Marcel Küppers

Informations- und Cybersicherheit

Ein strategischer Praxis-Leitfaden für moderne CISOs und Security-Entscheider

mitp

Inhaltsverzeichnis

Kapitel 1

Einführung: Digitale Resilienz als Führungsaufgabe – Warum dieses Buch geschrieben wurde

Die Rolle der Informationssicherheit hat sich in den letzten Jahren fundamental gewandelt. In einer Ära, in der digitale Geschäftsmodelle zur Norm werden, Cyberbedrohungen zunehmend geopolitische Ausmaße annehmen und regulatorische Anforderungen exponentiell wachsen, ist die klassische Vorstellung von »IT-Sicherheit« als rein technischer Schutzmechanismus obsolet geworden. Sicherheit ist heute ein strategisches Steuerungselement – ein differenzierender Wettbewerbsfaktor, Risikopuffer und Innovationsmotor zugleich.

Dieses Kompendium richtet sich in erster Linie an Chief Information Security Officers (CISOs) und alle Entscheidungsträger, die moderne Sicherheitsprogramme gestalten, verantworten oder operationalisieren. Es vereint strategische Perspektiven, operative Best Practices und regulatorische Orientierungshilfen, um den komplexen Herausforderungen eines integrierten Cybersecurity-Managements gerecht zu werden.

Der moderne CISO ist nicht länger nur technischer Sicherheitsverantwortlicher, sondern ein Business Leader mit tiefem Verständnis für Geschäftsprozesse, Risikoportfolios und Unternehmensgovernance. Die Fähigkeit, Cybersicherheitsmaßnahmen in unternehmerischen Mehrwert zu übersetzen, ist zum zentralen Erfolgsfaktor avanciert. Sicherheit darf nicht mehr als Kostenfaktor wahrgenommen werden, sondern als Enabler für Wachstum, Innovation und Resilienz.

1.1 Ziel und Struktur dieses Buches

Digitale Resilienz beschreibt die Fähigkeit eines Unternehmens, auf digitale Bedrohungen nicht nur zu reagieren, sondern ihnen proaktiv zu begegnen, daraus zu lernen und gestärkt hervorzugehen. Diese Fähigkeit ist heute ein entscheidender Wettbewerbsfaktor

Doch wie operationalisiert man diesen abstrakten Begriff? Welche organisatorischen Modelle, technischen Architekturen, Rollenprofile und Metriken braucht es, um echte Resilienz zu gestalten? Hier kommt der CISO ins Spiel.

Dieses Buch liefert praxisnahe Antworten auf Fragen wie:

- Wie etabliere ich ein technologiegestütztes Governance-Modell für Informationssicherheit?
- Welche Architekturprinzipien brauche ich für eine Zero Trust-Strategie in einer hybriden Landschaft?
- Wie baue ich ein Detection Engineering-Team, das MITRE ATT&CK nicht nur kennt, sondern lebt?
- Wie verknüpfe ich Sicherheitsziele mit Business-KPIs?
- Wie plane ich den Aufbau eines SOC, das skalierbar, messbar und eng mit dem Business verzahnt ist?
- Wie integriere ich Threat Intelligence in operative Prozesse?
- Wie kann ich mich auf post-quantenkryptographische Bedrohungen vorbereiten?

Die Kapitel sind modular aufgebaut und folgen dem Lebenszyklus einer modernen Sicherheitsorganisation – von Strategie über Architektur und Betrieb bis zu Kultur und Kommunikation. Sie enthalten Frameworks, Metriken, Architekturansätze, Playbooks und Praxisbeispiele, die direkt anwendbar sind. Dieses Buch ist kein theoretisches Kompendium. Es ist ein Arbeitsmittel, ein Kompass und ein Sparringspartner für die anspruchsvollste Führungsrolle der digitalen Gegenwart: die des modernen CISO.

Hinweis

Aus verlagstechnischen Gründen konnten nicht alle Themen bzw nicht in voller Tiefe berücksichtigt werden – dazu zählen unter anderem Security Awareness Programme, Sicherheitskultur und Security Champions Programme, OT-Security oder IoT-Security. In einigen Kapiteln wird explizit auf die Webseite des Buches (www.cycademy.de/ciso-buch) hingewiesen, auf der sich ergänzende Kapitel, vertiefende Analysen und unterstützende Materialien befinden.

Um die im Buch behandelten Konzepte greifbar und praxisnah zu veranschaulichen, begleitet uns durch viele Kapitel ein fiktives Unternehmen: die Tecronix AG. Sie steht exemplarisch für die Realität vieler Industrieunternehmen, die sich mit

ähnlichen Herausforderungen konfrontiert sehen: steigende regulatorische Anforderungen, zunehmende IT-/OT-Konvergenz, wachsende Angriffskomplexität und zugleich hoher Innovationsdruck durch Digitalisierung und Globalisierung.

