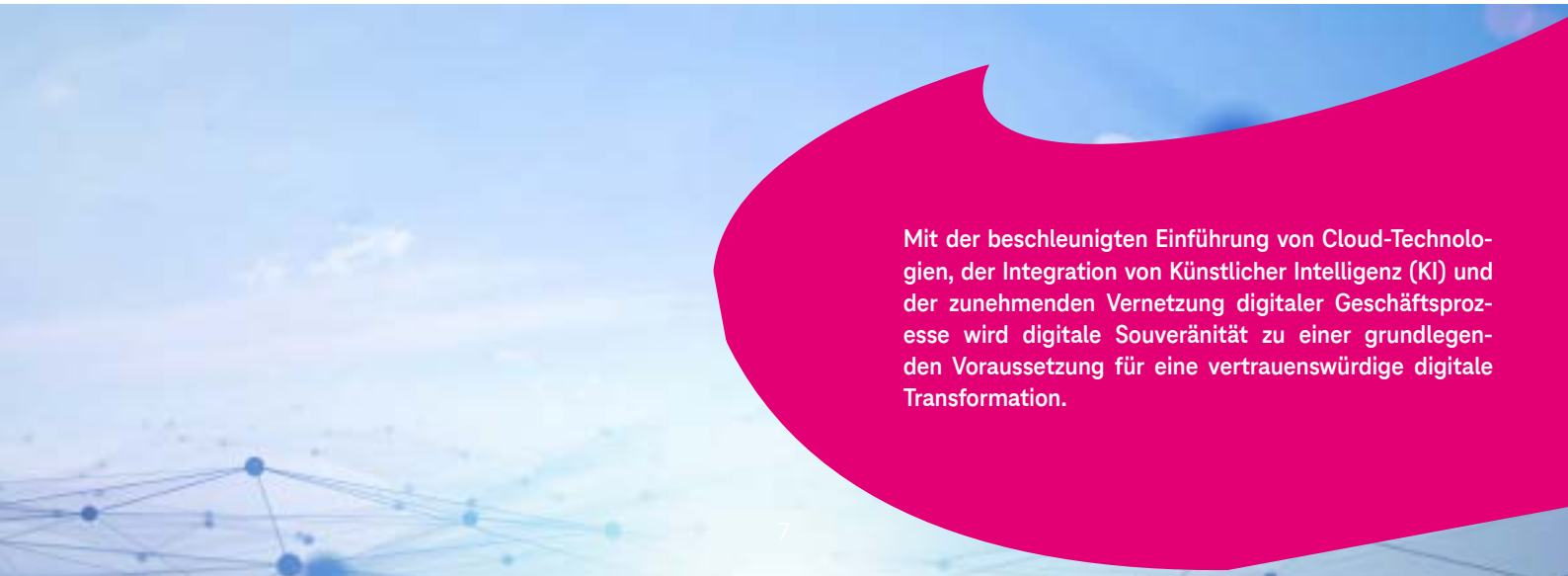
Souveränität kann nicht nur als Sicherheitsanforderung betrachtet werden, sondern auch als strategischer Ermöglicher von Innovation. Mehrere europäische Initiativen veranschaulichen diese Richtung:

- **EUCS** soll einen einheitlichen Sicherheitszertifizierungsrahmen für Cloud-Dienstleister schaffen, die ihre Services in Europa anbieten. Im Mittelpunkt stehen Sicherheitsnachweise, Transparenz und Governance. Die laufenden politischen Diskussionen verdeutlichen zudem, dass Kriterien der digitalen Souveränität bei der Weiterentwicklung des Zertifizierungsschemas eine zunehmend wichtige Rolle spielen.

- **European Data Spaces** fördern sektorspezifische Datenräume für Branchen wie das Gesundheitswesen, die Industrie, die Energiewirtschaft, den Mobilitätssektor und den Finanzsektor. Ziel ist es, eine sichere Zusammenarbeit zu ermöglichen und gleichzeitig die Kontrolle über Dateneigentum, Zugriffsrechte und Datennutzungsrichtlinien zu gewährleisten.

