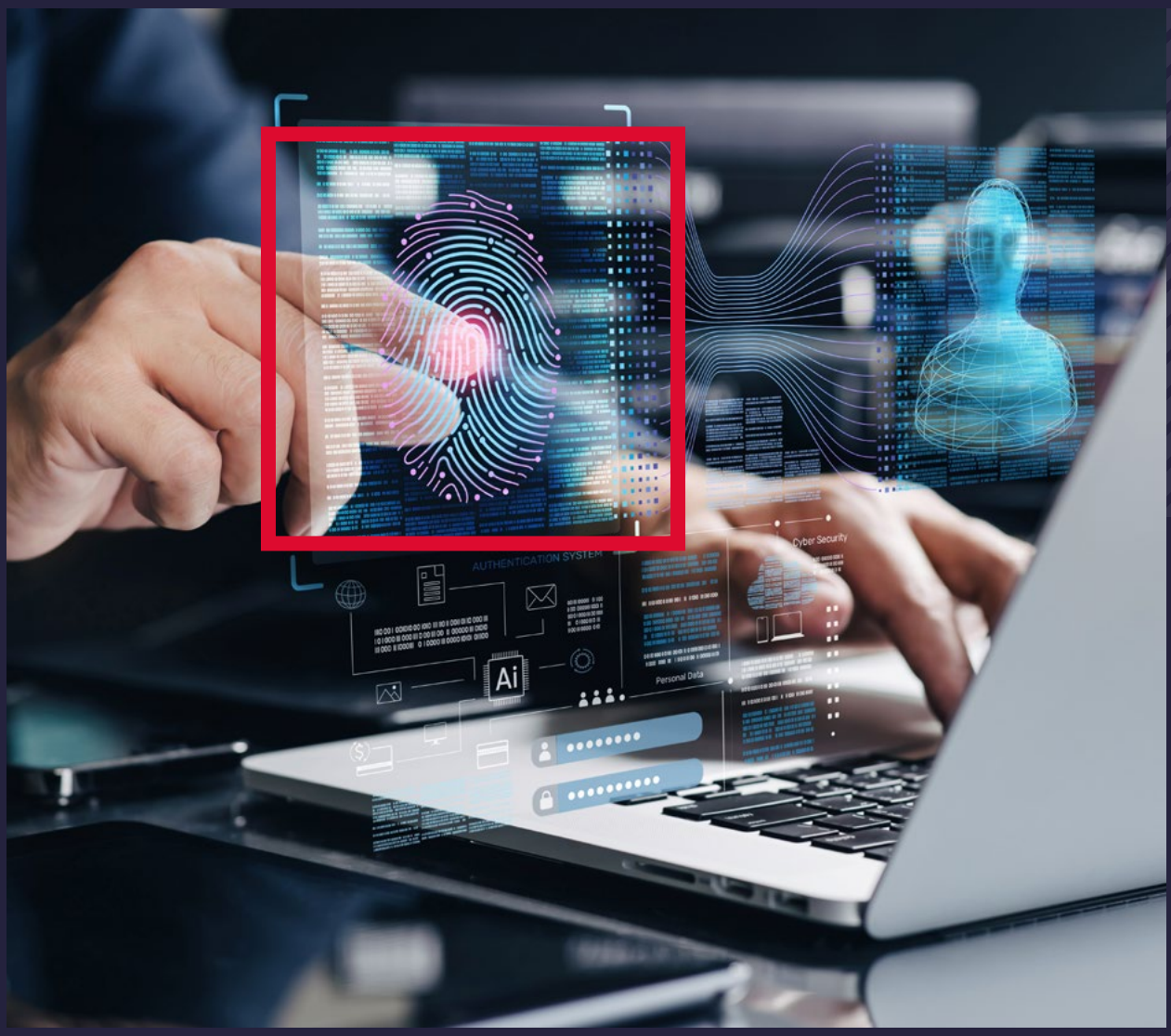
CONSILEON



Schutz vor digitalen Bedrohungen

Von Prävention bis Notfallmanagement

consileon.de

Inhaltsverzeichnis

Einleitung

In einer zunehmend digitalen Wirtschaft sind Daten reines Kapital und auch deswegen lohnendes Angriffsziel. Unternehmen sehen sich hochentwickelten Cyberbedrohungen gegenüber: von gezieltem Phishing und Ransomware über Industriespionage bis zu systematischem Datendiebstahl. Die Methoden werden komplexer, die Folgen gravierender. Kein Unternehmen ist davor gefeit, Opfer einer Attacke zu werden.