Die Tecronix AG ist keine theoretische Konstruktion, sondern bewusst so modelliert, dass sie typische Konfliktlinien, technologische Abhängigkeiten und sicherheitsstrategische Entscheidungen sichtbar macht. Ihre Geschäftsprozesse, Systemlandschaften und Risikoprofile dienen als roter Faden für die Umsetzung der in diesem Buch vorgestellten Methoden, Architekturen und Steuerungsmodelle.

1.2 Das fiktive Beispielunternehmen – Tecronix AG

Die Tecronix AG – ein Unternehmen mit 6.000 Mitarbeitenden, einer hybriden IT-Landschaft, Cloud-first-Strategie, produktionsnaher OT und weltweiter Marktpräsenz – ist ein exemplarisches Abbild der Herausforderungen, vor denen viele deutsche Mittelständler heute stehen. Das Unternehmen muss seine Sicherheitsarchitekturen transformieren, regulatorische Anforderungen (DSGVO, NIS2, TISAX) erfüllen, eine fragmentierte Tool-Landschaft konsolidieren und gleichzeitig seine Innovationsfähigkeit durch IIoT- und Cloud-Initiativen erhalten.

1.2.1 Geschäftstreiber & IT-Abhängigkeiten

Die Sicherheitsstrategie der Tecronix AG ist unmittelbar mit den Geschäftszielen und Wertschöpfungsketten des Unternehmens verknüpft. Folgende übergeordnete Business Driver wirken direkt auf Sicherheitsbedarfe und IT-Abhängigkeiten:

- Innovation durch Digitalisierung: Entwicklung smarter IIoT-Produkte und digitaler Serviceangebote (z. B. Predictive Maintenance, digitale Zwillinge) erfordert sichere Dev-, Integrations- und Betriebsplattformen.
- Produktionsverfügbarkeit & Just-in-Time-Fertigung: Produktionsausfälle durch IT-/OT-Störungen wirken sich direkt auf Lieferzusagen, Vertragsstrafen und Kundenbindung aus.
- Globalisierung & Marktzugang: Einhaltung internationaler Sicherheits- und Datenschutzstandards (z. B. TISAX, NIS2, DSGVO) ist Voraussetzung für OEM-Zulassung und Marktzugang.
- Vertrauenswürdigkeit gegenüber Kunden & Investoren: Sicherheit als Wettbewerbsvorteil – insbesondere bei Ausschreibungen und ESG-Berichterstattung.
- Agilität & Time-to-Market: DevOps-getriebene Entwicklung erfordert einen »Secure by Design«-Ansatz, der Geschwindigkeit und Sicherheit vereint.

1.2.2 Kritische Assets und Geschäftsprozesse

Die geschäftskritische Infrastruktur der Tecronix AG ist hochgradig digitalisiert und global vernetzt. Folgende Asset-Klassen und Prozesse stellen besonders hohe Schutzbedarfe:

- CAD- und Konstruktionsdaten: IP-Verlust, Plagiate, Entwicklungsverzögerungen.
- Produktionssteuerung (SCADA, SPS, MES): Produktionsausfälle, Wiederanlaufkosten.
- F&E-Simulationen & Embedded Software: Rückrufe, Produkthaftung, Compliance-Risiken.
- Digitale Zwillinge & PLM-Systeme: Kritisch für Predictive Maintenance und Produktlebenszyklen.
- SAP ERP & CRM: Risiken durch Betrug, Kompromittierung, Business Email Compromise.
- Remote Access Tools: Angriffsfläche bei fehlendem JIT-Zugriff oder fehlender Protokollierung.
- Kunden- und Zuliefererplattformen: Reputations- und Haftungsrisiken.
- Cloud-Workloads (z. B. Office 365, GitHub): Credential Stuffing, Token-Leaks.
- IAM & HR-Systeme: DSGVO-relevante Daten, Rollen- und Berechtigungsrisiken.

Vertiefung in der Praxis: Die CISO-Masterclass

Dieses Buch bildet die Grundlage für eine umfassende CISO Masterclass. In dieser Weiterbildung werden alle Themenfelder des Kompendiums – von Governance über Zero Trust bis Detection Engineering – in intensiven Praxis-Sessions, Fallstudien und interaktiven Übungen vertieft und in 1:1 Coaching Sessions am eigenen Unternehmen angewendet.

Die Masterclass richtet sich an CISOs, Sicherheitsarchitekten und Programmverantwortliche, die ihre Organisation strategisch und operativ auf das nächste Level heben wollen.

