

Marcel Küppers

Informations- und Cybersicherheit

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



Inhaltsverzeichnis

1	Einführung: Digitale Resilienz als Führungsaufgabe – Warum dieses Buch geschrieben wurde	15
1.1	Ziel und Struktur dieses Buches	15
1.2	Das fiktive Beispielunternehmen – Tecronix AG	17
1.2.1	Geschäftstreiber & IT-Abhängigkeiten	17
1.2.2	Kritische Assets und Geschäftsprozesse	18
2	Rolle und Verantwortung eines modernen CISOs	19
3	Security als Business Enabler – vom Kostenfaktor zur Wertschöpfung	29
3.1	Der Paradigmenwechsel: Vom Schutz zur Befähigung	29
3.2	Vier strategische Wirkdimensionen von Security	31
3.3	Methoden zur Positionierung von Security als Enabler	37
3.4	Handlungsempfehlungen	48
3.5	Referenzen	57
4	Security-Organisation und Stakeholder-Management	59
4.1	Aufbau einer modernen Security-Organisation	61
4.1.1	Leitprinzipien moderner Security-Organisationen	61
4.1.2	Zielbild: Das »Security Office« als Steuerzentrale der Unternehmenssicherheit	62
4.2	Organisatorische Verankerung der CISO-Funktion	81
4.3	Organisatorische Skalierung und Personalstruktur	84
4.4	Stakeholder Management	87
4.4.1	Stakeholder-Karte definieren: Wer ist entscheidend für Security-Erfolg?	87
4.4.2	Kommunikationsmodelle für unterschiedliche Zielgruppen	90
4.4.3	Erwartungsmanagement: Proaktiv statt reaktiv führen	95
4.4.4	Transparenz durch KPIs, Dashboards und Storytelling	98
4.5	Umsetzung bei der Tecronix AG	100
4.6	Referenzen	102

5	Security-Governance-Modelle	103
5.1	Begriffsabgrenzung und Zielsetzung	103
5.2	Zentrales Governance-Modell	105
5.3	Föderiertes Governance-Modell	108
5.4	Vergleich zentraler und föderierter Governance-Modelle	111
5.5	Hybride Governance-Modelle	112
5.6	Handlungsempfehlungen für CISOs bei der Etablierung effektiver Governance-Modelle	115
5.7	Fazit: Governance als strategischer Enabler	117
5.8	Umsetzung bei Tecronix AG	118
5.9	Referenzen	120
6	Security-Strategieentwicklung und Maturity Roadmapping	121
6.1	Elemente einer integrierten Security-Strategie	122
6.2	Der Weg zur Strategie: Vorgehensmodell für CISOs	126
6.2.1	Analysephase – Ausgangslage bewerten	126
6.2.2	Zielbilddefinition – Wohin soll die Sicherheitsfunktion sich entwickeln?	127
6.2.3	Gapanalyse & Initiativenbildung – Was fehlt, um das Ziel zu erreichen?	129
6.2.4	Roadmap-Entwicklung – Wie sieht der Umsetzungsplan aus?	130
6.2.5	Verankerung und Kommunikation – Wie wird die Strategie gelebt?	132
6.3	Maturity Roadmapping: Vom IST zum SOLL	134
6.3.1	Maturity Model Design: Steuerbarkeit durch Capabilities und Reifegrade	134
6.3.2	Roadmap-Strukturierung: Von Quick Wins zu struktureller Resilienz	137
6.3.3	Verankerung in der Unternehmenssteuerung	139
6.4	Umsetzung bei der Tecronix AG	141
6.5	Referenzen	149
7	Vergleich moderner Cybersecurity-Frameworks – NIST CSF 2.0, ISO/IEC 27001:2022, CIS Controls v8	151
7.1	Framework-Profil im Überblick	151
7.2	Vergleich nach Schwerpunkten	153
7.3	Auswahlkriterien für die Framework-Nutzung	154
7.4	Best Practices für den Framework-Einsatz	159
7.5	Umsetzung bei der Tecronix AG	162
7.6	Referenzen	165