- **IPCEI-CIS** unterstützt den Aufbau europäischer Cloud- und Edge-Infrastrukturen. Die Initiative konzentriert sich auf Interoperabilität, Resilienz und die Verringerung strategischer Abhängigkeiten, um gleichzeitig skalierbare Innovationen zu ermöglichen.

- **Schrems III** – Die anhaltende Diskussion verdeutlicht die Weiterentwicklung der Regelungen für den internationalen Datentransfer und unterstreicht die wachsende Bedeutung souveräner Cloud- und Sicherheitsarchitekturen. Diese ermöglichen es Unternehmen, die Kontrolle über sensible Daten zu bewahren und regulatorische Anforderungen zuverlässig zu erfüllen.



Mit der beschleunigten Einführung von Cloud-Technologien, der Integration von Künstlicher Intelligenz (KI) und der zunehmenden Vernetzung digitaler Geschäftsprozesse wird digitale Souveränität zu einer grundlegenden Voraussetzung für eine vertrauenswürdige digitale Transformation.

6. Mehr als Datenresidenz: Die Säulen der digitalen Souveränität

Digitale Souveränität hat sich zu einer prägenden strategischen Leitlinie für Europas digitale Zukunft entwickelt. Dennoch wird sie von vielen Unternehmen noch immer in erster Linie mit der Datenresidenz gleichgesetzt. Tatsächlich reicht digitale Souveränität jedoch weit über den physischen Speicherort von Daten hinaus.

Digitale Souveränität in der Praxis

Digitale Souveränität beschreibt die Fähigkeit einer Organisation, die wirksame Kontrolle über ihre digitale Umgebung zu bewahren – einschließlich ihrer Infrastruktur, Daten, Geschäftsprozesse und kritischen Technologieabhängigkeiten[7].

Sie umfasst die operative Kontrolle, Transparenz in der Governance, den Umgang mit Infrastrukturabhängigkeiten, die Auswirkungen unterschiedlicher Rechtsräume, das Vertrauen in die Lieferkette sowie die Fähigkeit, auch unter sich verändernden geopolitischen Rahmenbedingungen resilient zu bleiben.

Vier Schlüsseldimensionen der digitalen Souveränität sind:

- Datensouveränität: Kontrolle über den Datenzugriff, die Nutzung und die Steuerung, einschließlich der Frage, wer auf Daten zugreifen kann und unter welcher Zuständigkeit.
- Operative Souveränität: Kontrolle über kritische Infrastruktur sowie operative Prozesse, die Kontinuität und Resilienz gewährleisten Selbst unter äußeren Störungen.
- Technologische Souveränität: Die Fähigkeit, Abhängigkeiten von Schlüsseltechnologien zu verwalten, um Flexibilität und Interoperabilität zu gewährleisten, und eine geringere Abhängigkeit von einzelnen Anbietern oder externen Ökosystemen.
- Rechtliche Souveränität: Die Fähigkeit, sicherzustellen, dass Systeme und Daten geregelt durch vorhersehbare Zuständigkeitsrahmen, die minimieren Aussetzung gegenüber widersprüchlichen oder extraterritorialen Rechtsansprüchen.

[7] Forbes 2026

Digitale Souveränität bedeutet nicht vollständige Unabhängigkeit. Moderne Unternehmen agieren in globalen Ökosystemen aus Cloud-Anbietern, Softwareherstellern und Servicepartnern. Ziel ist vielmehr, in diesen vernetzten Umgebungen ein hohes Maß an vertrauenswürdiger Kontrolle und Transparenz sicherzustellen.

In der Praxis erfordert dies Transparenz in:

- Wer die Umwelt betreibt und verwaltet
- Welche Jurisdiktionen die operative Kontrolle beeinflussen
- Wie privilegierter Zugang geregelt wird
- Wo Daten und Telemetrie verarbeitet werden
- Wie Verschlüsselung und Identität verwaltet werden
- Welche externen Abhängigkeiten für die Operationen entscheidend sind

Gleichgewicht zwischen Souveränität und Innovation

Digitale Souveränität wird häufig als Zielkonflikt zwischen Kontrolle und Innovation verstanden. In der Praxis können Unternehmen jedoch beides miteinander vereinbaren – durch Betriebsmodelle, die moderne Cyberabwehr mit wirksamer Governance, hoher Transparenz und klaren Verantwortlichkeiten verbinden.

