T Security

360° Security

We secure your success

Connecting your world.

360° Security

We secure your success

Version 2.0 | Oktober 2026

T Security

We secure your success

Unsere strategischen Partner

CISCO · FORTINET · paloalto NETWORKS · Microsoft · CROWDSTRIKE · zscaler

Die Cybersicherheitslage bleibt hochdynamisch und herausfordernd. Geopolitische Spannungen und zunehmend professionelle Angreiferstrukturen verschärfen die Bedrohungslage. Und auch künstliche Intelligenz hält die Welt der Cybersicherheit weiter auf Trab – im Guten wie im Schlechten. KI ermöglicht eine extrem effektive Erkennung von Schwachstellen, weshalb mehr Sicherheitslücken denn je geschlossen werden. Darüber hinaus können auch Angriffsversuche schneller erkannt werden. Gleichzeitig nutzt jedoch auch die Gegenseite KI-Tools, um Einfallstore zu finden und Angriffe zu automatisieren, wodurch auch Cyberkriminelle immer effizienter agieren.

Um dieser Entwicklung wirksam zu begegnen, braucht es Erfahrung, Technologie und verlässliche Strukturen: Mit über 2.600 Mitarbeitenden im Bereich Cybersicherheit setzen wir uns jeden Tag rund um die Uhr für eine sichere, digitale Welt ein. Wir begleiten den gesamten Sicherheitszyklus – von der Erkennung und Bewertung über die Abwehr bis hin zur schnellen Wiederherstellung im Ernstfall. Unsere Kund*innen profitieren dabei von unserer tiefgehenden Branchenexpertise, von integrierten Sicherheitslösungen und praxiserprobten Konzepten, die sich flexibel an individuelle Anforderungen anpassen lassen und ganzheitliche Sicherheit gewährleisten.

Zahlen, Daten, Fakten

> 2.600 Mitarbeitenden

> 25 Jahre Erfahrung

15 Security Operations Center (SOC)

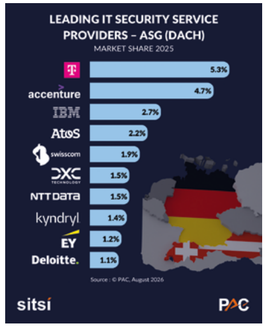
400 Millionen gemanagte Identitäten und Zertifikate

Sicherheit liegt in unserer DNA

Eine unserer besten Referenzen sind wir selbst: Wir bieten unseren Kund*innen die gleichen hochprofessionellen Technologien und Dienstleistungen an, mit denen wir weltweit auch die Deutsche Telekom schützen. Neben vielen Partnerlösungen entwickeln wir, aufbauend auf unserer umfangreichen Erfahrung, auch eigene innovative Sicherheitslösungen. Dazu zählen unter anderem Machine Learning, KI-Tools, Vulnerability Scanning, Identitätsmanagement sowie intelligente Systeme zur Angriffserkennung und -überwachung.

Dabei unterstützen wir:

- **Cyber Defense**
  IT- und OT-Systeme absichern
- **Infrastruktursicherheit**
  Das Unternehmensnetzwerk vor unberechtigten Zugriffen schützen
- **Sichere Identitäten**
  Digitale Identitäten und Zugriffe sicher managen
- **Compliance**
  Regularien und Vorgaben wie NIS-2, KRITIS oder EU AI Act umsetzen
- **Sicherer Einsatz von KI**
  Datenabfluss und Manipulation verhindern



"Deutsche Telekom (T Security) stands out in Europe's managed security services market by combining large-scale SOC operations, deep telecom infrastructure, and strong cyber defense expertise. Its portfolio gives customers a practical path to stronger resilience, faster response, and more mature security operations."

Claudio Stahnke
Senior Industry Analyst bei Frost & Sullivan

Als europäischer Anbieter stehen wir für europäische Werte ein. Digitale Souveränität und Datenschutz sind für uns keine lästige Pflicht, sondern wichtige Anliegen, die wir voll und ganz unterstützen. Herzstück unserer Cyber Defense Services ist unser Security Operations Center (SOC). Hier werden alle sicherheitsrelevanten Informationen gebündelt und ausgewertet. Ein internationales Team sorgt rund um die Uhr für Transparenz über die aktuelle Bedrohungslage. So lassen sich Angriffe frühzeitig erkennen, gezielt abwehren und fundiert analysieren.

Wie können wir Sie unterstützen? Egal, ob es um den Schutz Ihrer Infrastruktur, Ihrer KI-Anwendungen oder digitaler Identitäten geht: Wir sind Ihr starker und erfahrener Partner für Cyber Security.

Gemeinsam arbeiten wir für eine sichere digitale Welt. Jeden Tag, rund um die Uhr. Für den Mittelstand genauso wie für Konzerne.

Thomas Tschersich
Chief Security Officer (CSO)
Deutsche Telekom AG

360° Security
Sicherheit ohne Kompromisse

Wir arbeiten rund um die Uhr dafür, dass Digitalisierung sicherer wird. Mit dem größten Security Operations Center (SOC) Europas sorgen wir nicht nur für die Sicherheit unserer eigenen kritischen Infrastruktur, sondern bieten unsere Expertise auch anderen Unternehmen an. Dabei ist uns wichtig, die gesamte Sicherheits-Journey im Blick zu behalten. Machen wir uns auf den Weg!

Security ist ein permanenter Verbesserungsprozess. Mit unserem ganzheitlichen Security-Programm sind Sie rundum bestens aufgestellt. An welcher Stelle möchten Sie einsteigen?

Risiken identifizieren und bewerten
Was müssen Sie schützen und aus welchen Gründen? Kennen Sie Ihr Risiko? Egal, wo Sie gerade stehen – wir unterstützen Sie dabei, Sicherheit ganzheitlich und strategisch anzugehen. Mit Fast-Checks und umfassender Beratung, Risiko-Assessments, Security-Audits, Pentesting und Red Teaming helfen wir Ihnen bei der fundierten Risikobewertung.

Assets schützen
Wie schützen Sie Ihre Infrastruktur, Endpoints und Identitäten? Aufbauend auf der Risikobewertung lassen sich Schutzstrategie und Sicherheitsarchitektur passgenau definieren und umsetzen. Unser umfassendes Portfolio bietet Ihnen eine große Auswahl an Sicherheitslösungen und Schutzmaßnahmen.

Angriffe erkennen
Wann erkennen Sie einen Angriff? Mit den Services aus unserem Security Operations Center (SOC) können Sie sich entspannen: Wir haben die Lage 24/7 im Blick. Angriffe werden mit Unterstützung durch KI und Automatisierung nach durchschnittlich 15 Minuten erkannt.

Auf Angriffe reagieren
Was passiert im Ernstfall? Wir übernehmen, wenn es ernst wird, denn eine schnelle Reaktion ermöglicht es, Schäden zu minimieren. Angriffe werden sofort gestoppt und eingedämmt. Unsere eingespielten und top-qualifizierten Teams stehen rund um die Uhr bereit und leisten professionelles Krisenmanagement.

Wiederherstellen
Wie geht es nach dem Ernstfall weiter? Mit Wiederherstellungsmaßnahmen und professioneller Forensik tragen wir dazu bei, dass Sie schnell wieder zum Normalbetrieb übergehen können. Wichtig ist, aus dem Vorfall zu lernen, um gestärkt daraus hervorzugehen.

„Die großen Erfahrungen und Kompetenzen in anspruchsvollen Umgebungen tragen zum Erfolg und zur führenden Position der Deutschen Telekom im deutschen Markt für Cybersecurity-Beratung bei. Dank eines großen, hoch qualifizierten Teams und End-to-End-Services ‚Made in Germany' ist die Deutsche Telekom mit ihrer Tochter Deutsche Telekom Security ein führender Anbieter von Technical Security Services in Deutschland.

Mit ihren umfassenden, innovativen Next-Gen SOC/MDR Services ‚Made in Germany' und ihrem großen, qualifizierten Team überzeugt die Deutsche Telekom als ein führender Anbieter in Deutschland. Mit ‚Security made in Germany' und einem innovativen Angebot, das von hoch qualifizierten Mitarbeitern bereitgestellt wird, positioniert sich die Deutsche Telekom als führender Anbieter von SOC-/MDR-Dienstleistungen für den deutschen Mittelstand."

Frank Heuer
Principal Analyst bei ISG

Vorteile auf einen Blick

- **Netzkompetenz in der DNA:**
  Durch unser eigenes Netzwerk erkennen wir verdächtige Aktivitäten oft schon auf Netzebene, bevor Kundensysteme betroffen sind. Dadurch wird Geschwindigkeit gewonnen.
- **KI-gestütztes SOC:**
  KI-gestützt werden 6 Millionen Angriffe täglich analysiert. Durch maschinelles Lernen erkennt das SOC ungewöhnliche Muster, um eine beschleunigte Incident Response einzuleiten.
- **Compliance ohne Kopfschmerzen:**
  Durch die kontinuierliche und schnelle Reaktion auf Cybervorfälle werden auch zentrale technische Anforderungen der NIS-2-Richtlinie erfüllt.