Mehr Informationen und Anmeldemöglichkeiten unter:

www.cycademy.de/ciso-masterclass

Kapitel 2

Rolle und Verantwortung eines modernen CISOs

Die Rolle des Chief Information Security Officer (CISO) entstand in vielen Unternehmen ursprünglich als Reaktion auf technologische Gefahren – Viren, Netzwerkwürmer, interne Regelverletzungen. Der erste bekannte CISO der Welt wurde 1994 bei Citigroup nach einem massiven Hack eingesetzt – seine Aufgabe: digitale Katastrophen vermeiden. In der Anfangsphase war die Rolle:

- in der IT angesiedelt
- primär auf Perimeterschutz (Firewalls, Antivirus) fokussiert
- von Compliance (z. B. SOX, PCI DSS, ISO 27001) getrieben

CISOs agierten oft als reaktive Problemlöser mit starkem Technikfokus – ohne Einfluss auf strategische Entscheidungsprozesse oder Geschäftsinnovationen.

In Zeiten digitaler Transformation, vernetzter Wertschöpfung und permanent verfügbarer Cloud-Infrastrukturen ist die Informationssicherheit nicht nur ein IT-Thema, sondern ein unternehmenskritischer Erfolgsfaktor.

Moderne CISOs sind keine reinen Technologieverwalter mehr. Sie sind Führungskräfte mit einem breiten Verantwortungsprofil, das von Governance über Security Engineering bis zur Krisenkommunikation reicht. Sie agieren an der Schnittstelle zwischen Geschäftsstrategie, technischer Komplexität und regulatorischen Anforderungen – und müssen dabei sowohl die technische als auch wirtschaftliche Sprache fließend beherrschen.

Mehrere Entwicklungen haben die CISO-Rolle grundlegend transformiert:

- Digitale Geschäftsmodelle:
  IT ist heute kein Hilfsmittel – sie ist das Geschäft. Ob Plattformökonomie, Cloud-ERP oder vernetzte Produktionsanlagen – jede Schwäche in der Cyber-Resilienz gefährdet das Geschäftsmodell selbst.
- Externe Bedrohungslandschaft:
  Vom Script-Kiddie zum APT: Bedrohungen sind heute hochprofessionell, geopolitisch und finanziell motiviert. Ransomware-Angriffe auf mittelständische Produzenten können innerhalb von Stunden Millionenverluste verursachen.

- Regulatorische Dynamik:
  Datenschutz-Grundverordnung (DSGVO), NIS2, DORA, KRITIS-VO, TISAX – die Anforderungen steigen, und Sicherheitsverantwortung ist nun rechtlich delegiert und haftbar.
- Öffentliches Vertrauen als Währung:
  Kunden, Partner und Investoren erwarten digitale Vertrauenswürdigkeit – Security-by-Design, Zertifizierungen und Transparenz.

Diese Entwicklungen machen aus dem CISO einen aktiven Gestalter von Geschäftssicherheit, Innovationsfähigkeit und digitalem Vertrauen – nicht mehr nur einen technischen Wächter.

Zu den klassischen Verantwortungsbereichen eines modernen CISOs gehören:

- Governance & Leadership
  - Entwicklung und Umsetzung der Informationssicherheitsstrategie
  - Aufbau und Pflege eines ISMS (z. B. nach ISO/IEC 27001)
  - Erstellung und Pflege der Policy-Landschaft (Policies, Standards, Guidelines)
  - Steuerung von Security-Gremien, Kommunikation mit Vorstand und Aufsichtsrat
- Risk Management & Compliance
  - Durchführung von Risikoanalysen und Business Impact Assessments (BIA)
  - Überwachung regulatorischer Anforderungen (z. B. DSGVO, NIS2, TISAX, LkSG)
  - Aufbau eines GRC-Frameworks inkl. Audit-, Reporting- und Kontrollsystem
  - Steuerung des Third-Party Risk Managements (TPRM)
- Security Architecture & Engineering
  - Vorgabe der Sicherheitsarchitektur (Zero Trust, Defense-in-Depth, Cloud Security)
  - Integration von Security in IT-, OT- und Cloud-Infrastrukturen
  - Förderung von »Secure by Design« im Softwareentwicklungsprozess (DevSecOps)
  - Steuerung technischer Programme: IAM, PAM, DLP, SIEM, SOC
- Operations & Incident Management
  - Aufbau und Leitung eines Security Operations Centers (SOC)
  - Definition und Betrieb des Incident Response Plans (inkl. Notfallmanagement)

  - Steuerung von Forensik, Threat Intelligence, Detection-as-Code
  - Reporting an Behörden im Fall von Security-Incidents (DSGVO, KRITIS etc.)
- Awareness, Schulung & Kultur
  - Entwicklung unternehmensweiter Awareness-Programme
  - Durchführung von Phishing-Simulationen, Schulungen, Rollentrainings
  - Etablierung einer »Security-First«-Kultur
  - Kommunikation von Sicherheitswerten und ethischem Verhalten
- Budgetierung & Performance Management
  - Planung und Steuerung des Security-Budgets
  - Aufbau von KPIs & Metriken zur Wirksamkeit des Programms
  - Nutzung von Maturity-Modellen (CMMI, NIST CSF) zur Leistungssteuerung
  - Berichtswesen gegenüber Controlling, Compliance und Audit

Moderne CISOs berichten heute nicht mehr zwingend an den CIO, sondern an:

- den CEO (strategischer Führungsanspruch)
- den CFO (Risiko- & Investitionsperspektive)
- oder sogar direkt an das Board/Audit Committee (Unabhängigkeit und Kontrollfunktion)

Dies signalisiert: Cybersecurity ist kein IT-Problem, sondern ein betriebswirtschaftliches und strategisches Risiko, vergleichbar mit Rechtsrisiken, Reputationsschäden oder Complianceverstößen.