Das erforderliche Maß an Souveränität hängt von Faktoren ab wie:

- Regulatorische Verpflichtungen
- Exposition kritischer Infrastruktur
- Risikoprofil und Bedrohungslandschaft
- Datensensitivität
- Abhängigkeiten von Drittanbietern

Das Ziel ist nicht, Innovation zu opfern, sondern um widerstandsfähige Umgebungen zu ermöglichen, in denen Innovation und Souveränität koexistieren.

6. Jenseits der Datenresidenz: Die Säulen der digitalen Souveränität

Datensouveränität: Zugang, Standort und Kontrolle

Datensouveränität wird häufig auf die Datenresidenz reduziert, doch beide Begriffe sind nicht gleichzusetzen. Während die Datenresidenz beschreibt, wo Daten gespeichert werden, definiert die Datensouveränität, wer auf diese Daten zugreifen kann, welchem Rechtsraum dieser Zugriff unterliegt und in welchem Umfang die Kontrolle darüber gewährleistet ist.

Diese Unterscheidung ist insbesondere in verteilten Cloud-Umgebungen von entscheidender Bedeutung. Denn selbst wenn Daten in Europa gespeichert werden, können administrativer Zugriff, Supportprozesse oder das Management von Verschlüsselungsschlüsseln weiterhin außerhalb Europas oder unter einer externen Rechtsordnung erfolgen.

Wichtige Überlegungen sind:

- Privilegierte Zugriffskontrolle
- Zuständigkeit für Zugriffsanfragen
- Rechtliche Kontakte gegenüber externen Behörden
- Standort der Telemetrie- und Metadatenverarbeitung
- Kontrolle über Verschlüsselung und Schlüsselverwaltung

Encryption as a Sovereignty Control

Verschlüsselung ist ein zentraler Baustein zur Stärkung der digitalen Souveränität. Modelle wie Customer-Managed Keys (CMK) oder External Key Management (EKM) ermöglichen es Unternehmen, die unabhängige Kontrolle über den Zugriff auf ihre Daten zu behalten. Insbesondere in regulierten Branchen ist ein wirksames Management von Verschlüsselungsschlüsseln nicht nur eine Sicherheitsanforderung, sondern auch eine wesentliche Voraussetzung für die Wahrung der digitalen Souveränität.

Datenklassifikation und Tiering

Nicht alle Daten erfordern das gleiche Maß an Kontrolle. Organisationen übernehmen Klassifikationsmodelle, die Souveränitätsanforderungen an folgende Anforderungen anpassen:

- Sensibilität und geschäftliche Kritikalität
- Regulatorische Exposition
- Operative Auswirkungen

Dies ermöglicht einen ausgewogenen Ansatz und erhält die Innovation aufrechterhalten und Skalierbarkeit, während bei Bedarf strengere Kontrollen angewendet werden

Datensouveränität: Die Fähigkeit, vollständige Kontrolle über die eigenen Daten auszuüben. Ohne sie verlieren Sie die Macht zu entscheiden, wer auf Ihre Daten zugreifen kann und wie sie verwendet werden können.

Operative Souveränität: Kontrolle & Resilienz

Mit der zunehmenden Vernetzung digitaler Geschäftsprozesse müssen Unternehmen nicht nur bewerten, welche Technologien sie einsetzen, sondern auch, wer diese betreibt und wo kritische Abhängigkeiten bestehen.

Moderne Security Operations stützen sich für Erkennung, Reaktion und Analysen häufig auf global verteilte Cloud-Ökosysteme. Diese Modelle ermöglichen zwar Skalierbarkeit und den Einsatz hochentwickelter Sicherheitsfunktionen, können jedoch zugleich Abhängigkeiten schaffen, die mit externen Rechtsräumen und Betriebsmodellen verbunden sind.