8	Risikomanagement mit dem FAIR-Modell – Quantifizierung digitaler Risiken	167
8.1	Grundlagen des FAIR-Modells	168
8.2	Der FAIR-Analyseprozess in der Praxis	169
8.3	FAIR im Kontext der Unternehmenssteuerung	173
8.4	Grenzen und Herausforderungen des FAIR-Modells	174
8.5	Anwendung bei der Tecronix AG	177
8.6	Referenzen	181
9	Interne Kontrollsysteme (IKS) & Audit-Readiness	183
9.1	Was ist ein Internes Kontrollsystem (IKS)?	184
9.2	Die fünf Kernelemente eines CISO-orientierten IKS	185
9.3	IKS-Typen in der Praxis	188
9.4	Audit-Readiness als Dauerzustand	190
9.5	Integration von IKS und DevSecOps – »Controls as Code«	193
9.6	Kontrollkataloge – Strategische Auswahl für ein CISO-orientiertes IKS	196
9.7	CISO-Metriken für IKS und Audit-Readiness	200
9.8	Umsetzung bei der Tecronix AG	202
9.9	Referenzen	204
10	DSGVO, TISAX, NIS2, KRITIS-VO, DORA – Anforderungen und Umsetzung in modernen Sicherheitsprogrammen	207
10.1	DSGVO – Datenschutz-Grundverordnung	208
10.2	TISAX – Trusted Information Security Assessment Exchange	210
10.3	NIS2 – EU-Richtlinie zur Netz- und Informationssicherheit	213
10.4	KRITIS-VO – Verordnung zur Bestimmung Kritischer Infrastrukturen	216
10.5	DORA – Digital Operational Resilience Act	219
10.6	Fazit	222
10.7	Referenzen	222
11	Drittparteien- und Lieferantenrisikomanagement	225
11.1	Ziele und Prinzipien	225
11.2	TPRM-Lifecycle-Modell	226
11.3	Werkzeuge und Metriken	229
11.4	Umsetzung bei der Tecronix AG	231

12	Zero-Trust-Architektur für hybride Infrastrukturen	237
12.1	Einleitung	237
12.1.1	Herausforderungen traditioneller Sicherheitsmodelle	237
12.1.2	Ziele und Nutzen von Zero Trust	237
12.2	Grundprinzipien von Zero Trust	238
12.3	Architekturübersicht	241
12.3.1	Zielarchitektur und Designprinzipien	241
12.3.2	Rollenmodell: PDP, PEP, Policy Engine	241
12.3.3	Interaktionsmodell: Benutzer, Geräte, Anwendungen, Daten	242
12.3.4	High-Level Referenzarchitektur	242
12.3.5	Integration in bestehende Infrastruktur	243
12.4	Technologische Komponenten	244
12.4.1	Identitäts- und Zugriffsmanagement (Identity & Access Management)	244
12.4.2	Gerätezustand und Endpoint Security	245
12.4.3	Netzwerk- und Anwendungskontrollen	246
12.4.4	Datenzugriffs- und Klassifizierungsmechanismen	248
12.4.5	Protokollierung, Monitoring und Detection	250
12.5	Implementierungsstrategie	251
12.5.1	Reifegradmodell und Initialbewertung	251
12.5.2	Phasenmodell der Einführung	252
12.5.3	Governance, Rollen und Verantwortlichkeiten	253
12.5.4	Erfolgsfaktoren und typische Stolpersteine	254
12.5.5	Messung des Fortschritts	254
12.5.6	Use Cases und Szenarien	255
12.5.6	Risiken und Herausforderungen	257
12.5.6	KPIs und Erfolgsmetriken	260
12.5.5	Fazit und Handlungsempfehlungen	261
12.6	Referenzen	269
13	Identitäts- und Zugriffsmanagement im Zeitalter von Zero Trust – IAM, PAM und CIEM in modernen Unternehmen	271
13.1	Strategische Bedeutung von IAM	273
13.2	Komponenten eines modernen IAM-Ökosystems	274
13.3	Zugriffskontrollmodelle	277
13.4	Privileged Access Management (PAM)	280
13.5	Cloud Infrastructure Entitlement Management (CIEM)	284
13.6	CIEM in der Praxis	285