Ein Tag im SOC

2,5 Mrd. sicherheitsrelevante Events aus 3.300 Datenquellen

100 Mio. E-Mails und Spam untersucht

> 6 Mrd. auf Cyberangriffe überprüfte Datensätze unseres DNS-Servers

KI sicher einsetzen

Wir unterstützen Unternehmen dabei, ihre eigenen KI-Projekte von Anfang an sicher und verantwortungsvoll zu gestalten – von der Prozessdefinition bis hin zur Umsetzung eines datengetriebenen Geschäftsmodells innerhalb klarer ethischer Leitplanken. Ob Sprachassistenten, Suchalgorithmen oder die Steuerung industrieller Anlagen: Wir sorgen dafür, dass Innovation und Sicherheit Hand in Hand gehen.

Kennen Sie Ihr Risiko?
Risiken identifizieren und bewerten

Herausforderung – Warum ist dieses Thema heute relevant?

Historisch gewachsene IT-Landschaften, hybride Cloud-Umgebungen und die bereits im Einsatz befindlichen unterschiedlichen Sicherheitswerkzeuge führen dazu, dass Unternehmen zwar viele Daten und Strukturen besitzen, jedoch selten ein konsolidiertes Sicherheits-Lagebild. Management und IT benötigen Transparenz über den tatsächlichen Reifegrad der Informationssicherheit sowie eine belastbare Bewertung technischer und organisatorischer Risiken.

Typische Fragestellungen in dieser Phase sind:

- Governance & Compliance: Welche regulatorischen oder kundenseitigen Anforderungen an IT-Sicherheit sind bekannt und evaluiert?
- Business Continuity Management: Sind alle Risiken bezüglich des Wertschöpfungsprozesses und der allgemeinen Geschäftsprozesse identifiziert und bewertet?
- Informations-Sicherheits-Management: Welche technischen und organisatorischen Maßnahmen zur Risikoreduzierung wurden identifiziert, priorisiert und umgesetzt?
- Asset-Management: Sind alle Komponenten bekannt und wurden diese nach ihren Risiken klassifiziert?
- Penetrationstests: Wie oft und in welcher Tiefe wurden die Tests durchgeführt und welche Maßnahmen wurden daraus abgeleitet?

Unser Ansatz – Wie gehen wir das Problem an?

Security darf nicht ausschließlich als technische Aufgabe verstanden werden. Ein wirksames Sicherheitsniveau entsteht erst dann, wenn Menschen, Prozesse, Organisation und Technologie aufeinander abgestimmt sind und gemeinsam betrachtet werden. Ziel eines ganzheitlichen Ansatzes ist es daher, nicht nur technische Schwachstellen zu identifizieren, sondern die Sicherheitsfähigkeit des Unternehmens in ihrer Gesamtheit zu bewerten.

Auf der Ebene der Menschen wird analysiert, wie ausgeprägt das Sicherheitsbewusstsein der Mitarbeitenden ist, ob Verantwortlichkeiten verstanden werden und wie sicherheitsrelevante Vorgaben im Arbeitsalltag tatsächlich umgesetzt werden. Dabei stehen unter anderem Awareness, Rollenverständnis, Kommunikationswege, der Umgang mit verdächtigen Situationen sowie die Reaktionsfähigkeit bei Sicherheitsvorfällen im Mittelpunkt.

Die Prozessanalyse untersucht, ob sicherheitsrelevante Abläufe klar definiert, dokumentiert und wirksam umgesetzt sind. Dazu gehören beispielsweise Berechtigungsvergaben, Eintritts- und Austrittsprozesse, das Schwachstellen- und Patchmanagement, der Umgang mit Dienstleistern, die Reaktion auf Sicherheitsvorfälle sowie Notfall- und Wiederanlaufverfahren. Neben der formalen Ausgestaltung wird insbesondere geprüft, ob die Prozesse im Alltag gelebt, kontrolliert und regelmäßig verbessert werden.

Auf organisatorischer Ebene werden Governance, Zuständigkeiten und Entscheidungswege betrachtet. Analysiert wird, ob Sicherheitsrollen eindeutig vergeben sind, ausreichende Ressourcen zur Verfügung stehen und Security angemessen in Management-, Risiko- und Geschäftsprozesse eingebunden ist. Ebenso wird bewertet, ob Risiken transparent berichtet, Maßnahmen konsequent nachverfolgt und Sicherheitsanforderungen über Unternehmensbereiche hinweg einheitlich gesteuert werden.

Die technische Ebene wird durch gezielte Penetrationstests abgedeckt. Diese ergänzen das Assessment um die Validierung der bisher umgesetzten Maßnahmen und Identifikation potenziell neuer Schwachstellen. Durch die Kombination manueller Prüfungen erfahrener Security-Fachleute mit unterstützenden Werkzeugen und KI-basierten Funktionen wird sichtbar, welche Schwachstellen tatsächlich ausnutzbar sind, welche Angriffswege realistisch erscheinen und welche geschäftlichen Auswirkungen daraus entstehen können.

So entsteht ein belastbares IT-Sicherheitslagebild, das technische Feststellungen mit menschlichen, prozessualen und organisatorischen Ursachen verknüpft. Auf dieser Grundlage lassen sich Sicherheitsmaßnahmen risikoorientiert priorisieren und gezielt in ein wirksames Gesamtsystem überführen.

Ihr Mehrwert – Welchen konkreten Nutzen haben Sie?

Transparenz schafft Sicherheit. Erst ein belastbares Lagebild ermöglicht es, Risiken und Schwachstellen nach ihrem tatsächlichen Einfluss auf das Unternehmen zu priorisieren und Maßnahmen zielgerichtet abzuleiten. Durch die kontinuierliche Überwachung und Bewertung identifizierter Schwachstellen entsteht ein fortlaufender Verbesserungsprozess, der die Sicherheitslage nachhaltig stärkt und die Cyberresilienz kontinuierlich erhöht.

Add-on Feature: Managed Exposure Service

Kontinuierlich Schwachstellen und Fehlkonfigurationen erkennen und nachhaltig beheben. Ein Managed Exposure Service bietet einen Service zur automatisierten Behebung von Schwachstellen, Fehlkonfigurationen und Compliance-Verstößen.

Vorteile auf einen Blick

- **Transparenz über die Sicherheitslage**
  Ganzheitliche Sicht auf den aktuellen Sicherheitsstatus über Organisation, Prozesse und Technologie hinweg.
- **Fundierte Risikobewertung**
  Identifikation und Bewertung technischer sowie organisatorischer Risiken unter Berücksichtigung ihrer Auswirkungen auf Geschäftsprozesse.
- **Priorisierung der Maßnahmen**
  Risiken und Schwachstellen werden nach Business-Relevanz priorisiert, sodass Ressourcen gezielt dort eingesetzt werden, wo sie den größten Sicherheitsgewinn erzielen.
- **Validierung durch Penetrationstests**
  Manuelle und werkzeuggestützte Penetrationstests zeigen, welche Schwachstellen tatsächlich ausnutzbar sind und welche realen Angriffswege bestehen.
- **Management-gerechte Entscheidungsgrundlage**
  Executive Reports mit klaren Handlungsempfehlungen schaffen Transparenz und unterstützen Investitions- und Management-Entscheidungen.
- **Nachhaltige Verbesserung der Sicherheitslage**
  Kontinuierliche Überprüfung, Neubewertung und Nachverfolgung identifizierter Risiken schaffen einen messbaren Verbesserungsprozess und stärken die Cyberresilienz.

Souveräne Sicherheit mit Plan
Aus Erkenntnissen werden Entscheidungen

Herausforderung – Warum ist dieses Thema heute relevant?

Ein nachhaltiges Sicherheitsniveau entsteht erst dann, wenn technische Erkenntnisse, regulatorische Anforderungen und Business-Ziele in einer gemeinsamen Roadmap zusammengeführt werden. Dafür braucht es eine zentrale Governance und eine verantwortliche Rolle, die Maßnahmen priorisiert, Entscheidungen vorbereitet und die kontinuierliche Umsetzung sicherstellt.

Gerade im Kontext regulatorischer Anforderungen wie NIS-2 und DORA sowie der Anforderungen an KRITIS-Betreiber und beim Aufbau von Informationssicherheitsmanagementsystemen (ISMS) nach ISO 27001 oder BSI IT-Grundschutz reichen punktuelle Sicherheitsmaßnahmen nicht aus. Informationssicherheit muss systematisch gesteuert, nachvollziehbar dokumentiert und kontinuierlich verbessert werden.

Unser Ansatz – Wie gehen wir das Problem an?

Auf Basis der Assessment-Ergebnisse wird eine individuelle Security-Roadmap entwickelt. Diese umfasst den Aufbau oder die Weiterentwicklung eines Informationssicherheitsmanagementsystems (ISMS) auf Basis von ISO 27001 oder BSI IT-Grundschutz, die Vorbereitung auf NIS-2- oder KRITIS-Anforderungen sowie Business Continuity Management und Security Governance. Die Maßnahmen werden priorisiert und in einer realistischen Umsetzungsplanung zusammengeführt.

Eine zentrale Rolle übernimmt der Informationssicherheitsbeauftragte (ISB). Er ist der organisatorische Treiber, der Sicherheitsziele operationalisiert, Maßnahmen koordiniert, Verantwortlichkeiten klärt und die kontinuierliche Verbesserung des ISMS im Alltag verankert. Ohne eine solche Rolle bleiben Roadmaps häufig Projektpläne – mit ISB werden sie zu gelebter Sicherheitssteuerung.