Diese Aspekte sollten bewertet werden:

- wer die Sicherheitsumgebungen betreibt
- wo Telemetrie- und Protokolldaten verarbeitet werden
- wer über operativen Zugriff verfügt
- wie die Zuständigkeiten und Entscheidungsbefugnisse im Incident Response definiert sind
- ob der Sicherheitsbetrieb auch unter veränderten Rahmen bedingungen aufrechterhalten werden kann

Betriebsmodelle für Sovereign Security Operations

Organisationen verwenden je nach Risiko unterschiedliche Modelle und Regulatorische Anforderungen:

- Interne SOCs für maximale Kontrolle und Sichtbarkeit
- Europäische MSSPs für regionale Governance und operative Ausrichtung
- Hyperskalierungsintegrierte Modelle für Skalierbarkeit, die erfordern Sorgfältiges Management von Abhängigkeit und Zuständigkeit Risiko

Operationelle Souveränität: Die Fähigkeit, kritische Infrastrukturen und Betriebsprozesse eigenständig zu steuern und aufrechtzuerhalten. Fehlt diese Fähigkeit, besteht das Risiko, die Kontrolle über geschäftskritische Prozesse zu verlieren und anfälliger für externe Störungen zu werden.

6. Jenseits der Datenresidenz: Die Säulen der digitalen Souveränität

Technologische Souveränität: Management von Abhängigkeitsrisiken

Unternehmensumgebungen sind zunehmend von einer kleinen Zahl globaler Technologieanbieter abhängig. Diese Plattformen bieten zwar hohe Skalierbarkeit und leistungsfähige Funktionen, können jedoch Konzentrationsrisiken erhöhen und die Flexibilität von Unternehmen einschränken.

Zu den wichtigsten Herausforderungen gehören:

- Vendor-Lock-in
- Begrenzte Interoperabilität
- Abhängigkeit von proprietären Ökosystemen
- Exposition gegenüber externer Governance

Multi-Cloud- und Hybridstrategien

Viele Organisationen setzen auf Multi-Cloud- und Hybridarchitekturen, um die Flexibilität zu erhöhen und Abhängigkeiten zu reduzieren.

Diese Ansätze unterstützen:

- Workload-Portabilität
- Verbesserte Interoperabilität
- Flexible Governance-Modelle
- Segmentierung basierend auf Risiko und Sensibilität
- Reduziertes Konzentrationsrisiko

Vollständige Unabhängigkeit ist in der Praxis nicht realistisch. Technologische Souveränität ist daher vor allem als Resilienzstrategie zu verstehen. Ihr Ziel besteht darin, unkontrollierte Abhängigkeiten zu reduzieren und gleichzeitig die Anpassungs- und Handlungsfähigkeit von Unternehmen zu stärken.

Technologische Souveränität: Die Fähigkeit, Schlüsseltechnologien eigenständig zu entwickeln, bereitzustellen und zu kontrollieren. Fehlt diese Fähigkeit, entsteht eine erhebliche Abhängigkeit von anderen Staaten oder Unternehmen bei kritischen Technologielösungen. Dadurch werden die eigene Handlungsfähigkeit und Wettbewerbsfähigkeit eingeschränkt.

Rechtssouveränität: Verständnis der Zuständigkeit Exposition

Rechtliche Souveränität beschreibt, welchen Rechtsräumen digitale Umgebungen unterliegen und wer rechtliche Hoheit über Systeme und Daten ausüben kann.

Dazu gehört insbesondere die Bewertung folgender Aspekte:

- Zuständigkeit und Eigentumsstruktur des Anbieters
- Exposition gegenüber extraterritorialer Gesetzgebung
- Rechtliche Mechanismen für Datenzugriffsanfragen
- Transparenz und Durchsetzbarkeit von Governance-Modellen

Der Speicherort der Daten allein reicht nicht aus

Die Speicherung von Daten in europäischen Rechenzentren beseitigt rechtliche Risiken nicht automatisch.

Risiken können dennoch entstehen aus:

- Ausländisches Eigentum an Dienstleistern
- Grenzüberschreitende Operationen und Unterstützungsmodelle
- Mechanismen der internationalen rechtlichen Zusammenarbeit
- Extraterritoriale rechtliche Verpflichtungen

Unternehmen müssen daher sowohl den Standort ihrer Infrastruktur als auch die rechtlichen Rahmenbedingungen bewerten, denen ihre Dienstanbieter unterliegen. Ziel ist es, Unsicherheiten zu reduzieren, klare Verantwortlichkeiten zu schaffen und den Betrieb an den europäischen rechtlichen und regulatorischen Anforderungen auszurichten.