14	Cloud Security (AWS, Azure, SaaS-Modelle)	291
14.1	Strategischer Kontext moderner Cloud-Sicherheit	291
14.2	Cloud Security Governance und Architektur	294
14.3	AWS-spezifische Sicherheitsaspekte	301
14.4	Azure-spezifische Sicherheitsaspekte	303
14.5	SaaS Security Governance – Strategien und Kontrollen für Microsoft 365, Salesforce & Co.	310
14.6	Metriken und KPIs für Cloud Security	315
14.7	Cloud Security Governance und Architektur – Praxisbeispiel Tecronix AG	317
15	Secrets Management & Credential Hygiene	321
15.1	Einleitung	321
15.2	Strategische Bedeutung: Secrets als Hochrisiko-Angriffsvektor	322
15.3	Grundlagen: Was zählt als »Secret« – und wie entstehen daraus Sicherheitsrisiken?	323
15.4	Technische und organisatorische Kontrollmaßnahmen	324
15.4.1	Architektur eines Secrets Management Stack	326
15.5	Operative Best Practices für Security Teams	327
15.5.1	Für CISOs und Architekten	328
15.5.6	Für DevOps und Engineering-Teams	330
15.5.6	Best Practices je Secret-Typ	331
15.6	Credential Hygiene – Beyond Secrets	332
15.7	Governance & Audit	334
15.7.1	Kontrollfragen für interne Audits	334
15.7.2	Maturity-Modell für Secrets Management	336
15.8	Fazit: Geheimnisse brauchen System – nicht Gewohnheit	337
15.9	Umsetzung bei der Tecronix AG: Enterprise-Ready Secrets Management in der Praxis	338
15.10	Referenzen	342
16	Moderne Application Security – Strategien für den CISO	345
16.1	Strategische Rolle der Application Security	345
16.2	Kernbausteine der Application Security	346
16.2.1	Static Application Security Testing (SAST)	347
16.2.2	Dynamic Application Security Testing (DAST)	348
16.2.3	Runtime Application Self-Protection (RASP)	350
16.2.4	Software Composition Analysis (SCA)	352
16.2.5	Software Bill of Materials (SBOM)	354
16.3	Governance & KPIs im Application Security Programm	356
16.4	Integration in DevSecOps	359
16.5	Reifegradmodell für Application Security	362

16.6	Fazit: Application Security als strategische Disziplin	364
16.7	Umsetzung bei der Tecronix AG	366
16.8	Referenzen	370
17	Aufbau und Betrieb eines Security Operations Centers (SOC)	371
17.1	Strategische Zielsetzung eines SOC	371
17.2	Typologie von SOC-Modellen	372
17.3	Aufbauphasen eines SOC	373
17.4	Betrieb und kontinuierliche Verbesserung	378
17.5	Governance und Steuerung	380
17.5.1	Strategisches Operating Model	381
17.5.2	Steuerungs- und Kommunikationsstrukturen	382
17.5.3	Compliance und Audit Readiness	383
17.5.4	Risiko- und Performance-Monitoring	384
17.5.5	Integration in das Unternehmens-ISMS	385
17.6	Wirtschaftlichkeit und Return on Security Investment (ROSI)	386
17.6.1	Kostenstrukturen eines SOC	387
17.6.2	Nutzenkategorien	388
17.6.3	Return on Security Investment (ROSI) Modellierung	389
17.6.4	Wirtschaftliche Optimierungsstrategien	391
17.6.5	Kommunikation mit Management und Controlling	392
17.7	Ausblick: SOC der Zukunft	393
17.7.1	AI- und ML-gestützte Anomalie-Erkennung	393
17.7.2	Automatisierung auf allen Ebenen	394
17.7.3	Threat-led SOC	395
17.7.4	Integration von OT-/ICS-Umgebungen	397
17.7.5	Relevante Modelle zur Reifegradmessung	399
17.7.6	Fazit	400
18	SIEM, UEBA, SOAR – Einsatz und Optimierung	405
18.1	Einleitung	405
18.2	SIEM – Fundament der Security Monitoring Architektur	406
18.3	UEBA – Frühwarnsystem für untypisches Verhalten	419
18.4	SOAR – Automatisierung & Orchestrierung der Reaktion	423
18.5	Referenzen	432
19	Detection Engineering und Threat Hunting im modernen Security Operations Framework	435
19.1	Detection Engineering: Prinzipien & Praxis	435
19.2	Threat Hunting: Proaktive Erkennung jenseits der Alarme	444
19.3	Detection Engineering & Threat Hunting bei Tecronix AG	457
19.4	Referenzen	460