Cybersecurity ist weit mehr als eine technische Aufgabe. Sie ist eine unternehmensweite Management-Aufgabe, die Organisation, Technologie und Mensch gleichermaßen betrifft. Letztgenannter bleibt die größte Schwachstelle – ob durch Unachtsamkeit, mangelnde Sensibilisierung oder gezielte Manipulation.

Prävention – Risiken erkennen, bevor sie entstehen

Schutz – Systeme und Prozesse widerstandsfähig gestalten

Notfallmanagement – Im Ernstfall handlungsfähig bleiben

1. Prävention – Risiken erkennen, bevor sie entstehen
Cyberresilienz beginnt mit Voraussicht: durch klare Sicherheitsrichtlinien, regelmäßige Awareness-Schulungen und ein strukturiertes Risikomanagement. Nur wer seine Schwachstellen kennt, kann sie wirksam schließen. Prävention bedeutet, Sicherheit vom Top-Management bis zu den Endanwendern fest in die Unternehmenskultur zu integrieren.

2. Schutz – Systeme und Prozesse widerstandsfähig gestalten
Effektiver Schutz erfordert ganzheitliche Sicherheitsstrategien, die technologische Abwehrmaßnahmen mit organisatorischen Prozessen verzahnen. Moderne Security-Architekturen, kontinuierliches Monitoring und automatisierte Reaktionsmechanismen bilden das Rückgrat einer resilienten IT-Infrastruktur. Ziel ist es, Angriffe frühzeitig zu erkennen und zu neutralisieren, bevor sie Schaden anrichten.

3. Notfallmanagement – handlungsfähig im Ernstfall
Trotz Prävention und Schutzmechanismen kann es zum Ernstfall kommen. Entscheidend ist dann, schnell und koordiniert zu reagieren. Ein professionelles Incident-Response- und Business-Continuity-Management stellt sicher, dass Ausfälle minimiert und Geschäftsprozesse aufrechterhalten werden. Cyberresilienz bedeutet, Angriffe abfedern zu können, funktionsfähig zu bleiben und vor allem gestärkt daraus hervorzugehen.

Consileon: Ganzheitliche Cybersecurity für Ihr Unternehmen

Consileon unterstützt Unternehmen dabei, IT-Sicherheit, Cybersecurity und organisatorische Resilienz zu einer integrierten Strategie zu verbinden. Unser Ansatz geht über reine Technologie hinaus: Wir fördern Bewusstsein, strukturieren Prozesse und stärken Ihre Fähigkeit, auf Vorfälle vorbereitet zu sein – für nachhaltigen Schutz, Stabilität und Zukunftssicherheit in einer digitalen Welt.

”Cybersecurity ist kein Produkt, sondern ein Prozess. Nur wer Technik, Organisation und Menschen gleichermaßen einbezieht, kann sich langfristig gegen digitale Bedrohungen behaupten. Bei Consileon unterstützen wir Sie in Form von Trainings, strategischer Beratung und Umsetzung, sowohl technisch als auch organisatorisch.“

Andreas Grau
Experte für Cybersecurity bei Consileon

Bedrohungsszenario – Digitale Risiken für Unternehmen nehmen rasant zu

Die aktuelle Datenlage zeigt, dass Cyberangriffe auf Unternehmen konstant zunehmen. Laut Bundeskriminalamt wurden im Jahr 2024 **131.391 Fälle von Cyberkriminalität im Inland** registriert. Zusätzlich zählten die Behörden **201.877 Straftaten**, die aus dem Ausland oder von unbekannten Orten ausgingen. Die Aufklärungsquote liegt bei lediglich **32 Prozent**, ein Zeichen dafür, dass viele Täter unerkannt bleiben.[1]