Rechtliche Souveränität: Die Fähigkeit sicherzustellen, dass Daten, Systeme und Betriebsprozesse ausschließlich den von Ihnen festgelegten Rechtsordnungen und Gerichtsbarkeiten unterliegen.

7. Souveräner Cyberabwehr in der Praxis

Viele bestehende Ansätze zur digitalen Souveränität wurden für klassische IT-Umgebungen entwickelt. Ihr Schwerpunkt liegt auf Datenresidenz und lokal betriebenen Infrastrukturen – nicht auf einer modernen, KI-gestützten Cyberabwehr im Cloud-Maßstab. Dadurch entsteht in vielen Unternehmen der Eindruck, sie müssten sich zwischen fortschrittlichen Sicherheitsfunktionen und dem Erhalt der digitalen Souveränität entscheiden.

Die nächste Phase der souveränen Cyberabwehr

Unternehmen in ganz Europa stehen zunehmend unter Druck, ihre Cyberabwehr zu modernisieren und gleichzeitig operationelle Governance sowie Mechanismen zur Wahrung der digitalen Souveränität zu stärken. Dies gilt insbesondere für regulierte Branchen und Betreiber kritischer Infrastrukturen.

Gleichzeitig benötigen sie moderne Fähigkeiten zur Bedrohungserkennung, automatisierte Reaktionsmechanismen, die Analyse großer Telemetriemengen sowie Echtzeittransparenz. Zugleich müssen sie sicherstellen, dass ihre Sicherheitsprozesse den europäischen Governance- und Rechtsrahmen entsprechen und klare Verantwortlichkeiten gewährleisten.

Die nächste Entwicklungsstufe einer souveränen Cyberabwehr geht daher weit über den Standort der Infrastruktur hinaus. Erforderlich sind Betriebsmodelle, die durchsetzbare Souveränitätsmechanismen unmittelbar in die Security Operations integrieren – ohne Kompromisse bei Leistungsfähigkeit, Skalierbarkeit oder Resilienz einzugehen.

Souveränität wirksam in Security Operations verankern

Digitale Souveränität darf sich nicht allein auf Richtlinien, vertragliche Zusicherungen oder den Speicherort von Daten stützen. Sie muss technisch und operationell in den Umgebungen durchgesetzt werden, in denen Cyberabwehrmaßnahmen stattfinden.