Ergänzend wird der Zero-Trust-Ansatz als strategisches Leitprinzip berücksichtigt: Never trust, always verify. Identitäten, Geräte, Anwendungen und Zugriffe werden kontinuierlich geprüft. Berechtigungen folgen dem Least-Privilege-Prinzip. So wird die Angriffsfläche reduziert und die Roadmap mit einer modernen Zielarchitektur verbunden.

Ihr Mehrwert – Welchen konkreten Nutzen haben Sie?

Unternehmen erhalten nicht nur einen Maßnahmenkatalog, sondern einen strukturierten Weg zu mehr Cyberresilienz. Compliance-Anforderungen werden nachweisbar erfüllt, Investitionen zielgerichtet eingesetzt und Sicherheitsmaßnahmen kontinuierlich weiterentwickelt.

- **Roadmap**
  Priorisierte Maßnahmen aus Assessment, Compliance und Business-Anforderungen.
  Realistische Umsetzung statt isolierter Einzelmaßnahmen.
- **ISB**
  Zentraler Treiber für Koordination, Verantwortlichkeiten, Umsetzung und Management-Kommunikation.
  Security wird organisatorisch verankert und strategisch vorangetrieben.
- **ISMS**
  Managementsystem für Informationssicherheit, Risiken, Maßnahmen und kontinuierliche Verbesserung.
  Nachvollziehbare Steuerung, Entwicklung und Optimierung der Informationssicherheit.
- **Zero Trust**
  Strategisches Leitprinzip für Identitäten, Zugriffe, Geräte und Anwendungen.
  Reduzierte Angriffsfläche und moderne Zielarchitektur.

Vom Risiko zur Resilienz

Die ersten beiden Phasen der 360°-Security-Journey bilden das Fundament für alle weiteren Security-Services. Security Assessments schaffen Transparenz. Penetration Tests und technische Analysen validieren bestehende Konfigurationen und identifizieren potentielle Schwachstellen. Managed Exposure Services sorgen dafür, dass Findings kontinuierlich überwacht, priorisiert und nachhaltig behoben werden. ISMS, ISB, Governance, Compliance und Zero Trust schaffen daraus einen langfristigen organisatorischen und architekturellen Rahmen.

Erst diese Kombination ermöglicht es Unternehmen, Sicherheitsmaßnahmen strategisch statt reaktiv zu steuern: Risiken erkennen, priorisieren, beheben, steuern und kontinuierlich verbessern.

Vorteile auf einen Blick

- Management-gerechte Transparenz über den aktuellen Sicherheitsstatus
- Priorisierung der größten Risiken und Quick Wins
- Validierung technischer Risiken durch Penetration Tests und Assessments
- Kontinuierliche Behebung von Schwachstellen und Fehlkonfigurationen mit Managed Exposure Services
- Verbindung technischer Erkenntnisse mit Business- und Compliance-Anforderungen
- Roadmap zum Aufbau des ISMS (ISO 27001 / BSI IT-Grundschutz) NIS-2, KRITIS und BCM
- Klare Rolle des ISB als Treiber der Informationssicherheit
- Zero Trust als strategischer Zielrahmen für moderne Sicherheitsarchitekturen
- Nachhaltige Erhöhung der Cyberresilienz

Ihr Netz. Ihr Schutzschild.
Sicherheit beginnt im Netzwerk

Wenn Netzwerke ausfallen, steht nicht nur die IT still – ganze Geschäftsprozesse kommen zum Erliegen und Geschäftsmodelle geraten ins Risiko. 2026 markiert einen Wendepunkt: Netzwerke sind nicht länger reine Transportinfrastruktur, sondern die entscheidende Ebene für Resilienz, Souveränität und Steuerbarkeit. Regulatorische Anforderungen wie NIS-2, geopolitische Spannungen und datenintensive Technologien wie KI erhöhen den Druck auf Unternehmensarchitekturen spürbar. Gleichzeitig verlieren klassische Sicherheitsmodelle an Wirksamkeit: Perimeter lösen sich auf, IT wird verteilter, Abhängigkeiten werden komplexer. Sicherheit kann nicht mehr nachgelagert gedacht werden – sie muss integraler Bestandteil der Netzwerkarchitektur sein. Secure Networking steht für diesen Paradigmenwechsel: Netzwerke werden zur aktiven Sicherheitsarchitektur. Sie schaffen Transparenz, steuern Zugriffe und ermöglichen Kontrolle über verteilte IT-Landschaften hinweg. Wer diese Ebene beherrscht, sichert nicht nur Systeme, sondern die eigene digitale Handlungsfähigkeit.

Digitale Geschäftsprozesse – von Produktion und Logistik bis zu Filialbetrieb, Cloud-Nutzung und hybrider Zusammenarbeit – sind heute stärker denn je auf eine sichere, performante und steuerbare Vernetzung angewiesen. Fällt diese Basis aus, sind nicht nur IT-Systeme, sondern ganze Wertschöpfungsprozesse gefährdet.

Moderne IT-Landschaften sind geprägt von Multi-Cloud, verteilten Standorten, Partnerökosystemen und datenintensiven Anwendungen. Die Folge: steigende Komplexität, wachsende Abhängigkeiten und eine zunehmend dynamische Infrastruktur. Daraus entsteht ein struktureller Zielkonflikt: Mehr Verschlüsselung erhöht die Sicherheit, reduziert jedoch die klassische Sichtbarkeit im Netzwerk. KI- und Echtzeitanwendungen treiben zugleich die Anforderungen an Performance und Latenz deutlich nach oben.

Regulatorische Vorgaben wie NIS-2 erhöhen den Druck zusätzlich. Gefordert sind durchgängige Governance, belastbares Risikomanagement und vollständige Transparenz über alle Systeme hinweg – unabhängig von Standort oder Plattform. Hinzu kommen geopolitische Einflüsse: Fragmentierte Infrastrukturen, unterschiedliche Rechtsräume und steigende Abhängigkeiten von Providern erschweren eine konsistente Steuerung über Ländergrenzen hinweg.

Die zentrale Frage für CIOs lautet daher: Wie lassen sich Sicherheit, Performance, Compliance und Steuerung in einer global verteilten IT-Architektur wirksam miteinander in Einklang bringen?

Netzwerk weiterdenken

Über **200 Mrd. €**
Schaden durch Cyberangriffe

Cyberangriffe nehmen zu, der Anteil am Gesamtschaden steigt auf **70 %**

Quelle: www.bitkom.org/sites/main/files/2025-12/bitkom-studienbericht-wirtschaftsschutz-2025.pdf

Sicherheit, Performance, Compliance und Steuerbarkeit vereint

Secure Networking transformiert Netzwerke von passiven Infrastrukturen zu aktiven Steuerungsplattformen. Sicherheit, Performance und Governance werden direkt in der Architektur verankert und Komplexität wird damit beherrschbar. Für das Business bedeutet das: mehr Steuerbarkeit, reduzierte Risiken sowie sinkende Betriebs- und Auditkosten.

Ein zentraler Ansatz ist **Zero Trust**: Vertrauen entsteht nicht mehr durch Netzwerkgrenzen, sondern durch Identität, Kontext und Risiko. Jeder Zugriff wird kontinuierlich überprüft – unabhängig vom Standort. Das reduziert Angriffsflächen und ermöglicht eine präzisere Steuerung von Zugriffen bei gleichzeitig klaren Verantwortlichkeiten.

Vorteile auf einen Blick

- **Einheitliche Security-Policies** über alle Standorte, Clouds und Nutzer*innen hinweg
- **Reduzierte Komplexität** durch integrierte Netzwerk- und Sicherheitsarchitektur
- **Höhere Resilienz** durch Segmentierung und kontrollierte Datenflüsse
- **Transparenz und Governance** für Compliance, Betrieb und Audits

Moderne **SASE-Architekturen** bündeln Netzwerk- und Sicherheitsfunktionen in einer integrierten Plattform. Sicherheitsrichtlinien werden über Standorte, Clouds und Nutzer*innen hinweg einheitlich durchgesetzt, während SD-WAN den Datenverkehr dynamisch optimiert. Das reduziert Komplexität im Betrieb und verbessert die Auslastung vorhandener Ressourcen.

Durch **Transparenz und Segmentierung** werden Datenströme sichtbar, gezielt gesteuert und voneinander abgegrenzt. Risiken sinken, Compliance wird einfacher nachweisbar und Audit-Aufwände lassen sich signifikant reduzieren.

Automatisierung und zentrale Steuerung schaffen schließlich eine Architektur, die Sicherheit nicht nur bereitstellt, sondern aktiv durchsetzt. Das Ergebnis: eine sichere, performante und steuerbare Vernetzung von Nutzer*innen, Anwendungen, Standorten und Datenflüssen als Grundlage für digitale Geschäftsprozesse und nachhaltige Handlungsfähigkeit.

Wer das Netzwerk im Griff hat, hat die Sicherheit im Griff.

Dr. Niklas Horstmann
COO der Deutschen Telekom Security GmbH

Wer sich nicht kennt, kann sich nicht schützen

Identität ist die neue Sicherheitsgrenze – und das Fundament jeder digitalen Interaktion. Als einer der wenigen europäischen Anbieter betreiben wir die gesamte Vertrauenskette selbst: vom Hardware-Chip bis zur qualifizierten Signatur.

94 %
der Angriffe stehen im Zusammenhang mit gefälschten Identitäten.