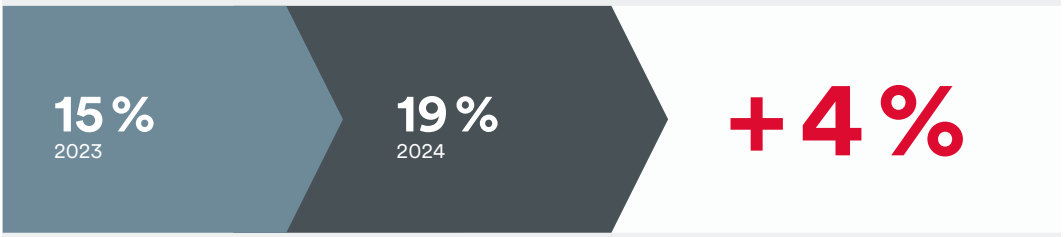
Cyberkriminalität

→ **131.391** Fälle von Cyberkriminalität (Inland)
→ **201.877** Straftaten (Ausland oder unbekannte Orten)

Auch die wirtschaftlichen Schäden steigen rapide: **Bitkom** beziffert den Gesamtschaden durch Cyberangriffe auf deutsche Unternehmen im Jahr 2024 auf **178,6 Milliarden Euro**, rund 30 Milliarden mehr als im Vorjahr. Ein großer Teil entfällt auf Erpressung mit Ransomware und Daten- oder Identitätsdiebstahl.[2]

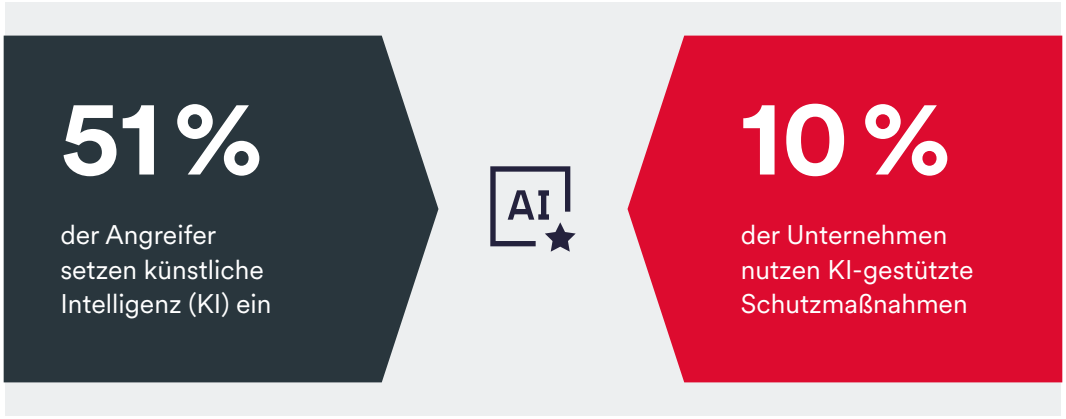
Quellen
1 BKA Bundeslagebild Cybercrime 2024
2 Artikel DataAgenda

Immer mehr Unternehmen werden Opfer von IT-Sicherheitsvorfällen



Bei 84 Prozent der Fälle spielte Phishing eine zentrale Rolle.

Die TÜV Cybersecurity-Studie 2025 unterstreicht zudem, dass die Angriffsformen raffinierter werden: **19 Prozent der Unternehmen** waren 2024 Opfer mindestens eines IT-Sicherheitsvorfalls (+4 Prozent im Vergleich zum Vorjahr). In **84 Prozent** der Fälle spielte **Phishing** eine zentrale Rolle. **51 Prozent** der befragten Unternehmen gehen davon aus, dass Angreifer bereits **künstliche Intelligenz (KI)** einsetzen, während nur **10 Prozent** selbst KI-gestützte Schutzmaßnahmen nutzen.