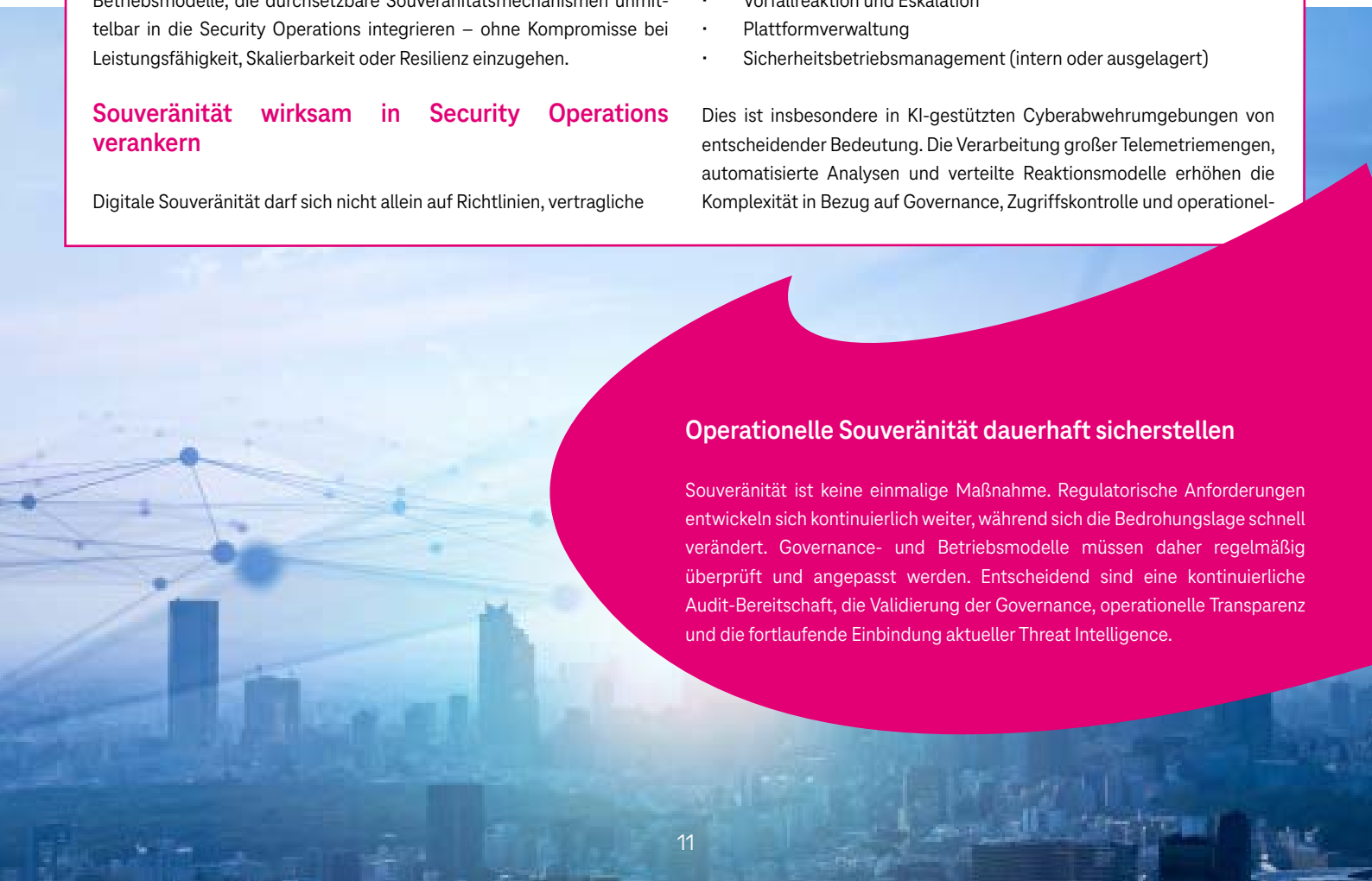
Zu den wichtigsten Funktionen gehören:

- Kontrollierter und prüfbarer Betriebszugang
- Transparente Governance- und Rechenschaftsrahmenwerke
- Klar definierte operative Verantwortlichkeiten
- Unabhängige oder kundengesteuerte Verschlüsselungsmodelle
- End-to-End-Auditability über Sicherheitsworkflows hinweg
- Operative Ausführung im Einklang mit vertrauenswürdigen Zuständigkeitsrahmenwerken

In der Praxis verlangen Organisationen zunehmend die Gewissheit, dass diese Kontrollen konsequent über tägliche Aktivitäten hinweg angewendet werden, darunter:

- Bedrohungsüberwachung und -erkennung
- Vorfallreaktion und Eskalation
- Plattformverwaltung
- Sicherheitsbetriebsmanagement (intern oder ausgelagert)

Dies ist insbesondere in KI-gestützten Cyberabwehrumgebungen von entscheidender Bedeutung. Die Verarbeitung großer Telemetriemengen, automatisierte Analysen und verteilte Reaktionsmodelle erhöhen die Komplexität in Bezug auf Governance, Zugriffskontrolle und operationel-



Operationelle Souveränität dauerhaft sicherstellen

Souveränität ist keine einmalige Maßnahme. Regulatorische Anforderungen entwickeln sich kontinuierlich weiter, während sich die Bedrohungslage schnell verändert. Governance- und Betriebsmodelle müssen daher regelmäßig überprüft und angepasst werden. Entscheidend sind eine kontinuierliche Audit-Bereitschaft, die Validierung der Governance, operationelle Transparenz und die fortlaufende Einbindung aktueller Threat Intelligence.