55 %
vergeben Zugriffe noch immer über manuelle Verfahren.

<50 %
wissen, wer auf ihre Cloud-Ressourcen zugreifen kann.

-42 %
geringere Schadenkosten durch Zero Trust – rund 1,6 Mio. €.

Quellen: Branchenstudien zu Identity Security & Zero Trust, 2024 / 2025.

Warum Identity Security geschäftskritisch ist

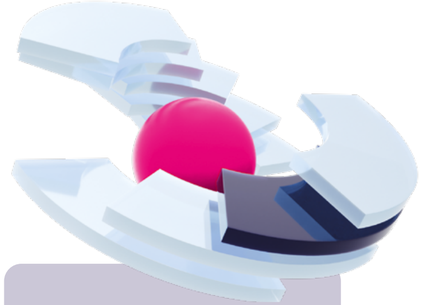
Vertrauen schaffen
Digitale Identitäten als Grundlage jeder sicheren Interaktion

Zero Trust ermöglichen
Zugang nur für die richtigen Personen, Geräte und Services

Skalieren & automatisieren
Weniger manuelle Prozesse, schnellere Abläufe, weniger Fehler

Souveränität sichern
NIS-2, eIDAS und DSGVO erfüllt – mit voller Datenhoheit in der EU

Nahtlose Experience
Einfache Zugriffe steigern Produktivität und Zufriedenheit



Marktführerschaft

Identity-Security-Projekte, die wir umgesetzt haben

- ePersonalausweis & Reisepass
- Elektronische Gesundheitskarte
- Qualifizierte Signatur in Deutschland
- Smart Metering Root
- Behördenfunk
- External Key Management Google Cloud & AWS

Ein Ökosystem – vom Chip bis zur Signatur

Einzelne Produkte schützen Lücken. Unsere Zero Trust Identity Fabric schützt das Ganze – jeder Layer erhöht Reifegrad und Resilienz. Das Ergebnis: ein sicheres, souveränes und KI-fähiges Fundament.

Layer 01
Secure Elements & Hardware-Anker
Verschlüsselte Chips binden Identitäten an Hardware – gegen Manipulation, Cloning und KI-Spoofing. Betrieben auf dem eigenen TCOS.
ROOT OF TRUST

Layer 02
PKI & Trust Center
Das Rückgrat: verifizierte Identitäten für Menschen und Maschinen, Zertifikate als verankertes Vertrauen. Best-in-class auditiert.
MADE IN GERMANY

Layer 03
Identität & Zugang
IAM, Multi-Faktor-Authentifizierung und Governance steuern, wer wann worauf zugreift – nach dem Least-Privilege-Prinzip.

Layer 04
Schutz & Erkennung
PAM sichert privilegierte Konten, SIEM/SOC erkennt und reagiert auf Basis von Echtzeit-Identitätssignalen.

Magenta Security MFA NEU
Zero-Trust-Zugang und adaptive Multi-Faktor-Authentifizierung als Managed Service.

Mobile ID NEU
Die digitale Mitarbeiteridentität auf jedem Smartphone: Anmeldung, Signatur, E-Mail-Verschlüsselung und Zutritt – in einer App.

Magenta Security Sign
Souveräne E-Signatur-Plattform: eIDAS-konform (EES/FES/QES), Zero-Document-Knowledge, Betrieb in Deutschland.

PKI · Secure Elements · Cloud Data Security
Eigenes Trust Center, Qualified.ID, Hardware-Anker und souveränes Key-Management aus der T Cloud.

Keine Digitalisierung ohne Identity Security

- Souverän & EU-betrieben
- eIDAS- & DSGVO-konform
- Modular kombinierbar
- Alles aus einer Hand

Ihr Lagebild. In Echtzeit.

Wann wissen Sie, dass gerade etwas passiert? Mit unseren Visibility- und Intelligence-Services behalten Sie auch in komplexen Umgebungen den Überblick. Angriffe werden identifiziert, bevor sie sich ausbreiten. Wir schaffen das Lagebild, das Sie für eine effektive Reaktion brauchen.

Ein Tag im SOC der Deutschen Telekom

2,5 Mrd.
sicherheitsrelevante Events aus 3.300 Datenquellen

7 Mio.
analysierte Web-Sessions, > 100 GB Datenvolumen

> 6 Mrd.
DNS-Datensätze auf Cyberangriffe geprüft

5.000
Viren und Malware entdeckt

12 Mio.
Angriffe auf unsere 6.000 Honeypots

100 Mio.
E-Mails gescannt

Die zunehmende Digitalisierung und Vernetzung von Unternehmensprozessen führt zu einer stetig wachsenden Angriffsfläche für Cyberbedrohungen. Moderne IT-Landschaften, hybride Infrastrukturen und Cloud-Services erhöhen nicht nur die Effizienz, sondern auch die Komplexität der Sicherheitsanforderungen. Die zentrale Herausforderung besteht darin, Bedrohungen frühzeitig zu erkennen, Risiken ganzheitlich zu bewerten und Sicherheitsmaßnahmen wirksam zu orchestrieren – ohne den Geschäftsbetrieb zu beeinträchtigen.

Unser integriertes Cyber Defense & Security Operations Center (SOC) erfasst jederzeit die sich ständig verändernde Bedrohungslandschaft und bietet Unternehmen proaktiven Schutz vor der wachsenden Zahl globaler Cyberbedrohungen. Mit mehr als 1.800 Security-Spezialist*innen weltweit, modernsten Technologien und einer 24/7-Verfügbarkeit sorgt unser SOC dafür, dass Angriffe nahezu in Echtzeit erkannt, abgewehrt und detailliert analysiert werden. Dieses umfassende Lagebild ermöglicht es, Schwachstellen frühzeitig zu identifizieren und Angriffsmuster zu verstehen, um zukünftige Bedrohungen noch effektiver zu verhindern.

Vorteile auf einen Blick

- Ganzheitlicher Schutz für IT, OT und geschäftskritische Cloud-Infrastrukturen
- KI-gestützte Angriffserkennung für schnelle und präzise Reaktion
- Moderner, leistungsfähiger Tool-Stack
- 24/7-Überwachung für kontinuierliche Detection & Response
- Visibilität in der gesamten Infrastruktur

Vom Alarm zur Reaktion

Erkennen allein reicht nicht. Was zählt, ist die richtige Reaktion. Mit unseren Active-Defense-Services stoppen und dämmen wir Angriffe aktiv ein, statt nur zu warnen. Wir greifen dort ein, wo es darauf ankommt. Und schützen so Ihre Systeme in Echtzeit.

Die Bedrohung ist so hoch wie nie zuvor

In einer Zeit zunehmend komplexerer Cyberbedrohungen – oft unterstützt durch KI – reicht bloßes Erkennen von Angriffen nicht mehr aus. Ein strategisches und konsequentes Vorgehen sowie proaktive Sicherheitsmaßnahmen sind entscheidend. Unsere **Managed Detection and Response (MDR) Services** bieten kontinuierliche Überwachung, frühzeitiges Erkennen von Bedrohungen und gezielte Reaktionen, die Ihr Unternehmen rund um die Uhr schützen. Mithilfe modernster Technologien, KI-gestützter Analysen und Expertenwissen stoppen wir Angriffe, dämmen ihre Ausbreitung ein und beheben die Ursachen, um Ihre Geschäftsabläufe nachhaltig zu sichern.

In der modernen Cyberabwehr verschiebt sich der Fokus hin zu proaktiven Sicherheitsstrategien. Präventive Maßnahmen wie Endpoint Detection & Response (EDR) oder Exposure Management ermöglichen es uns, Anomalien und Schwachstellen frühzeitig zu erkennen und zu beheben, bevor Schaden entstehen kann. Gleichzeitig wächst die Response-Fähigkeit des SOC, indem es eigenständige Sofortmaßnahmen ergreifen kann: Durch Breach Containment kann das SOC rund um die Uhr potenzielle Bedrohungen schnell und ohne kundenseitiges Zutun eindämmen. Dies erhöht die Effizienz und minimiert Risiken deutlich.

28 %
der befragten Unternehmen erleben fast täglich Ransomware-Angriffe – mehr als doppelt so viele wie 2024[1]

50 %
nennen KI-unterstützte Cyberangriffe die größte Herausforderung[2]

66 %
können einen totalen Betriebsstillstand nach einem Cyberangriff nicht ausschließen[1]

[1] Deloitte Cyber Security Report 2026: **Wie resilient sind Österreichs Unternehmen in Sachen Cybersicherheit?**
[2] KPMG: **Cybersecurity in Österreich 2026**

Vorteile auf einen Blick

Kontinuierliche Abwehr
Bedrohungen werden in Echtzeit erkannt, analysiert und gestoppt, bevor sie Schaden anrichten.

Kompletter Überblick
Unsere Services schaffen Visibilität über Ihre gesamte IT-Umgebung – auch in hybriden und cloudbasierten Infrastrukturen.

24/7-Monitoring
Ständige Kontrolle und schnelle Reaktion durch unser Expertenteam.

KI-gestützte Präzision
Hochentwickelte Algorithmen und Technologien ermöglichen die präzise Erkennung und Bearbeitung von Bedrohungen.

Fachliche Unterstützung
Security-Expert*innen übernehmen die Analyse und Reaktion, sodass Ihre Ressourcen entlastet werden.