Obwohl Bedrohungslage, Cloud-Technologie und Regulierung global sind, wird die Rolle des CISO nicht einheitlich verstanden. Sie ist stark von kulturellen Faktoren, Regulierungsumfeld, Corporate Governance-Traditionen und Branchenstandards geprägt.

Drei exemplarische Einflussfaktoren:

1. **Rechtlicher Rahmen:**
   In den USA kann der CISO bei einem Sicherheitsvorfall persönlich haftbar gemacht werden (siehe SEC-Regelung 2023). In der EU hingegen steht die kollektive Verantwortung stärker im Fokus (z. B. NIS2-Direktive: Verantwortung der Geschäftsleitung).
2. **Kulturelle Führungstraditionen:**
   In angelsächsischen Ländern ist es üblich, den CISO auf CxO-Ebene mit Budgethoheit anzusiedeln. In vielen mitteleuropäischen Unternehmen agiert der

CISO dagegen noch oft unterhalb der CIO-Ebene, mit eingeschränktem Einfluss.

3. **Organisationsreife und Marktdruck:**
   In regulierten Branchen wie Finanzwesen oder Pharma ist die CISO-Rolle global meist hoch entwickelt. In industriellen Mittelstandsbranchen (z. B. Maschinenbau) variieren Rollenbild und Ressourcen deutlich – insbesondere außerhalb der Headquarter-Zone.

Tabelle 2.1 stellt die typische CISO-Verortung und einige Besonderheiten des Rollenverständnisses in den Schlüsselregionen dar.

Region	Typische CISO-Verortung	Besonderheiten
DACH	Oft unterhalb CIO, steigender Trend zu CEO-Nähe	Traditionell technikorientiert, starke DSGVO-Fixierung
USA	CISO auf C-Level oder direkt unter CEO	Hoher Druck durch Regulierer (SEC, FTC), starke Business-Fokussierung
Frankreich	CISO oft dem Chief Risk Officer (CRO) unterstellt	Fokus auf Risikointegration, Datenschutzbehörden sehr aktiv
UK	CISO direkt an Board oder über Group Risk	Sehr starke Ausrichtung auf GRC-Integration und Business Enablement
Asien	CISO selten formell etabliert; starke Hierarchie	Entscheidungsträger sind CIOs, Security »integriert« in IT

Tabelle 2.1: Wahrnehmung des CISOs in Schlüsselregionen

Die Bedeutung und strategische Positionierung des CISOs sind auch entscheidende Faktoren, die das Vergütungspaket stark beeinflussen. Auch hier gibt es international gesehen große Diskrepanzen. Einen guten Überblick bietet der Global Chief Information Security Officer Organization and Compensation Survey[1].

Die heutige CISO-Rolle ist kein monolithischer Titel, sondern ein multifunktionales Rollenbündel. Je nach Unternehmensstruktur, Bedrohungslage, Reifegrad und regulatorischem Umfeld muss der CISO sich kontinuierlich zwischen vier Rollen bewegen – mit hoher Kontextsensitivität und Führungsstärke.

1. Technologe – Architekt der Resilienz

In seiner Rolle als Technologe begreift der CISO Sicherheitsarchitektur nicht als eine lose Sammlung von Tools oder punktuellen Maßnahmen, sondern als ein kohärentes, steuerbares Gesamtsystem. Dieses wirkt über sämtliche Technologie-Schichten hinweg – von Netzwerken und Multi-Cloud-Umgebungen über Identitäts- und Datenmanagement bis hin zu modernen Applikationslandschaften. Ziel

1 https://www.heidrick.com/-/media/heidrickcom/publications-and-reports/2024-global-ciso-organization-and-compensation-survey.pdf

ist es, eine widerstandsfähige Architektur zu schaffen, die Sicherheitsziele messbar unterstützt und dynamisch auf neue Bedrohungsszenarien reagiert.

Die Rolle des CISO verlangt in diesem Kontext kontinuierliche, technologiegestützte Selbstreflexion:

- Wie effektiv ist unsere Angriffserkennung über alle relevanten Domänen hinweg – insbesondere Endpoint, OT, Cloud und SaaS?
- Wie reif und konsistent ist unsere IAM-Architektur, insbesondere im Hinblick auf föderierte Identitäten, privilegierten Zugriff und Secrets-Management?
- Ist Zero Trust bei uns ein gelebtes Architekturprinzip – oder bleibt es ein rein rhetorisches Versprechen?