Trotz dieser Bedrohungslage bewerten **91 Prozent** ihre eigene Cybersicherheit als „gut“ oder „sehr gut“. Gleichzeitig setzen jedoch nur **22 Prozent** Sicherheitsstandards konsequent um, und **nur sehr wenige** führen regelmäßige Cyberaudits bei ihren Zulieferern durch.[3]

Quellen
3 TÜV Cybersecurity Studie 2025

Consileons modulares Cybersecurity-Angebot

Cyberresilienz entsteht, indem Prävention, Schutz und Notfallmanagement nahtlos ineinandergreifen. Unternehmen brauchen sichere Technologien, klare Prozesse und sensibilisierte Mitarbeiter, um Risiken frühzeitig zu erkennen, Angriffe abzuwehren und jederzeit handlungsfähig zu bleiben.

Consileon verbindet diese drei Dimensionen zu einem modularen Cybersecurity-Angebot, das individuell auf den Bedarf jedes Unternehmens abgestimmt wird.
Unsere Module decken das gesamte Spektrum ab – von präventiver Sensibilisierung über strategische Sicherheitsberatung bis hin zur technischen Umsetzung sowie Notfall- & Krisenbewältigung.

Ob Awareness-Trainings, Compliance-Beratung (NIS-2, DORA, CRA, EU-AI-Act, uvm.) oder Implementierung robuster Sicherheitsarchitekturen: Alle Leistungen greifen ineinander und bilden zusammen eine ganzheitliche Sicherheitsstrategie, die Ihr Unternehmen nachhaltig stärkt.

ANGEBOT

Beratung – Strategie mit Weitblick

Effektive Cybersecurity beginnt mit klaren Strukturen und fundierter Analyse. Consileon unterstützt Unternehmen mit Expertise und pragmatischen, angemessenen Lösungen dabei, ihre Sicherheitsstrategie zu entwickeln, Prozesse zu optimieren und regulatorische Anforderungen wie NIS-2 oder DORA , sowie (Branchen-) Standards wie TISAX oder ISO 27001.

**Trainings –
Wissen schafft Sicherheit**

Gezielte Schulungen fördern das Sicherheitsbewusstsein in allen Unternehmensbereichen. Von der Geschäftsführung bis zu den Mitarbeitern werden gesetzliche Anforderungen und aktuelle Bedrohungen durch praxisnahe Szenarien verständlich vermittelt. Dies reduziert Risiken und stärkt das Sicherheitsbewusstsein.

**Technische Umsetzung –
Schutz, der wirkt**

Sicherheitskonzepte werden erst wirksam, wenn sie technisch gelebt werden. Consileon begleitet Unternehmen bei der konkreten Umsetzung von Penetrationstests und Sicherheitsarchitekturen über Security-by-Design bis hin zu DevSecOps-Prozessen.
Das Ergebnis sind robuste Systeme, geschützte Daten und ein belastbares Sicherheitsfundament für die digitale Zukunft.