Unsere Angebote zur Cyberabwehr

- **MDR Enterprise**
  Ein Managed-Detection-and-Response-Service (MDR), der Sicherheitsereignisse kontinuierlich analysiert und korreliert, Bedrohungen frühzeitig erkennt und bei Angriffen schnelle Gegenmaßnahmen unterstützt. MDR Enterprise für komplexere bzw. größere Kundenumgebungen mit weitergehender Integration und kundenspezifischen Anforderungen gedacht ist.
- **MDR Pro**
  Umfassender MDR-Service für Unternehmen mit erhöhtem Schutzbedarf, der kontinuierliche Überwachung, professionelle Bedrohungsanalyse und schnelle Reaktion auf Sicherheitsvorfälle verbindet.
- **CyberProtect**
  Einstiegslösung für Managed Detection & Response, die Unternehmen einen unkomplizierten Zugang zu professioneller Bedrohungserkennung und Unterstützung bei Sicherheitsvorfällen bietet.

Erst Angriffe abwehren, dann das Restrisiko versichern: Auf Wunsch verbindet die Telekom professionelle Cyberabwehr mit finanzieller Absicherung im Schadensfall (Cyberversicherung). → Mehr Infos auf Seite 29.

Ein hundertprozentiger Schutz kann nie garantiert werden. Im Fall eines Cyberangriffs zählt jede Sekunde. Deshalb ist es wichtig, unmittelbar auf Sicherheitsvorfälle zu reagieren, um Schäden zu minimieren und Ihre Systeme schnell wiederherzustellen. Dabei greifen wir auf bewährte Prozesse, modernste Technologien und umfassendes Fachwissen zurück. So stellen wir sicher, dass Bedrohungen schnell behoben und zukünftige Angriffe noch besser abgewehrt werden können.

Digitale Souveränität
Wahlfreiheit, Sicherheit und Kontrolle

Sicherheitsverantwortliche stehen unter Druck: Immer mehr Cloud- und KI-Anwendungen müssen abgesichert werden. Gleichzeitig werden (auch regulatorische) Forderungen nach Souveränität lauter. Wie funktioniert souveräne Cybersecurity?

>80 %
der eingesetzten Hard- und Software in der EU stammt aus Nicht-EU-Ländern[1]

Warum wird Souveränität so wichtig?

Geopolitische Spannungen
Geopolitische Spannungen und Unwägbarkeiten nehmen zu, weshalb Abhängigkeiten von nichteuropäischen Technologieanbietern zunehmend kritisch eingestuft werden.

Regulierungen
Die EU-Kommission reagiert auf die geopolitische Lage mit umfassenden Maßnahmen, damit Europa unabhängiger von außereuropäischer digitaler Infrastruktur wird.

Operationale Souveränität

Um Datensouveränität sicherzustellen, kommt es nicht nur darauf an, wo Daten gespeichert werden. Auch die operationale Ebene spielt eine wichtige Rolle. Das heißt:

- **Wer hat Zugriff – und unter welcher Rechtsordnung?**
- **Wie werden Betriebsabläufe gesteuert und Vorgaben durchgesetzt?**
- **Hält das Modell Audits und regulatorischen Prüfungen stand?**

> **Angesichts geopolitischer Spannungen und der Anfälligkeit von Lieferketten überprüfen Regierungen, öffentliche Institutionen und private Unternehmen gleichermaßen ihre Abhängigkeiten von ausländischen Technologieanbietern und globalen Cloud-Infrastrukturen.**
>
> **World Economic Forum**
> Global Cybersecurity Outlook 2026[2]

[1] Draghi_Report 2024 / Europäische Kommission
[2] https://www.weforum.org/publications/global-cybersecurity-outlook-2026/in-full/3-the-trends-reshaping-cybersecurity/

Unser Angebot:
Sovereign Cortex with T Security

Gemeinsam bieten die Deutsche Telekom und Palo Alto Networks ein datensouveränes Betriebsmodell für die Cyberabwehr: Sovereign Cortex with T Security. Die Lösung kombiniert marktführende KI-Cybersicherheit mit einer datensouveränen Architektur, die speziell für Europa entwickelt wurde. Die Daten werden ausschließlich innerhalb Europas verarbeitet. Die Schlüssel werden von der Deutschen Telekom in deutschen Rechenzentren erzeugt, gespeichert und verwaltet. Auf diese Weise kann niemand außerhalb der Deutschen Telekom die Daten lesen.

Optimal für die kritische Infrastruktur: „Sovereign Cortex with T Security“ erfüllt damit auch hohe regulatorische Anforderungen inklusive DORA, NIS-2 und DSGVO.

KI-gestützte Sicherheitsplattform
von Palo Alto Networks

Fortschrittliche Technologie
Die Plattform vereint Endpoint Security, SIEM, Sicherheits-orchestrierung und Automatisierung für durchgängige Erkennung, Analyse und Reaktion.

Proaktive Prävention, Erkennung und Response
Angriffe werden erkannt, priorisiert und automatisiert adressiert, bevor sie geschäftskritisch werden.

Gemeinsame Datenbasis
Nutzerdaten, Alerts und Incidents laufen in einer integrierten Plattform zusammen statt in isolierten Tools.

Globale Threat Intelligence und Innovation
Plattformweiterentwicklung und Threat Intelligence unterstützen aktuelle und zukünftige Sicherheitsanforderungen.

+

Souveränität, Compliance und Service
von T Security

External Key Management in deutschen Rechenzentren
Sichere Schlüsselverwaltung nach höchsten Standards
- Datensouveräner Betrieb
- C5-Testierung
- IAM-Services
- Betrieb und Support durch Personal innerhalb der EU
- Nachvollziehbare Logs für Compliance und Audits

24/7 SOC und Monitoring
Kontinuierliche Überwachung und schnelle Incident Response
- Betrieb in der EU
- Zusätzlich Telekom Threat Intelligence
- Kundenindividuelle ASP
- Anbindung ans CERT

Service-Management
Prozesse für einen stabilen und sicheren Betrieb
- Eskalations-Management
- Change-Management
- Unterstützung für Audits
- Reporting
- Cyber Defense Reviews

Wir übernehmen, wenn es ernst wird
Telekom Incident Response

Bei einem schwerwiegenden IT-Sicherheitsvorfall erreichen Sie uns unter:

+49 228 555 225 000

Was passiert, wenn ein Angriff wirklich durchkommt? Entscheidend ist, wie schnell Sie reagieren. Unsere qualifizierten Incident Response Teams stehen rund um die Uhr bereit, übernehmen das Krisenmanagement und minimieren den Schaden. Denn das Timing entscheidet, ob ein Vorfall beherrschbar bleibt.

Krisenmanagement
Bewertung, Risikoeinschätzung und Organisation

Wenn ein Cyberangriff den Geschäftsbetrieb bedroht, braucht es koordinierte Führung, belastbare Entscheidungen und klare Kommunikation. Wir helfen, ein Lagebild aufzubauen, Rollen zu klären und Entscheidungen vorzubereiten. Wir helfen bei der effektiven Zusammenarbeit der internen Teams genauso wie bei der Interaktion mit externen Stakeholdern. So bleiben Sie auch unter Druck handlungsfähig und behalten die Kontrolle über die Krise.

Incident Response
Eindämmung, Bereinigung und Wiederaufbau

Fehler bei der Reaktion auf einen Cyberangriff können schwerwiegende Folgen haben. Incident Response ist die koordinierte Aufarbeitung und Reaktion nach einem Vorfall. Wir unterstützen bei der technischen Bewertung und der Eindämmung des Angriffs. Unsere Experten koordinieren Spezialisten und begleiten den sicheren Wiederanlauf. Immer mit dem Ziel, die Höhe des Schadens, Ausfallzeiten und Folgeangriffe zu reduzieren.

Digitale Forensik
Beweissicherung, Analyse und Ursachenermittlung

Digitale Forensik liefert belastbare Fakten. Wir sichern, analysieren und bewerten digitale Spuren. So werden Angriffsweg, Einfallsvektor und Umfang des Vorfalls nachvollziehbar. Unsere Ergebnisse helfen, technische Maßnahmen, Managemententscheidungen, Meldepflichten und Kommunikation auf eine belastbare Grundlage zu stellen. So wird der Vorfall nicht nur bewältigt, sondern verstanden und in konkrete Verbesserungen übersetzt.

Warum Telekom?

Bereit für den Notfall

Unser Incident Response Service bietet Ihnen eine rund um die Uhr erreichbare Notfallhotline mit einer Fallannahme innerhalb einer Stunde.

Mit und ohne Agent

Wir arbeiten mit vorhandenen Strukturen und Software. Wenn kurzfristig mehr Sichtbarkeit nötig ist, unterstützen wir beim Deployment geeigneter Monitoring-Lösungen.

Telekom Sicherheitsverbund

Wir nutzen Erkenntnisse aus unserem SOC, CERT und Cyber Threat Intelligence für die Lagebewertung und die Aufarbeitung von Fällen.

Ein Ansprechpartner, ein Lagebild

Ein zentraler Case Handler steht Ihnen für die Vorfallsbehandlung zur Verfügung und koordiniert Leistungen und Spezialisten der Telekom.

Remote und vor Ort

Wir bieten Ihnen Unterstützung im DACH-Raum durch Experten für Incident Response, Krisenmanagement, digitale Forensik und Wiederaufbau.