Die technologische Realität heutiger Unternehmen ist geprägt von rasant wachsender Komplexität: Kubernetes-basierte Workloads, hybride und Multi-Cloud-Infrastrukturen, stark vernetzte SaaS-Landschaften und der Betriebstechnologie-Sektor (OT) erzeugen ein hochdynamisches, verteiltes Systemgefüge. In diesem Spannungsfeld muss der CISO nicht nur über tiefes technisches Verständnis verfügen, sondern auch in der Lage sein, diese Komplexität auf strategische Steuerungspunkte zu abstrahieren.

Die Kunst liegt darin, operative Resilienz mit architektonischer Klarheit zu verbinden – durch Prinzipien wie deklarative Sicherheit, Policy-as-Code, Identitätszentrierung und verteidigungsfähige Netzwerke. Nur wer Technik und Strategie integriert denkt, kann Sicherheitsarchitekturen schaffen, die nicht nur heutigen, sondern auch zukünftigen Bedrohungen standhalten.

2. Risikomanager – Lotse im Entscheidungsozean

Als Risikomanager agiert der CISO als Übersetzer zwischen technischer Komplexität und geschäftlicher Entscheidungsfähigkeit. Seine Kernaufgabe besteht darin, Sicherheitsrisiken nicht isoliert zu betrachten, sondern diese in den Kontext strategischer und operativer Unternehmensziele zu stellen. Hierzu setzt er auf strukturierte, standardbasierte Risikoanalyse-Methoden – etwa FAIR (Factor Analysis of Information Risk) für quantitative Modelle, ISO/IEC 27005 für risikobasierte Steuerung oder das NIST Risk Management Framework (RMF) zur Integration in unternehmensweite Governance-Strukturen.

Im Zentrum steht nicht nur die Identifikation und Bewertung von Bedrohungen, sondern die Fähigkeit, Entscheidungsträgern belastbare, nachvollziehbare und wirtschaftlich sinnvolle Handlungsempfehlungen bereitzustellen. Dabei zählen nicht nur CVSS-Scores, sondern insbesondere:

- Geschäftsrelevanz der betroffenen Assets (z. B. Umsatzbeitrag, regulatorische Kritikalität)
- Wirksamkeit vorhandener Kompensationsmaßnahmen

- Zeitfenster der Exponierung und Angriffswahrscheinlichkeit
- Risikoentwicklung im Zeitverlauf (Trendanalysen, Szenarien)

Die zentrale Herausforderung liegt darin, technische Fachexpertise in konsistente, wiederholbare und entscheidungsfähige Risikobilder zu überführen – in einem Umfeld, das geprägt ist von Unsicherheit, schnellen Bedrohungszyklen und komplexen Abhängigkeiten. Der CISO muss Risikomanagement als Business-Funktion etablieren, die genauso robust und verlässlich agiert wie Finanzen oder Supply Chain – mit klar definierten Schwellenwerten, Eskalationspfaden und Governance-Prozessen.

Beispiel

Ein kritisches SAP-System zur Steuerung der globalen Lieferkette weist eine ungepatchte Schwachstelle mit CVSS 10 auf. Der CISO isoliert die technische Lücke nicht, sondern analysiert das Geschäftsrisiko im Zusammenhang: Welche Umsatzströme hängen von diesem Modul ab? Welche Sicherheitskontrollen (z. B. Netzsegmentierung, Monitoring) wirken kompensierend? Welche Angriffsvektoren sind realistisch? Er modelliert das Risiko auf Basis eines FAIR-Modells, quantifiziert potenzielle Verlustszenarien in Euro und legt dem CFO eine klar strukturierte Entscheidungsunterlage mit drei Alternativszenarien vor – jeweils mit zugehörigen Kosten, Restrisiken und Umsetzungshorizonten.

3. Führungskraft und Teambuilder

In seiner Rolle als Führungskraft steht der CISO vor einer doppelten Herausforderung: Er muss einerseits technologisch hochqualifizierte Spezialistenteams wie Detection Engineers, Cloud Security Architects oder IAM-Strategen führen – andererseits ist er verantwortlich für die Gestaltung und Steuerung tiefgreifender organisationaler Veränderungen in Richtung eines resilienten, sicherheitsbewussten Unternehmens.

Der moderne CISO agiert dabei nicht als operativer Dirigent im Tagesgeschäft, sondern als architektonischer Impulsgeber für Struktur, Kultur und Kompetenzaufbau. Er versteht, dass nachhaltige Sicherheit nicht allein durch Technologie entsteht, sondern durch menschenzentrierte Führungsmodelle und eine wirksame Veränderungsarchitektur.

Konkret bedeutet das:

- Aufbau dezentraler Security Chapter Leads in den Business Units, die als Bindeglieder zwischen zentraler Security Governance und operativer Verantwortung fungieren.