1. Trainings

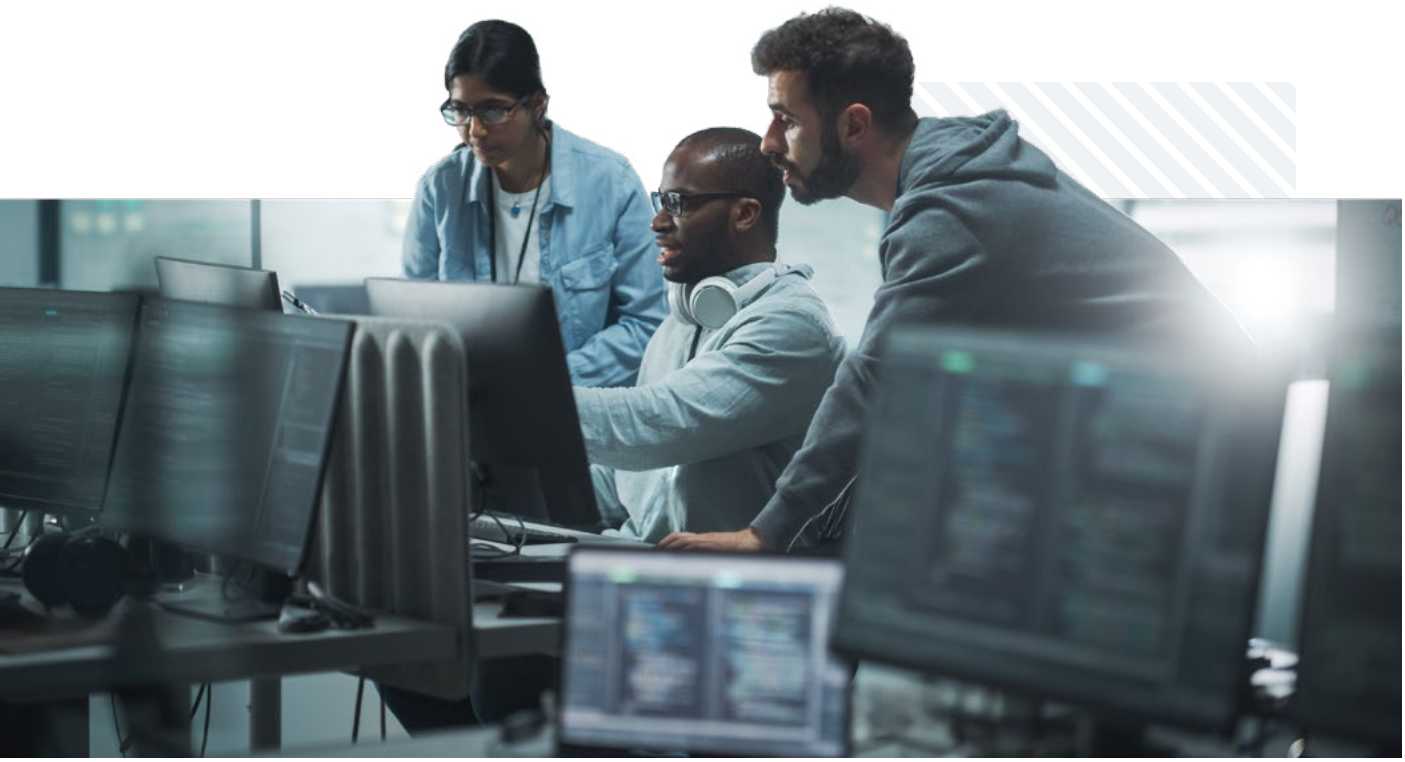
Cybersecurity-Trainings – Wissen schafft Sicherheit

Technologie kann schützen. Doch erst das richtige Verhalten der Mitarbeiter macht ein Unternehmen wirklich sicher. Ein unbedachter Klick auf einen schädlichen Link, ein zu schwaches Passwort oder ein zu sorglos geteilter Zugang sind oft die Einfallstore für Angreifer. Die Vielzahl aller Sicherheitsvorfälle lassen sich auf menschliches Fehlverhalten zurückführen – ein Risiko, das durch gezielte Sensibilisierung deutlich reduziert werden kann.

Mit praxisorientierten Trainings schafft Consileon Bewusstsein, Wissen und Handlungssicherheit auf allen Unternehmensebenen. Die Schulungen werden durch erfahrene Fachexperten und Berater der Consileon durchgeführt, die ihr Wissen aus realen Projekten einbringen – anschaulich, aktuell und wirksam.

Unsere Trainings gehen über reine Pflicht- oder Compliance-Schulungen hinaus. Sie fördern eine echte Sicherheitskultur, in der Mitarbeiter verstehen, wie ihr Verhalten unmittelbar zur Verteidigung des Unternehmens beiträgt. Ob Social-Engineering-Abwehr, Phishing-Simulationen, Datenschutz oder sichere Softwareentwicklung – alle Formate sind modular aufgebaut, praxisnah und auf die jeweilige Zielgruppe abgestimmt.

So entsteht eine nachhaltige Lernkultur, die Sicherheit im Arbeitsalltag verankert und damit den entscheidenden Beitrag zur Cyberresilienz leistet.



Workshop für Entscheider: Orientierung und Verantwortung

Führungskräfte und Entscheider erhalten einen kompakten Überblick über aktuelle Bedrohungsszenarien, rechtliche Rahmenbedingungen und organisatorische Anforderungen. Das Training vermittelt, wie Cyberrisiken strategisch gesteuert und unternehmerische Verantwortlichkeiten klar verankert werden können – als Grundlage für eine wirksame Sicherheitskultur.