Belastbare Forensik

BSI-zertifiziertes Labor, moderne Analysewerkzeuge und standardisierte Verfahren für belastbare Ergebnisse – im Bedarfsfall auch gerichtsfest.

Fallbeispiel:
Ein Angreifer im Netz

Einen diffusen Cyberangriff gilt es aufzuhalten, bevor Schaden entsteht. Entscheidend wird, wie schnell ein gemeinsames Lagebild entsteht.

Der erste Alarm
Zunächst wirkt alles wie eine Systemstörung: Anmeldungen schlagen fehl, Server reagieren langsam, Anwendungen hängen. Dann melden Sicherheitssysteme verdächtige Aktivitäten: Malware im Netzwerk.

Die Lage wird unübersichtlich
Die Überprüfung der Alarme zeigt, dass kritische Systeme betroffen sind und es ist unklar, worauf der Angreifer bereits Zugriff hat. Ein Produktionsstopp steht im Raum. In diesem Moment wird deutlich: Die Organisation braucht Incident-Response-Unterstützung.

Gemeinsam vom Alarm zum Maßnahmenplan
Ein Krisenteam wird gebildet. Es entsteht ein Lagebild aus betroffenen Systemen, operativen Abhängigkeiten und Geschäftsrisiken. Sofortmaßnahmen werden priorisiert und umgesetzt. So kann die Ausbreitung des Angriffs gestoppt werden.

Forensik schafft Klarheit
Telekom Forensiker untersuchen Logdaten, Systeme und verdächtige Dateien. Der initiale Zugriff, die Ausbreitung des Angriffs und mögliche Datenabflüsse werden rekonstruiert. Innerhalb von Stunden sind erste Ergebnisse verfügbar und werden für den Krisenstab aufbereitet.

Strukturierter Wiederanlauf
Der Wiederanlauf erfolgt kontrolliert und nach Geschäftsrelevanz priorisiert. Betroffene Systeme werden bereinigt oder neu aufgebaut, Zugangsdaten rotiert und Sicherheitskontrollen nachgeschärft. Auch dabei unterstützen Experten der Telekom vor Ort.

Was bleibt
Der Angriff wird gestoppt, bevor er flächendeckenden Schaden verursacht. Das Unternehmen erhält belastbare Erkenntnisse und konkrete Verbesserungsmaßnahmen. Aus dem Vorfall entsteht eine sicherere und resilientere Organisation.

Bundesamt für Sicherheit in der Informationstechnik
- Qualifizierter APT-Response-Dienstleister
- IT-Sicherheitsdienstleister in dem Geltungsbereich Vorfallbearbeitung

Sie wollen Ihre Reaktion verbessern?

Wir unterstützen Sie mit passenden Leistungen zur Verbesserung Ihrer Incident Response.

Incident-Response-Unterstützung
Informieren Sie sich über den Magenta Security Incident Response Service und sichern Sie sich strukturierte DFIR-Unterstützung für den Ernstfall.

Teams gezielt vorbereiten
Stärken Sie Rollen, Abläufe und Entscheidungsfähigkeit mit Tabletop-Übungen sowie Workshops zu Incident Response, Digitaler Forensik oder Wiederanlauf nach einem IT-Sicherheitsvorfall.

Reaktion realistisch testen
Prüfen Sie Ihre Tools, Prozesse und Teams mit Penetration Testing, Red Teaming und Purple Teaming unter realitätsnahen Bedingungen.

Wenn Angreifer agieren, verlieren Organisationen Kontrolle.

Incident Response dreht dieses Verhältnis um.

Stärker zurück. Sicherer in die Zukunft.

Cyber Resilience & sichere Wiederherstellung nach dem Ernstfall

Ein Cyberangriff endet nicht mit der Eindämmung. Entscheidend ist, wie schnell, sauber und sicher ein Unternehmen wieder in den Normalbetrieb zurückkehrt. Genau hier setzt unsere Expertise für Cyber Resilience an: Wir begleiten Kund*innen vor, während und nach dem Ernstfall – mit professioneller Analyse, belastbaren Backup- und Recovery-Konzepten, klaren Wiederanlaufplänen und kontinuierlicher Verbesserung, wenn es doch mal so weit kommt.

Im Mittelpunkt steht nicht ein einzelnes Tool, sondern die sichere Wiederherstellung geschäftskritischer Systeme als Ganzes. Wir verbinden langjährige Erfahrung aus Backup-Projekten und Security-Know-how mit modernen Cyber-resilience-Methoden und operativer Praxis aus komplexen Kundenumgebungen.

Unsere Expertise

>50 Expert*innen
für Cyber Resilience und Recovery

Cyber Resilience braucht mehr als Technologie – sie braucht Menschen, die Backup, Security, Infrastruktur und Betrieb verstehen. Mit über 50 Expertinnen und Experten aus unterschiedlichen Rollen und Phasen unterstützen wir Kund*innen dabei, Recovery nicht erst im Ernstfall anzugehen, sondern fest im Sicherheits- und Betriebsmodell zu verankern.

500+ Systeme
erfolgreich in moderne Recovery-Strukturen überführt

Wir haben bereits mehrere hundert Systeme aus Management- und Kundenumgebungen in moderne Data-Protection- und Recovery-Strukturen integriert. Dabei geht es nicht nur um Datensicherung, sondern um getestete Wiederherstellungsszenarien je Workload – von klassischen Infrastrukturen mit komplexen Datenbanken und Applikationen bis hin zu Cloud- und SaaS-Plattformen.

>10 Jahre
bewährte Erfahrung
aus der eigenen Betriebsumgebung

Wir beraten nicht nur theoretisch, sondern setzen moderne Cyber-Resilience-Ansätze auch selbst im eigenen Betrieb ein. Über Jahre gewachsene Backup-Landschaften wurden konsolidiert, mehrere Einzellösungen zu einer zentralen Architektur zusammengeführt und Recovery-Szenarien für unterschiedliche Workloads aufgebaut. Daraus entsteht Praxiserfahrung, die direkt in Kundenprojekte einfließt.

Unser Vorgehen:

5 Schritte zu mehr Cyber Resilience

Vorbereiten
Wir analysieren bestehende Backup- und Recovery-Strukturen, bewerten Risiken und definieren gemeinsam mit dem Kundenunternehmen Ziele für RTO, RPO, Schutzbedarf und Wiederanlaufprioritäten (Stichwort: Minimum Viable Company). Daraus entstehen belastbare Konzepte, die zu Organisation, Infrastruktur und Kritikalität der Systeme passen.

Absichern
Wir unterstützen beim Aufbau robuster Datensicherungs- und Recovery-Architekturen, passend zur vorhandenen IT-Landschaft – inklusive unveränderlicher Sicherungen, logisch getrennter Architekturen, regelmäßiger Snapshots und klarer Verantwortlichkeiten im Betrieb.

Erkennen
Cyber Resilience bedeutet, Risiken frühzeitig sichtbar zu machen und für den Ernstfall vorbereitet zu sein. Deshalb betrachten wir Backups nicht nur als Kopie, sondern als wertvolle Quelle für Sicherheitsanalysen. Anomalien, bekannte Angriffsmuster und kompromittierte Datenstände lassen sich so schneller erkennen und in die Recovery-Entscheidung einbeziehen.

Wiederherstellen
Im Ernstfall begleiten wir die kontrollierte, vorab abgestimmte Rückkehr in den Normalbetrieb. Ziel ist eine sichere, priorisierte und nachvollziehbare Wiederherstellung geschäftskritischer Systeme – schnell, aber nicht hektisch, strukturiert nach definierten Recovery-Plänen.

Verbessern
Jeder Vorfall ist auch eine Chance, besser zu werden. Nach der Wiederherstellung unterstützen wir bei Lessons Learned, der Optimierung der Backup-Strategie, der Anpassung von Wiederanlaufplänen und der nachhaltigen Stärkung der individuellen Cyber Resilience.

Vorteile für unsere Kund*innen

- **Deutliche Effizienzgewinne durch Konsolidierung und moderne Backup-Methoden**
  Moderne Backup- und Recovery-Architekturen reduzieren Speicherbedarf, Betriebsaufwand und Komplexität – Einsparungen von bis zu 70 % sind möglich. Diese Effekte entstehen durch Konsolidierung, Deduplizierung, Kompression und optimierte Betriebsmodelle.

- **Kontinuierliche Prüfung statt blinder Wiederherstellung**
  Nach einem Angriff reicht es nicht, irgendeinen alten Datenstand wiederherzustellen – entscheidend ist der letzte saubere Stand. In modernen Cyber-Resilience-Szenarien werden Backups regelmäßig gegen aktuelle Erkennungslogiken und Angriffspattern geprüft. So lassen sich Auffälligkeiten schneller erkennen, betroffene Datenbereiche eingrenzen und Wiederherstellungspunkte fundierter auswählen.