- Etablierung eines Security Champions Programms, das Sicherheitsverantwortung in Produktteams verankert, kontinuierliches Lernen fördert und Peer-to-Peer-Einfluss nutzbar macht.
- Design agiler Security Operating Modelle, etwa angelehnt an das SAFe-Framework oder das Spotify-Modell, um Security als integralen Bestandteil iterativer Produktentwicklung zu verankern – inklusive klarer Rollen, Feedback-Zyklen und Entscheidungslogiken.

Die besondere Schwierigkeit liegt in der Führung durch Einfluss statt durch Hierarchie. Der CISO agiert oft ohne disziplinarische Weisungsbefugnis, muss aber dennoch kulturellen Wandel vorantreiben – in Umgebungen, die durch Silodenken, Veränderungsresistenz oder Misstrauen gegenüber zentraler Governance geprägt sind.

Hier sind ausgeprägte Fähigkeiten in transversaler Führung, interner Allianzbildung und strategischer Kommunikation gefragt. Der CISO muss narrative Kohärenz schaffen – das »Warum« der Security greifbar machen – und gleichzeitig Räume schaffen, in denen Sicherheit nicht als Blockade, sondern als Enabler verstanden wird.

4. Kommunikator – Übersetzer, Vermittler, Trusted Advisor

Der CISO bewegt sich täglich zwischen zwei Welten: technologischer Tiefenschärfe auf der einen und strategischer Kommunikation auf C-Level auf der anderen. In dieser Vermittlerrolle agiert er nicht nur als Experte, sondern als vertrauenswürdiger Berater für Vorstand, Kunden, Behörden und regulatorische Gremien. Sein Kommunikationsstil prägt die Glaubwürdigkeit der Sicherheitsfunktion – insbesondere in Krisenzeiten, bei Prüfungen oder bei strategischen Investitionsentscheidungen.

Ob in Vorstandsausschüssen, mit Aufsichtsräten oder gegenüber externen Stakeholdern: Der CISO muss ruhig, faktenbasiert und verständlich kommunizieren können – ohne in technische Detailverirrungen abzudriften, aber stets vorbereitet auf fundierte Rückfragen.

Gerade in stressbeladenen Kontexten – bei Incidents, Audit Findings oder medial begleiteten Angriffen – ist die kommunikative Fähigkeit des CISO entscheidend. Gefordert sind:

- Konsistenz in der Darstellung über alle Kommunikationskanäle hinweg
- Souveräne Ruhe, auch bei unvollständiger Informationslage
- Narrative Struktur, die Vertrauen erzeugt – nicht Panik

Der CISO muss in der Lage sein, hochkomplexe Sachverhalte auf die relevante Entscheidungsebene herunterzubrechen, ohne Substanz zu verlieren – und dabei sowohl Transparenz als auch Lösungskompetenz auszustrahlen.

Die beschriebenen vier Rollen – Technologe, Risikomanager, Führungskraft und Kommunikator – sind keine voneinander getrennten Silos. Vielmehr bilden sie ein integriertes Kompetenz- und Rollenmodell, das der moderne CISO situationsabhängig, aber konsistent bespielen muss. Die Herausforderung liegt nicht nur im Beherrschen jeder einzelnen Disziplin, sondern im schnellen, kontextsensiblen Wechsel zwischen ihnen – oft innerhalb eines einzigen Meetings.

Ein typischer Arbeitstag verlangt vom CISO, in wenigen Stunden von einem technischen Incident-Review in ein Audit-Briefing zu wechseln, anschließend eine Budgetverhandlung mit dem CFO zu führen und danach ein Security Awareness-Format mit Product Leads zu moderieren. Jeder dieser Kontexte stellt andere Anforderungen an Sprache, Argumentationsstil, Prioritäten – doch alle erfordern eine einheitliche strategische Linie.

Der CISO der Gegenwart bewegt sich sicher und souverän in einem dynamischen Spannungsfeld, das sich durch fundamentale Zielkonflikte auszeichnet:

- Technischer Drilldown vs. Strategische Abstraktion:
- Der CISO muss in der Lage sein, technische Risiken bis zur Root-Cause zu analysieren – gleichzeitig aber diese Erkenntnisse in eine verdichtete, entscheidungsfähige Form für die Geschäftsleitung zu übersetzen.
- Kontrolle & Policies vs. Befähigung & Kulturwandel:
- Während robuste Kontrollsysteme und klare Richtlinien essenziell bleiben, erkennt der CISO, dass nachhaltige Sicherheit nur durch Empowerment, Ownership und kulturelle Verankerung entsteht.
- Kostendruck vs. Investition in Vertrauen:
- Sicherheit wird oft als Kostenstelle betrachtet. Der CISO muss deshalb glaubwürdig aufzeigen, wie Investitionen in Resilienz, Verfügbarkeit und Compliance langfristig Vertrauen bei Kunden, Investoren und Aufsichtsbehörden schaffen – und somit geschäftskritisch sind.