Compliance Management Workshop: Regulatorik verstehen und umsetzen

Mit dem Inkrafttreten verschiedener EU-Richtlinien und regulatorischer Vorgaben steigen die Anforderungen an Cybersecurity, Resilienz und Meldepflichten kontinuierlich. In diesem praxisorientierten Workshop analysieren wir gemeinsam mit dem Unternehmen, welche Regelwerke relevant sind – etwa NIS-2, DORA oder TISAX – und entwickeln konkrete Schritte für eine effiziente und angemessene Umsetzung.

Awareness-Training: Sicherheit im Arbeitsalltag

Mitarbeiter lernen, Cyberrisiken im Alltag zu erkennen und sicher zu handeln – vom Umgang mit E-Mails über Passwortschutz bis zu Social-Engineering-Angriffen. Interaktive Elemente, Phishing-Simulationen und realistische Fallbeispiele fördern das Bewusstsein und stärken die Sicherheitskultur dauerhaft.

Mehr erfahren

Ihre Vorteile auf einen Blick:

- Regelkonform handeln: Führungskräfte und Teams verstehen gesetzliche Vorgaben und deren praktische Umsetzung.
- Sicherheitskultur stärken: Mitarbeiter werden zu aktiven Mitgestaltern der Cybersecurity.
- Praxisnah und verständlich: Inhalte werden an den jeweiligen Arbeitskontext angepasst.

2. Beratung

Cybersecurity-Beratung – Strategie mit Weitblick

In vielen Unternehmen wachsen IT-Sicherheitsmaßnahmen historisch: reaktiv, verteilt, oft ohne übergreifende Strategie. Dies mündet in Insellösungen, ineffizienten Prozessen und unklaren Verantwortlichkeiten. Wirksame Cybersecurity entsteht jedoch erst, wenn Technik, Organisation, Compliance und Menschen in einer gemeinsamen Sicherheitsarchitektur wirken.

Consileon unterstützt Unternehmen dabei, Cyberresilienz strategisch zu verankern – mit einem klaren Blick auf Geschäftsprozesse, Risiken und regulatorische Anforderungen. Unsere Berater kombinieren Management-Kompetenz mit technologischem Verständnis und begleiten Organisationen von der ersten Risikoanalyse bis zur Umsetzung einer tragfähigen Sicherheitsstrategie.

Dabei steht Pragmatismus vor Bürokratie: Wir entwickeln Lösungen, die zum Unternehmen passen – messbar, skalierbar und wirtschaftlich vertretbar. Ob Aufbau oder Optimierung eines ISMS, Umsetzung der NIS-2 Anforderungen bis hin zu ISO/ICE 27001 Zertifizierung oder TISAX-Teilnahme: Consileon sorgt für Struktur, Klarheit und Priorisierung.

Unsere Beratung schafft Compliance und echte Steuerungsfähigkeit. So wird Sicherheit zu einem Teil der Unternehmensstrategie und bildet die Grundlage für Vertrauen, Stabilität und nachhaltigen Geschäftserfolg.

Modulares Cybersecurity Assessment: Ausgangspunkt für gezielte Maßnahmen

In einem Cybersecurity Assessment werden bestehende Sicherheitsstrukturen analysiert, Risiken bewertet und Handlungsempfehlungen abgeleitet. Der Umfang dieser Standortbestimmung richtet sich nach Ihrem Bedarf und kann aus einzelnen Bausteinen für Sie zusammengestellt werden. Von einem kompakten Screening über eine umfassende Analyse mit Reifegradbewertung bis zum Audit inklusive Bericht und Maßnahmenplan.

Mehr erfahren

NIS-2-Beratung: Anforderungen verstehen und erfüllen

Die Umsetzung der EU-Richtlinie NIS-2 stellt viele Unternehmen vor neue Herausforderungen. Consileon begleitet Sie von der Betroffenheitsanalyse über die Definition organisatorischer und technischer Maßnahmen bis hin zur effektiven Verankerung im Unternehmen – zur nachhaltigen Sicherstellung von Compliance.