8. Sovereign Cortex with T Security

Unternehmen, die eine souveräne Cyberabwehr etablieren möchten, entscheiden sich nicht lediglich für einen Sicherheitsanbieter. Sie legen vielmehr fest, wie ihre Cyberabwehr in komplexen, regulierten Umgebungen gesteuert, betrieben und verantwortet wird. Genau hier setzt die Partnerschaft zwischen Palo Alto Networks und Deutsche Telekom an. Gemeinsam bieten sie ein Betriebsmodell für eine souveräne Cyberabwehr, das moderne Cybersecurity-Funktionen mit der erforderlichen Datensouveränität verbindet und deren Umsetzung innerhalb nachvollziehbarer, prüfbarer und wirksam durchsetzbarer Governance-Rahmen ermöglicht.

KI-gestützte Cyberabwehr mit vollem Leistungsumfang

Palo Alto Networks bietet KI-gestützte Cyberabwehr für Cloud-, Netzwerk-, Endpoint- und Security-Operations-Umgebungen. Dabei handelt es sich nicht um eine souveräne Variante mit eingeschränktem Funktionsumfang. Zum Einsatz kommt dieselbe Plattform, die von mehr als 70.000+ Kunden in über 150 Ländern genutzt wird, täglich 1,4 Milliarden Bedrohungsobjekte analysiert und von Gartner sowie Forrester in mehreren Sicherheitsbereichen als führend eingestuft wird. Die Bedrohungsinformationen von Unit 42 sowie die Security-Operations-Funktionen von Palo Alto Networks ermöglichen eine kontinuierliche Analyse der sich wandelnden Bedrohungslage. Gleichzeitig bringt die Deutsche Telekom ihre operative Souveränitätskompetenz sowie Managed Security Services in einem klar geregelten europäischen Betriebsmodell ein. Innerhalb dieses souveränen Betriebsmodells erhalten Unternehmen Zugriff auf den vollen Leistungsumfang moderner Cyberabwehr – eingebettet in klar definierte und wirksam umgesetzte Souveränitäts- und Governance-Mechanismen.

Operativ durchsetzbare Datensouveränität

Die Deutsche Telekom stellt die souveräne Betriebsebene bereit, die dieses Modell in der Praxis durchsetzbar macht. Dazu gehören der ausschließliche Zugriff durch operatives Personal innerhalb der EU, ein von der Deutschen Telekom kontrolliertes Management der Verschlüsselungsschlüssel, Audit-Protokollierung und operationelle Transparenz sowie die Verarbeitung und Speicherung der Daten am Standort Frankfurt. Die souveränen Betriebsleistungen werden durch die Deutsche Telekom erbracht. Dadurch wird Datensouveränität nicht nur vertraglich zugesichert, sondern operativ umgesetzt. Souveränität wird konsequent über Menschen, Prozesse und Technologien hinweg gewährleistet, sodass sich die operative Governance nicht allein auf Infrastrukturkontrollen beschränkt.

Entwickelt für eine wirksam gesteuerte Umsetzung – nicht nur für eine Governance-konforme Architektur:

- Operative Kontrollen, die Daten durchsetzen Souveränität in Ausführung
- EU-reines Einsatzpersonal.
- DT-gesteuerte Verschlüsselung.
- Audit-Logging und Transparenz.
- EU-basierte (Frankfurt-basierte) Verarbeitung.
- 24/7 verwaltete Sicherheitsoperationen

Steuerbare und nachvollziehbare KI-gestützte Security Operations

Mit der zunehmenden Integration von Künstlicher Intelligenz (KI) in die Cyberabwehr wird Governance zu einer strategischen Voraussetzung. Die Partnerschaft trägt diesem Anspruch unmittelbar Rechnung und stellt sicher, dass KI-gestützte Security Operations verantwortbar, nachvollziehbar und innerhalb souveräner Governance-Mechanismen betrieben werden. Damit besetzt sie eine strategische Position, die weder rein infrastrukturorientierte Anbieter von Souveränitätslösungen noch ausschließlich auf Cyberabwehr spezialisierte Technologieanbieter für sich allein glaubwürdig abdecken können.