20	Incident Response	463
20.1	Governance & Organisatorischer Rahmen	463
20.2	Incident Response Lifecycle: NIST, ENISA und BSI im Vergleich	469
20.3	Regulatorische Anforderungen an Incident Response	469
20.3.1	Europäische und nationale Rechtsgrundlagen	470
20.3.2	Branchenspezifische Regulierungen	470
20.4	Kommunikation, Reporting & Reputationsmanagement	474
20.5	Kontinuierliche Verbesserung & Resilienzaufbau	480
20.5.1	KPIs & Metriken	481
20.5.2	Red Teaming & Purple Teaming	481
20.5.3	Tabletop Exercises	482
20.6	Incident Response bei Tecronix AG	483
20.7	Referenzen	484
21	Cyber Threat Intelligence (CTI)	487
21.1	Einleitung	487
21.2	Begriff und Zielsetzung von Cyber Threat Intelligence	488
21.3	CTI-Arten	489
21.4	CTI-Prozessmodell	491
21.5	Datenquellen und Analyseverfahren	497
21.5.1	Datenquellenkategorien	498
21.5.2	Analyseverfahren	498
21.6	Integration in Sicherheitsprozesse	500
21.7	CTI-Plattformen, Standards und Austauschformate	504
21.7.1	STIX (Structured Threat Information Expression)	504
21.7.2	TAXII (Trusted Automated Exchange of Indicator Information)	505
21.7.3	MISP (Malware Information Sharing Platform & Threat Sharing)	506
21.7.4	Threat Intelligence Platforms (TIP)	507
21.8	Regulatorische Anforderungen an CTI	508
21.8.1	ISO/IEC 27001 (2022-Revision) – A.5.7 Threat Intelligence	509
21.8.2	NIS2-Richtlinie (EU 2022/2555) – Anforderungen an Threat Intelligence	510
21.8.3	TISAX (Trusted Information Security Assessment Exchange)	511
21.8.4	KRITIS-VO (DE) und IT-Sicherheitsgesetz 2.0	512
21.8.5	DORA (Digital Operational Resilience Act)	513
21.9	Einführung eines CTI-Programms	514
21.10	Fazit und Ausblick	521
21.11	Referenzen	522

22	Business Continuity & Disaster Recovery (BC/DR)	525
22.1	Strategische Bedeutung von BC/DR im Unternehmenskontext ...	526
22.2	Frameworks & Standards für Business Continuity & Disaster Recovery	528
22.3	Komponenten eines modernen BC/DR-Programms	530
22.3.1	Business Impact Analyse (BIA)	531
22.3.2	Risikoanalyse im Kontext von BC/DR	533
22.3.3	Wiederherstellungsstrategien	537
22.3.4	Notfallpläne (Contingency & Response Plans)	540
22.3.5	Governance & Dokumentation im BC/DR-Programm	544
22.4	Die Rolle des CISO	547
22.5	KPIs & Metriken	549
22.6	Umsetzung bei der Tecronix AG	551
22.7	Referenzen	553
23	Schulungen und Qualifizierungsstrategien im modernen Sicherheitsprogramm	555
23.1	Zielgruppen und Rollen	556
23.2	Aufbau eines rollenbasierten Schulungsprogramms	558
23.3	Integration in das Sicherheitsprogramm	561
23.4	Framework-Referenzen	563
23.5	Fazit	567
23.6	Referenzen	567
24	Künstliche Intelligenz im Kontext der Cybersecurity	569
24.1	Bedrohungen durch KI – Offensive Nutzung durch Angreifer	571
24.1.1	Deepfake- & Voice-Spoofing – KI-gestützte Täuschungsangriffe	573
24.1.2	KI-generiertes Phishing	575
24.1.3	AI-gestützte Malware-Evasion	577
24.1.4	Data Poisoning	580
24.1.5	Model Inversion & Membership Inference	583
24.2	Defensive AI – Einsatz im Security Stack	586
24.2.1	SIEM/XDR – KI-gestützte Alert-Priorisierung und Rauschentlastung	587
24.2.2	UEBA – User and Entity Behavior Analytics	591
24.2.3	SOAR – Automatisierung mit LLMs für kontextbasierte Reaktion	593
24.2.4	Threat Intelligence – Automatisierte Auswertung von Reports & Feeds	597

24.3	Governance, Risk & Compliance für AI	601
24.3.1	Relevante Rahmenwerke und Standards	601
24.3.2	CISO-Aufgaben in AI Governance	608
24.4	Operationalisierung: AI Security Engineering	611
24.4.1	Training – Schutz vor manipulierten oder unzuverlässigen Daten	611
24.4.2	Deployment – Schutz vor Missbrauch im Betrieb	614
24.4.3	Monitoring – Kontinuierliche Überwachung und Anomalieerkennung	616
24.4.4	Testing & Red Teaming – Offensive Tests gegen ML-Systeme	618
24.4.5	Fazit	620
24.5	Metriken & KPIs für AI-Security	621
24.6	Fazit und Ausblick	625
24.7	Referenzen	626
25	Post-Quantum Kryptographie	629
25.1	Stand der Technik 2026 – Algorithmen, Standards, Protokolle	630
25.1.1	NIST-Standards	631
25.1.2	Protokollintegration (IETF/Industrie)	633
25.1.3	Leitlinien & Roadmaps	635
25.2	Technik-Essenzen für CISOs	636
25.3	Häufige Fallstricke	638
25.4	Migrationsplan (CISO-Roadmap 36 Monate)	644
25.4.1	Programmaufbau, Governance und Arbeitsstränge	645
25.4.2	Phasenmodell: 0–6 / 6–18 / 18–36 Monate	649
25.4.3	Phase 6–18 Monate – Hybride Einführung & Härtung	652
25.4.4	Phase 18–36 Monate – Skalierung & PQC-only-Domänen .	655
25.5	Metriken & KPIs – CISO-/Board-taugliche Erfolgskennzahlen für PQC-Programme	659
25.6	Fazit	661
25.7	Referenzen	663
	Glossar	669
	Stichwortverzeichnis	681

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 Marktpresenz – 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

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 Survey¹.