Mehr erfahren

ISMS-Begleitung und Zertifizierung: Sicherheit nach anerkannten Standards

Ob ISO 27001 oder branchenspezifische Standards wie TISAX: Consileon unterstützt beim Aufbau, der Implementierung und kontinuierlichen Verbesserung eines Informationssicherheits-Managementsystems (ISMS) – inklusive Vorbereitung auf externe Audits und Zertifizierungen.

Mehr erfahren

Business-Continuity-Management (BCM)-Beratung: Handlungsfähigkeit sicherstellen

Unsere BCM-Beratung trägt dazu bei, Betriebsunterbrechungen durch IT-Ausfälle, Lieferkettenprobleme oder Personalengpässe zu verhindern. Wir unterstützen Sie dabei, geschäftskritische Prozesse zu identifizieren, Notfall- und Wiederanlaufstrategien zu entwickeln, Notfall- und Krisenübungen durchzuführen und diese Maßnahmen regelmäßig zu testen – damit Sie zu jeder Zeit handlungsfähig bleiben.

Ergänzend stellen wir auf Anfrage und interimsmäßig externe Informationssicherheitsbeauftragte (ISB) zur Verfügung, um Verantwortung, Steuerung und Kontinuität im Sicherheitsmanagement sicherzustellen.

Ihre Vorteile auf einen Blick

- Ganzheitliche Perspektive: Strategische, organisatorische und technische Aspekte – inklusive BCM – werden integriert betrachtet, um Risiken umfassend zu adressieren.
- Regulatorische Sicherheit: Die Beratung orientiert sich an aktuellen Normen und gesetzlichen Vorgaben, sowie an Anforderungen an BCM und Notfallmanagement.
- Nachhaltige Maßnahmen: Die Umsetzung der Empfehlungen führt zu messbaren Ergebnissen, erhöhen die operative Stabilität und stärken langfristig die Cyberresilienz und Geschäftskontinuität des Unternehmens.

3. Technik

Technische Umsetzung – Schutz, der wirkt

Cybersecurity kann nur dann richtig schützen, wenn Sicherheitskonzepte konsequent umgesetzt und regelmäßig überprüft werden: So wird die alltägliche Funktionalität ebenso sichergestellt wie Skalierbar- und Messbarkeit.

Consileon unterstützt Unternehmen bei der Integration ihrer Sicherheitsmaßnahmen in bestehende IT-Landschaften, Entwicklungsprozesse und Betriebsabläufe. Unsere Experten begleiten die Einführung moderner Security-Architekturen, führen Penetrationstests und Schwachstellenanalysen durch und etablieren Prinzipien wie Security-by-Design und DevSecOps als festen Bestandteil der IT-Strategie.

Die technische Umsetzung schafft Transparenz, Stabilität und Anpassungsfähigkeit. Durch kontinuierliches Monitoring, klare Governance-Strukturen und automatisierte Reaktionsmechanismen entsteht ein Sicherheitsniveau, das mit den technologischen Anforderungen und Geschäftsmodellen Ihres Unternehmens wächst.

So wird Sicherheit zum integralen Bestandteil digitaler Innovation und zum Enabler für nachhaltiges, vertrauenswürdiges Wachstum.

Ihre Vorteile auf einen Blick

- Technik mit Substanz: Sicherheitsmaßnahmen werden wirksam in bestehende Systeme und Prozesse integriert.
- Frühzeitige Risikoerkennung: Schwachstellen werden identifiziert, bevor sie ausgenutzt werden können.
- Sicherheit als Qualitätsfaktor: Durch DevSecOps und Security Engineering wird langfristig eine robuste und zukunftssichere IT-Infrastruktur aufgebaut.

Penetrationstests: Schwachstellen gezielt aufdecken

In realistischen Angriffsszenarien prüfen Consileon-Experten Webanwendungen, Infrastrukturen (IAC), Cloud-Design, Netzwerke sowie On-Prem-Systeme auf Sicherheitslücken. Dabei kommen Angriffssimulationen und -emulationen zum Einsatz. Die Ergebnisse bilden eine transparente, nachvollziehbare und praxisorientierte Grundlage für priorisierte Maßnahmen.