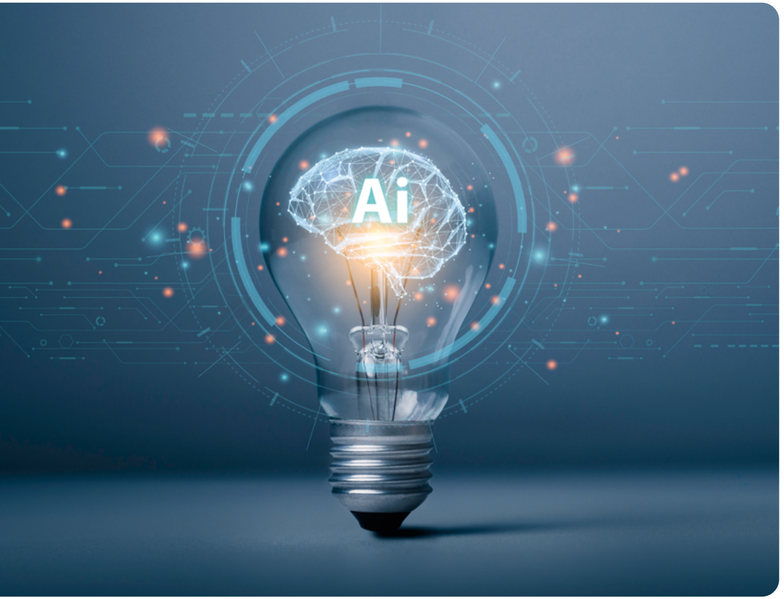
Wer im Normalbetrieb vorbereitet ist, kann im Krisenfall kontrolliert wiederherstellen.

Christian Tucholski
Head of Security,
operational services GmbH & Co. KG

360° KI-Sicherheit

Bedrohungen erkennen. Risiken steuern. Vertrauen sichern.

Künstliche Intelligenz verändert die Bedrohungslandschaft fundamental. Angriff und Verteidigung sind gleichermaßen betroffen. Wer Cyberresilienz aufbauen will, braucht Sicherheit, die genauso intelligent ist wie der Angriff.



Ausgangslage

KI verändert die Angriffsfläche grundlegend

Angreifer nutzen KI heute, um Angriffe zu automatisieren, zu personalisieren und in industriellem Maßstab zu skalieren. Unternehmen ohne entsprechende Gegenmaßnahmen verlieren den Wettlauf gegen maschinell optimierte Bedrohungen.

335.000
Cybercrime-Fälle in Deutschland 2025 [1]

36.706
DDoS-Angriffe auf Telekom-Netze 2025 (+25 %) [2]

289 Mrd. €
Schaden durch Cyberkriminalität in Deutschland 2025 [3]

Bedrohung 01

Deepfakes: Wenn Sehen und Hören aufhört zu schützen

KI-generierte Stimmen und Gesichter sind längst nicht mehr von echten zu unterscheiden. Angreifer setzen Voice Deepfakes gezielt im CEO-Fraud ein, umgehen Awareness-Maßnahmen und machen Spear-Phishing-Kampagnen durch synthetische Identitäten hyperrealistisch.

46 %
der Fraud-Experten berichten von Synthetic Identity Fraud in ihrem Unternehmen [4]

0,1 %
der Teilnehmer einer Studie erkannten alle Deepfake- und echten Inhalte korrekt, selbst bei gezielter Suche nach Fakes [5]

Voice Deepfake
Synthetische Stimmen imitieren Führungskräfte in Echtzeit. CEO-Fraud ist damit ohne echte Sprachproben in Minuten reproduzierbar.

Deepfake Spear-Phishing
Personalisierte Video- und Audio-Köder für hochwertige Ziele: kontextgenau, skalierbar, schwer erkennbar.

AI-gestütztes Social Engineering
Automatisierte Manipulation durch kontextsensitive Kommunikation, maßgeschneidert auf Zielpersonen aus öffentlichen Datenquellen.

Bedrohung 02

GPT-Cyber: KI als Waffe im Cyberspace

Generative KI senkt die Einstiegshürde für Cyberangriffe dramatisch. Selbst wenig erfahrene Angreifer können mit LLM-gestützten Tools Malware entwickeln, Phishing automatisieren und Schwachstellen eigenständig auskundschaften. Die Deutsche Telekom hat dafür bereits ein mehrstufiges KI-gestütztes Sicherheitskonzept entwickelt [6] zum Schutz von konventioneller IT&OT bis hin zur Absicherung von KI-Agenten-Ökosystemen.

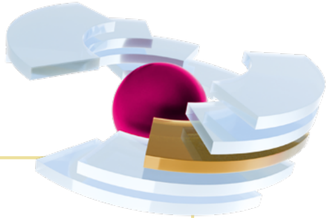
AI-Malware
Selbstoptimierende Schadsoftware lernt Erkennungsmuster aktiv und umgeht sie. Klassische Signaturerkennung versagt.

Automatisiertes Spear-Phishing
LLMs erstellen täuschend echte, kontextsensitive Nachrichten in Sekundenbruchteilen und skalieren das auf tausende Ziele gleichzeitig.

Prompt Injection
Eingeschleuster Schadkontext manipuliert KI-Systeme von innen. Angreifer übernehmen so die Kontrolle über KI-gestützte Prozesse. [7] [8]

AI-Reconnaissance
Automatisiertes Mapping von Angriffsflächen in Minutenschnelle, mit einer Geschwindigkeit und Skalierung, die manuelle Methoden allein nicht erreichen können. [9]

[1] BKA: Bundeslagebild Cybercrime 2025 — 335.000 Fälle, 202 Mrd. € Schaden, KI verschärft Bedrohungslage (Mai 2026) [2] BKA: Bundeslagebild Cybercrime 2025 — 36.706 DDoS-Angriffe im Telekom-Netz (+25 %) [3] Bitkom e.V.: Wirtschaftsschutz 2025 — 289 Mrd. € Schaden, 87 % der Unternehmen betroffen (Sept. 2025) [4] Statista (2024): 46 % der Fraud-Experten berichten von Synthetic Identity Fraud, 37 % von Voice Deepfakes, 29 % von Video Deepfakes — zit. in: UNESCO / Naffi (2025), deepfakes-and-crisis-of-knowingmm [5] IProov: Deepfake Statistics, Solutions & Biometric Protection — Nur 0,1 % der Teilnehmer erkannten alle Deepfake- und echten Inhalte korrekt, selbst bei explizitter Suche nach Fakes [6] Deutsche Telekom: Sicherheitskonzept für KI-Agenten-Ökosysteme — Risiken reduzieren (März 2026) [7] OWASP: Top 10 for LLM Applications 2025 — LLM01: Prompt Injection als kritischstes Risiko [8] OWASP: Top 10 for Agentic Applications 2026 — Peer-reviewed Framework für autonome KI-Systeme (Dez. 2025) [9] MITRE ATLAS: Adversarial Threat Landscape for AI Systems



Bedrohung 03

Agentic AI:
Wenn KI selbst handelt

Autonome KI-Agenten planen, entscheiden und führen Aktionen ohne menschliche Freigabe aus. Einmal kompromittiert, kann ein Agent Zugriffsrechte eskalieren, weitere Systeme manipulieren oder unbemerkt Daten exfiltrieren. Klassische Perimeter-Sicherheit versagt hier strukturell.

Privilege Escalation
Agenten übernehmen schrittweise höhere Berechtigungen und bewegen sich lateral durch Systeme.

Prompt Injection in Pipelines
Eingeschleuster Kontext manipuliert mehrstufige KI-Entscheidungsketten, ohne dass klassisches Monitoring es bemerkt.

Rogue Agents
Unkontrollierte Agenten handeln gegen Systemziele, ausgelöst durch fehlerhafte Instruktionen oder externe Manipulation.

Unkontrollierte Tool-Nutzung
Agenten missbrauchen API-Zugriffe und externe Dienste ohne Rückfrage, ohne Auditlog und ohne definierte Grenzen.

Gegenmaßnahmen: NHI & Zero Trust

NHI Management
Jeder Agent erhält minimale, zeitlich begrenzte Identitäten ohne dauerhaften Zugriff.

Zero-Trust-Architektur
Kein implizites Vertrauen. Jede Aktion wird kontextuell verifiziert.

Agent Sandboxing
Isolierte Ausführungsumgebungen begrenzen das Schadpotenzial kompromittierter Agenten.

Kontinuierliches Monitoring & Testing
Verhaltensanomalien werden in Echtzeit erkannt und automatisiert eskaliert.

KI-Sicherheit ist keine Ergänzung zur bestehenden Cyberstrategie. Sie ist deren neue Grundlage. Wer KI einsetzt, ohne sie abzusichern, schafft Angriffsflächen, die kein klassisches Tool erkennt.

"Deutsche Telekom Security's innovation strategy also extends into AI security. The company has developed a dedicated AI security portfolio that includes automated LLM and chatbot penetration testing through Deemster, runtime model protection, and AI governance advisory services."

Claudio Stahnke
Senior Industry Analyst bei Frost & Sullivan

[10] EU AI Act: Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates
[11] BSI: Lagebericht IT-Sicherheit 2025 — 309.000 neue Schadsoftware-Varianten täglich (+26 %)

Portfolio

KI-Sicherheit aus einer Hand

T Security bietet ein vollständiges Portfolio, das die gesamte KI-Sicherheitskette abdeckt: von der Analyse über Governance bis zur aktiven Verteidigung.

AI Security Assessment
Systematische Analyse der AI-Infrastruktur auf Schwachstellen, Fehlkonfigurationen und Angriffspotenziale, inklusive Modellen, Pipelines und Integrationspunkten.
→ Klarer Blick auf die tatsächliche Risikolage ohne Blindstellen.