Diese multidimensionale Führungsrolle erfordert nicht nur Fachkompetenz, sondern strategische Reife, kommunikative Exzellenz und kulturelle Wirksamkeit. Der CISO ist heute nicht mehr nur Sicherheitsmanager – er ist ein Business-Leader mit Sicherheitsverantwortung.

Um diese immer herausfordernde Rolle erfolgreich ausführen zu können, sollte ein moderner CISO folgende Schlüsselkompetenzen mitbringen:

- Technische Tiefe und Architekturverständnis
- Fundierte Kenntnisse in Netzwerksicherheit, Cloud Security, OT/ICS, IAM

- Verständnis moderner Architekturmuster (Zero Trust, Microsegmentation, DevSecOps)
- Fähigkeit zur Bewertung und Steuerung technischer Plattformen, z. B. SIEM, EDR, DLP, PAM
- Strategische und analytische Denkweise
- Entwicklung geschäftsorientierter Sicherheitsstrategien
- Risikobasierte Priorisierung von Maßnahmen (z. B. mittels BIA, FAIR)
- Steuerung über KPIs, Maturity Scores und Capability Assessments
- Kommunikations- und Führungsstärke
- Überzeugende Kommunikation auf Vorstandsebene (»Übersetzerfunktion« Technik ↔ Business)
- Führen interdisziplinärer Teams (Security Engineering, GRC, Awareness)
- Konfliktfähigkeit, Stakeholder-Management, Schulungs- und Coaching-Kompetenz
- GRC- und Regulatorik-Expertise
- Profundes Wissen zu ISO 27001, NIS2, DSGVO, TISAX, LkSG
- Erfahrung in Auditprozessen, Policy-Entwicklung, Datenschutz
- Fähigkeit zur Steuerung interner/externer Prüfungen und Maßnahmenverfolgung
- Change- und Projektmanagement
- Steuerung von Transformationsinitiativen (z. B. SOC-Aufbau, IAM-Neuorganisation)
- Agiles Projektmanagement (Scrum, SAFe)
- Programmmanagement und Steuerung multidisziplinärer Projekte
- Kulturelle & ethische Führungsrolle
- Aufbau einer Sicherheitskultur (»Security as Shared Responsibility«)
- Integrität, Ethik, Vorbildfunktion in sensiblen Entscheidungssituationen
- Umgang mit Whistleblowern, Datenschutzfällen, medialen Incidents

In der heutigen Wirtschaftswelt ist nahezu jedes Unternehmen ein digitales Unternehmen – insbesondere im industriellen Mittelstand, wo Produktionsprozesse, F&E und Logistik stark IT-gestützt ablaufen. Cybersecurity darf daher nicht isoliert als technische Disziplin betrachtet werden, sondern muss tief in das Geschäftsmodell und die Wertschöpfung integriert sein.

Der moderne CISO ist Gestalter und Risikomanager zugleich. Er muss Bedrohungen antizipieren, geschäftliche Risiken priorisieren, Ressourcen effektiv steuern und das Vertrauen aller Stakeholder sichern. Nur so wird aus Sicherheit ein echter Wettbewerbsfaktor.

Kapitel 3

Security als Business Enabler – vom Kostenfaktor zur Wertschöpfung

In der Vergangenheit wurde IT-Sicherheit oft primär als »notwendige Kostenstelle« betrachtet – getrieben durch regulatorische Anforderungen, Incident-Prävention und Auditfähigkeit. Dieses Bild greift im Zeitalter digitaler Geschäftsmodelle jedoch zu kurz. Moderne Security-Funktionen entwickeln sich zunehmend zu aktiven Werttreibern, die nicht nur Risiken kontrollieren, sondern konkret zur Umsatzsicherung, Markterschließung, Kundenbindung und Innovationsfähigkeit beitragen.

Indem Security von Beginn an in Produkte, Prozesse und Partnerschaften integriert wird, entsteht ein strategisches Differenzierungsmerkmal – etwa durch Compliance-zertifizierte Plattformen, Privacy-by-Design als Verkaufsargument oder Zero Trust als vertrauensbildendes Governance-Versprechen. Die wirtschaftliche Wirkung lässt sich heute messen: über Umsatzbeiträge, Auditbeschleunigung, vermiedene Vorfälle oder gesteigerte Renewal Rates.

Dieses Kapitel zeigt, wie Security vom passiven Kostenblock zum aktiven Geschäftsfaktor transformiert wird – mit konkreten Hebeln, Messmodellen und Umsetzungsarchitektur.

3.1 Der Paradigmenwechsel: Vom Schutz zur Befähigung

Traditionell wurde Informationssicherheit als Kostenstelle betrachtet – ein Bereich, der Kosten verursacht, Risiken eindämmt, aber wenig zum Umsatz oder zur Innovation beiträgt. Diese Sichtweise ist mittlerweile überholt. Im Zeitalter der digitalen Transformation ist Cybersecurity zur Grundvoraussetzung geschäftlicher Handlungsfähigkeit geworden.