Security Engineering: Sicherheit beginnt beim Design

Security Engineering setzt auf vorausschauende Planung, Entwicklung und Umsetzung sicherer Systeme, statt nur auf Bedrohungen zu reagieren. Consileon unterstützt dabei mit ganzheitlichen Architekturen, Prozessen und Technologien, die Sicherheitsanforderungen über den gesamten Lebenszyklus hinweg berücksichtigen und digitale Assets sowie Daten nachhaltig schützen.

DevSecOps: Sicherheit bei der Softwareentwicklung

Risiken minimieren, Kosten senken und die Time-to-Market verkürzen: Die Consileon-Experten sorgen durch die Integration von Sicherheitsaspekten im gesamten System Life Cycle (SDLC) dafür, dass Sicherheitslücken direkt im Prozess unabhängig von der Phase erkannt und behoben werden kann.

Identity & Access Management (IAM): Sichere Verwaltung digitaler Identitäten

Ein wirkungsvolles IAM stellt sicher, dass digitale Identitäten und Zugriffsrechte kontrolliert und nachvollziehbar verwaltet werden. Consileon unterstützt bei der IAM-Analyse und Strategie, dem Rollendesign inklusive Segregation of Duty (SoD), sowie der Konzeption und Dokumentation von Berechtigungsmodellen.

Darüber hinaus begleiten wir die Toolauswahl und Implementierung von IAM-Systemen, etablieren Rezertifizierungsprozesse und stellen die Erfüllung von Compliance- und Audit-Anforderungen sicher.

Mehr erfahren

Cyberresilienz als Erfolgsfaktor

Cyberresilienz entsteht, wenn **Prävention, Schutz und Notfallmanagement** nahtlos ineinandergreifen. Unternehmen, die Risiken frühzeitig erkennen, Systeme konsequent schützen und im Ernstfall in der Lage sind, schnell zu reagieren, sichern ihre Daten und ihre Zukunft!

Dabei gilt es, Menschen, Organisation und Technik als Einheit zu verzahnen. Mitarbeiter, die Risiken verstehen; Prozesse, die Verantwortung verankern; Technologien, die Sicherheit intelligent ermöglichen.

Consileon begleitet Unternehmen auf diesem Weg von der präventiven Sensibilisierung über strategische Beratung bis zur technischen Umsetzung und Notfallplanung. Unser Ziel ist ein Sicherheitskonzept, das lebt: vorausschauend, widerstandsfähig und nachhaltig.

So wird Cyberresilienz zu einem festen Bestandteil Ihrer Unternehmensstrategie und zu einem Wettbewerbsvorteil in einer zunehmend digitalen Welt.

Ihr Experte für Cybersecurity

Andreas Grau verfügt über langjährige Erfahrung in der Informationssicherheit, Cyberresilienz und IT-Governance. Er berät Unternehmen bei der Entwicklung und Umsetzung ganzheitlicher Sicherheitsstrategien – von der Risikoanalyse bis zur technischen Implementierung. Sein Fokus liegt auf praxisnahen, nachhaltigen Lösungen, die zum Unternehmen passen.

Andreas Grau
Senior Project Manager, Cybersecurity Experte,
Consileon Business Consultancy GmbH

+ 49 152 22877014
andreas.grau@consileon.de

Jetzt handeln – für mehr Sicherheit und Resilienz

Cybersecurity ist ein kontinuierlicher Prozess. Consileon begleitet Sie von der ersten Bestandsaufnahme bis zur erfolgreichen Umsetzung.

consileon.de/cybersecurity

Lösungen für morgen. Heute.

Ihre Vision, unser Antrieb. Mit über 550 Mitarbeiterinnen und Mitarbeitern ist Consileon Ihr starker Partner für Top-Managementberatung sowie Lösungen mit IT- und KI-Bezug.

Wir unterstützen Sie von der Konzeption bis zur Umsetzung in allen Bereichen der Digitalisierung und helfen Ihnen dabei, wichtige Herausforderungen von morgen mit Technikkompetenz zu lösen.

→ mehr zum Thema: consileon.de/cybersecurity

CONSILEON