AI Governance Consulting
Aufbau von Richtlinien, Kontrollmechanismen und Verantwortlichkeiten für sicheren KI-Einsatz. Orientierung an EU AI Act [10], DSGVO und BSI-Empfehlungen [11].
→ Compliance-sichere AI-Nutzung von Anfang an.

AI Penetration Testing
Offensive Sicherheitstests gegen KI-Systeme: Prompt Injection, Modell-Extraktion, adversarielle Angriffe und Agentic-AI-Szenarien, durchgeführt von spezialisierten Red Teams.
→ Reale Angriffssimulation vor dem echten Ernstfall.

AI Driven Cyber Security
KI-gestützte Verteidigungslösungen: automatisierte Bedrohungserkennung, intelligente SIEM-Integration und adaptive Incident Response rund um die Uhr.
→ Schneller, präziser und skalierbarer als klassische Ansätze.

Bedrohung → Portfolio

Welches Angebot adressiert welche Bedrohung?

Bedrohung	Assessment	Governance	PenTest	AI Defense
Voice Deepfakes & Social Engineering	✓	✓	✓	✓
AI-Malware & Automatisiertes Phishing	✓	-	✓	✓
Prompt Injection	✓	✓	✓	✓
Agentic AI / Rogue Agents	✓	✓	✓	✓
AI-Reconnaissance	✓	-	✓	✓

Schutz optimieren mit Cyber Security Versicherung

Cyberschutz neu gedacht: Sicherheit trifft Versicherung

Cyberangriffe zählen heute zu den größten Herausforderungen für Unternehmen. Entscheidend ist daher, Risiken frühzeitig zu identifizieren, Auswirkungen auf den Geschäftsbetrieb zu minimieren und verbleibende finanzielle Schäden abzusichern.

Deshalb bündeln **DeTeAssekuranz, Zurich** und **Telekom Security** ihre Kompetenzen in einer gemeinsamen Lösung: moderne Managed Detection & Response (MDR) Services kombiniert mit einem leistungsstarken Cyber-Versicherungsschutz.

Das Ergebnis ist ein ganzheitlicher Ansatz zur Stärkung Ihrer Cyber-Resilienz – von der technischen Erkennung und Reaktion auf Cyberbedrohungen bis zur finanziellen Absicherung im Schadenfall.

Cybersicherheit, die zu Ihrem Unternehmen passt

Risiken frühzeitig erkennen und reduzieren
Mit den MDR-Services werden sicherheitsrelevante Ereignisse kontinuierlich überwacht, analysiert und abgewehrt. So können Angriffe früher erkannt und Schäden reduziert werden.

Falls es dennoch zum Ernstfall kommt
Die Cyberversicherung unterstützt Ihr Unternehmen mit:

- Maßnahmen in Krisen und Notfällen
- Zugang zu Incident-Response- und Rechtsexperten
- Schnelle Schadenbearbeitung durch erfahrene Spezialisten

Cyberresilienz für Unternehmen jeder Größe

Cyberangriffe erkennen. Auswirkungen begrenzen. Finanzielle Risiken absichern.

Die gemeinsame Cyber-Lösung von DeTeAssekuranz, Zurich und Telekom Security schafft echte Cyber-Resilienz von KMU bis zu Großunternehmen.

Mehr Infos gibt es auf deteassekuranz.de/cyber_insurance

Drei Partner, eine *gemeinsame* Mission.

DeTeAssekuranz Versicherungsservice

DeTeAssekuranz bringt ihre langjährige Cyber- und Marktexpertise in die Entwicklung des Leistungsangebots ein und berät Kund*innen bei der Auswahl eines leistungsstarken Versicherungsschutzes. Als Makler beraten die Experten alle Kund*innen zur Cyberversicherung und sind der erste Ansprechpartner bei Fragen. Sie begleiten die passende Lösung aus Sicht des Versicherungsvertriebs und bringen ihre Branchenkompetenz in die Zusammenarbeit mit Zurich ein.

ZURICH

Zurich bringt als Risikoträgerin ihr Wissen in die Gestaltung und Verwaltung des Produktes ein und unterstützt Kund*innen im Schadenfall beratend etwa bei rechtlichen Themen. Darüber hinaus bietet Zurich mit ihrer operativen Einheit „Zurich Resilience Solutions“ weitere Dienstleistungen wie die quantitative Bewertung von Cyberrisiken und hilft dem Kundenunternehmen, eine ganzheitliche Sicht auf die individuelle Gefahrenlage zu erhalten.

T Security

Mit den Managed Detection & Response Lösungen von Telekom Security werden Unternehmen dabei unterstützt, Cyberbedrohungen frühzeitig zu erkennen und angemessen darauf zu reagieren. Der konkrete Leistungsumfang richtet sich nach der jeweils gewählten MDR-Lösung.

CyberProtect-Versicherung

Die Lösung für kleinere und mittlere Unternehmen mit einem Jahresumsatz von bis zu EUR 250 Mio.

Ihre Vorteile

- Einfaches Antragsverfahren durch verkürzten Fragebogen
- Kombination aus MDR-Service und Cyberversicherung
- Versicherungskapazität über die gesamte Vertragslaufzeit (mit Möglichkeit zur Wiederauffüllung)
- **Laufzeit: 12 Monate bis 24 Monate –** abgestimmt auf das Produkt
- Von Antrag bis Implementierung in kurzer Zeit!
- Attraktives Preis-Leistungs-Verhältnis

Technische Prävention und finanzielle Absicherung aus einer Hand.

MDR PRO-Versicherung

Die individuelle Lösung für Unternehmen mit anspruchsvollen Risiken und einem Jahresumsatz von bis zu EUR 2,5 Mrd.

Ihre Vorteile

- Versicherungskapazitäten von bis zu EUR 10 Mio. über die gesamte Vertragslaufzeit (mit Möglichkeit zur Wiederauffüllung)
- Attraktive Prämien durch Kombination mit MDR PRO
- **Laufzeiten: bis zu 36 Monate**
- Zukunftssicherer Schutz: kontinuierliche Weiterentwicklung entsprechend aktueller Cyberbedrohungen
- Absicherung von Auslandsstandorten möglich
- Individuelle Nachhaftungsoptionen

Der umfassende Cyber-Versicherungsschutz kann – je nach gewählter Lösung und individueller Vereinbarung – insbesondere folgende Bereiche umfassen:

- Schutz bei technischen Störungen und Bedienfehlern
- Präventives und akutes Krisenmanagement
- Daten- und Systemwiederherstellung
- Betriebsunterbrechungsschäden, einschließlich Ausfällen von IT-Dienstleistern
- PR- und Kommunikationskosten
- Schutz bei Cyber-Erpressung
- Bußgelder, Schadenersatzansprüche und Überwachungsdienstleistungen
- PCI-DSS-Vertragsstrafen
- Medienhaftpflicht und weitere Bausteine

Hinweis: Versicherer und alleiniger Risikoträger der dargestellten Cyber-Versicherung ist die Zurich Insurance Europe AG. DeTeAssekuranz ist als Versicherungsmaklerin tätig. Die Telekom Security erbringt die beschriebenen Cyber-Sicherheitsdienstleistungen. Die jeweiligen Leistungen werden von den genannten Unternehmen eigenverantwortlich erbracht. Die dargestellten Leistungen dienen einer allgemeinen Übersicht. Maßgeblich für Umfang und Voraussetzungen des Versicherungsschutzes sind ausschließlich die jeweiligen Versicherungsbedingungen, individuellen Vereinbarungen sowie mögliche regulatorische Anforderungen in den betroffenen Ländern. Nicht alle Leistungen stehen in jedem Fall oder in jeder Jurisdiktion zur Verfügung.

Sicherheit endet nicht bei einer einzelnen Maßnahme

Cyber Security ist ein kontinuierlicher Prozess. Entscheidend ist, Risiken ganzheitlich zu betrachten und in jeder Phase vorbereitet zu sein. Mit 360° Security von T Security erhalten Sie umfassenden Schutz über den gesamten Sicherheitszyklus hinweg:

Risiken identifizieren und bewerten
Schutzbedarf erkennen, Risiken bewerten und Schwachstellen mit Assessments, Audits, Pentesting und Red Teaming sichtbar machen.

Assets schützen
Infrastruktur, Endpoints und Identitäten mit einer passgenauen Sicherheitsstrategie und wirksamen Schutzmaßnahmen absichern.

Angriffe erkennen
Bedrohungen mit 24/7-SOC-Monitoring sowie KI und Automatisierung frühzeitig identifizieren.

Auf Angriffe reagieren
Angriffe schnell stoppen und eindämmen – unterstützt durch erfahrene Teams und professionelles Krisenmanagement.

Wiederherstellen
Systeme und Geschäftsbetrieb sicher wiederherstellen, Vorfälle forensisch aufarbeiten und die gewonnenen Erkenntnisse für mehr Resilienz nutzen.

Machen Sie Sicherheit zum Rundumschutz! Starten Sie jetzt mit T Security in Ihre 360°-Security-Journey. Und sichern Sie Ihr Unternehmen umfassend ab.

**360° geschützt.
Heute handeln.
Morgen sicherer sein.**

Kontakt für
Geschäftskunden:

Connecting
your world.

Starten Sie den Dialog mit dem Marktführer für Cybersicherheit

Kontakt
security.dialog@telekom.de
security.telekom.de

Herausgeber
Deutsche Telekom Security GmbH
Office Port 1
Friedrich-Ebert-Allee 71–77
53113 Bonn