Ein Betriebsmodell für eine souveräne Cyberabwehr

Dabei handelt es sich nicht um eine Technologieimplementierung, die nachträglich um Compliance-Kontrollen ergänzt wurde. Vielmehr ist es ein speziell entwickeltes Betriebsmodell, in dem Cyberabwehr, digitale Souveränität, KI-Governance und operationelle Verantwortlichkeiten von Beginn an integriert sind. Unternehmen erhalten damit nicht nur die erforderlichen Technologien, sondern ein umfassendes Betriebsmodell – einschließlich klar definierter operativer Kontrollmechanismen, Eskalationsprozesse, gemeinsamer Verantwortungsmodelle und eines 24×7 Managed Security Operations Service. Sie profitieren von einem einheitlichen, klar verantworteten Betriebsmodell, das Cyberabwehr, souveräne Governance, Managed Security Services und KI-gestützte Sicherheitsfunktionen zu einer ganzheitlichen Lösung verbindet.

Souveränität dort, wo sie zählt – über alle Umgebungen hinweg

Die Deutsche Telekom ermöglicht Unternehmen den Betrieb ihrer Cyberabwehr auf Basis eines konsistenten souveränen Betriebsmodells, das auf die regulatorischen Anforderungen in europäischen Umgebungen ausgerichtet ist. Dazu gehören die Kontrolle über die Datenresidenz, den operativen Zugriff sowie die Einhaltung regulatorischer Vorgaben. Dank ihrer souveränen Betriebskompetenz behalten Unternehmen jederzeit die Kontrolle darüber, wo Daten verarbeitet werden, wer darauf zugreifen kann und wie die Betriebsprozesse gesteuert werden. So wird digitale Souveränität über verschiedene Rechtsräume hinweg wirksam umgesetzt – ohne standardmäßig auf ein Höchstmaß an Kontrolle und die damit verbundenen maximalen Kosten angewiesen zu sein.

9. Zukunftsausblick

In einer sich schnell wandelnden globalen Landschaft werden diejenigen Unternehmen am erfolgreichsten sein, die moderne Cybersecurity-Funktionen mit einer vertrauenswürdigen Kontrolle über ihre digitalen Umgebungen verbinden. So schaffen sie die Voraussetzungen, sicher, regulatorisch konform und resilient zu agieren. Unternehmen sollten digitale Souveränität als grundlegendes Gestaltungsprinzip verstehen – nicht als nachträgliche Ergänzung. Entscheidend ist, den Schwerpunkt auf die operative Umsetzung von Souveränität statt auf deren bloße Definition in Richtlinien zu legen und Innovation sowie digitale Souveränität durch Governance-Modelle in Einklang zu bringen, die gleichermaßen Leistungsfähigkeit und Kontrolle gewährleisten.

Über Palo Alto Networks

Palo Alto Networks (NASDAQ: PANW), der globale Marktführer im Bereich KI-Cybersicherheit, schützt unsere digitale Lebensweise mit einem umfassenden Portfolio von Cybersicherheitslösungen und -plattformen in den Bereichen Netzwerk, Cloud, Sicherheitsoperationen, KI und Identität. Von 70.000+ Kunden vertraut und von Unit 42 Threat Intelligence angetrieben.
www.paloaltonetworks.com

Über Deutsche Telekom

Deutsche Telekom ist Europas führendes digitales Telekommunikationsunternehmen und betreut rund 220 Millionen Kunden in den Bereichen Mobilfunk, Festnetz und IT-Dienstleistungen. Über ihre Tochter-gesellschaften Deutsche Deutsche Telekom Security und T-Systems, die Gruppe, ist außerdem einer der größten Anbieter Europas von Cybersicherheit und verwalteten Sicherheitsdiensten. Mit Sicher-heitsoperationszentren in ganz Europa, ein durchgängiges europäisches Netzwerk und eine IT-Infra-struktur sowie jahrzehntelange Erfahrung im Service regulierte Branchen und öffentliche Kunden liefert Deutsche Telekom die europäischen Vertrauensanker für souveräne digitale Dienstleistungen.
www.telekom.com/companyprofil

Kontaktieren Sie uns noch heute!

Herausgeber:
Deutsche Telekom AG
Friedrich-Ebert-Allee 140
53113 Bonn
www.telekom.de

Connecting your world.

paloalto NETWORKS