Sicherheitsarchitektur, Datenschutz, Resilienz und Compliance sind keine reaktiven Schutzmaßnahmen mehr, sondern aktive Werttreiber:

Sie ermöglichen die sichere Einführung neuer Technologien (z. B. IIoT, Cloud, KI).

Sie sind Voraussetzung für regulatorische Zulassungen, Audits und Marktteilnahmen (z. B. TISAX, ISO 27001).

Sie schützen Reputation, Betriebsfähigkeit und Innovationsgeschwindigkeit.

In der ersten Phase der IT-Sicherheit – von den frühen 1990er Jahren bis etwa 2010 – dominierte ein technikorientiertes Verständnis von Sicherheit:

- Ziel war die Abwehr von Bedrohungen (z. B. Viren, Malware, interne Fehlbedienung).
- Maßnahmen waren reaktiv, oft durch Audits oder Compliance-Anforderungen getrieben.
- Security war abgekoppelt vom Business – häufig organisatorisch der IT oder dem Legal-Bereich unterstellt.

Typische Symptome dieser Ära: verspätete Einbindung, lange Freigabeschleifen, Blockadewahrnehmung (»Die Security-Leute sagen wieder Nein«), Zero-Innovation-Haltung (»Lieber sicher als schnell«).

Mehrere strukturelle Veränderungen erzwingen einen Paradigmenwechsel:

1. Digitale Geschäftsmodelle sind allgegenwärtig
   IT und OT sind das Rückgrat fast aller Wertschöpfungsprozesse (Cloud, IIoT, SaaS, KI).
2. Kunden und Investoren verlangen Sicherheit als Voraussetzung
   Sicherheit ist nicht mehr optional – sie ist Zugangskriterium zu Märkten, Kapital und Vertrauen.
3. Cyberbedrohungen sind dynamisch, adaptiv, wirtschaftlich motiviert
   Klassische Verteidigung reicht nicht, Resilienz und schnelle Reaktion sind essenziell.
4. Regulierungen verlangen Führung & Steuerung
   NIS2, DORA, TISAX, BSI IT-SiG fordern »Cyber Governance« auf Top-Management-Level.

Moderne Sicherheit ist kein Stoppzeichen, sondern ein Qualitätssiegel. Ihr Ziel ist es:

- Geschäftsinitiativen frühzeitig sicher zu ermöglichen, statt sie nachträglich zu kontrollieren
- Innovation sicher zu beschleunigen, nicht zu verlangsamen
- Risiken in strukturierte Entscheidungsgrundlagen zu transformieren, nicht in Angst

Dabei gilt: Eine Sicherheitsmaßnahme ist nur so wertvoll wie ihr Beitrag zur unternehmerischen Handlungsfähigkeit.

Praxisbezug Tecronix AG

Für ein Industrieunternehmen wie Tecronix AG mit globaler Lieferkette, Cloud-basierten IIoT-Produkten und OT-gestützter Produktion bedeutet dieser Wandel konkret:

- Security-by-Design für digitale Produkte (Secure DevOps, SBOM, API Hardening)
- Cloud-Migration mit CSPM und Zero Trust Foundation, statt ex-post Prüfungen
- OT-Integration mit Segmentierung und Asset Monitoring, statt Security durch Isolation
- Lieferantenabsicherung durch TPRM-Programme, statt Risikoakzeptanz auf dem Papier

Für den modernen CISO können daraus einige Verhaltensprinzipien abgeleitet werden, die innerhalb des neuen Paradigmas entscheidend sind:

- Frühzeitigkeit: Sicherheit beginnt bei der Projektidee, nicht beim GoLive.
- Business Alignment: Sicherheitsziele sind nur sinnvoll, wenn sie auf Geschäftsprioritäten einzahlen.
- Partnerschaft: Der CISO fungiert als Enabler, nicht als Gatekeeper – aktive Begleitung statt Kontrolle.
- Risikoübersetzung: Technische Schwächen werden in Business-Szenarien dargestellt.

Sicherheit ist heute grundlegender Bestandteil der Wettbewerbsfähigkeit. Nur wenn sie in Geschäft, Produkt und Transformation integriert ist, entfaltet sie ihren vollen Wert. Der CISO muss diesen Wandel nicht nur begreifen – er muss ihn treiben, verkörpern und methodisch verankern.

3.2 Vier strategische Wirkdimensionen von Security

Ein moderner CISO muss Sicherheitsmaßnahmen nicht als Pflichtaufgabe, sondern als Wertbeitrag zum Geschäft formulieren. Dies kann über vier strategische Wirkachsen gelingen.

Stichwortverzeichnis

T

U

V

W

Y

Z