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. Technologie – Architekt der Resilienz

In seiner Rolle als Technologie begreift der CISO Sicherheitsarchitektur nicht als eine lose Sammlung von Tools oder punktuellen Maßnahmen, sondern als ein kohärentes, steuerbares Gesamtsystem. Dieses wirkt über sämtliche Technologieschichten 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 – Technologie, 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.

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.
- **Risikübersetzung:** 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

A

ABAC 238
Adaptive 135
Advanced Persistent Threats 487
Alert-to-Ticket-Ratio 381
Amazon Web Services 301
Analysephase 126
Analysis and Production 494
API-Keys 321
Application Security 345
ATT&CK Coverage 396
Attribute-Based Access Control 278
Audit-Readiness 183, 190, 191
AWS 291, 299
Azure 291, 299, 303
Azure Defender for Cloud 307
Azure Key Vault 308

B

Backup-as-a-Service 539
Balanced Scorecard 40
Bring Your Own Device 246
BSIG & IT-Sicherheitsgesetz 2.0 470
BSI Standard 200-4 529
Business Alignment 411
Business Continuity & Disaster Recovery 525
Business Continuity Plans 385
Business Resilience 445
Business Strategy Alignment 127

C

Case Management 424
CI/CD Integration 360

CIEM 271
CIEM vs. CSPM 286
CIS Controls 151, 156, 197
CISO Office 63
Cloud Access Security Broker 247, 312
Cloud Identity Governance 294
Cloud Infrastructure Entitlement Management 272, 284
Cloud Security 291
COBIT 2019 198
Collection 492
Compliance Score 317
Conditional Access 304
Conditional Access Policies 310
Control Self-Assessments 187
Credential Hygiene 322
Credential Misuse 419
Credential Theft 466
CSPM 33
Cyber Threat Intelligence 487

D

DAST 345
Data Loss Prevention 249
Data Poisoning 580
Deep-Dive-Schulungen 559
Deepfake- & Voice-Spoofing 573
Defined 135
Detection-as-Code 410, 500
Detection Engineering 435
Detection Engineering Lifecycle 410
Detection Gaps 409
Detection Latency 440
detection use cases 408

Developer Enablement 361
 DevSecOps 328, 345, 502
 DH 629
 Disaster Recovery as a Service 539
 Disaster Recovery Plan 385, 540
 Dissemination 496
 Domänenspezialisierung 85
 DORA 207, 219, 470, 513
 Drittparteien-Scorecards 229
 DSGVO 207, 208, 470
 Due Diligence 227
 Dynamic Application Security Testing 348

E

ECC 629
 Einstiegsschulungen 558
 Enabler 122
 Endpoint Malware Detection 426
 Endpoint Security 245
 Erwartungsmanagement 95
 EU AI Act 603
 Evidenzmanagement 191
 Externe Kommunikation 476
 externe Stakeholder 89

F

Factor Analysis of Information Risk 168
 FAIR 167
 FAIR-Modell 535
 False-Positive-Rate 409
 FIPS 203 631
 FIPS 204 631
 FIPS 205 632
 FN-DSA 632
 föderierte Governance-Modell 108
 föderierte Modell 103

G

Gapanalyse 129
 GCP 299
 Governance & Policy Frameworks 185
 GRC 64

H

Harvest now, decrypt later 629
 HQC 633
 Human-in-the-Loop-Mechanismen 429
 hybride Governance 112
 hybride Modelle 103
 Hypothesenmodellierung 447

I

IAM 271
 Identity Federation 274
 Incident Response 463
 Incident Response Policy 465
 Incident-Response-Programm 463
 Infrastructure-as-Code 293, 321
 Initial 135
 Initial Access 322
 Intelligence Requirements 492
 Interne Kommunikation 474
 Interne Kontrollsysteme (IKS) 66, 183
 IOC 488
 IOC-Analyse 499
 ISO/IEC 22301
 2019 528
 ISO/IEC 27001 32, 151, 155, 196
 2022 473
 ISO/IEC 27005 167
 ISO/IEC 42001 605

J

Just-in-Time 260
 Just-in-Time Access 239, 325
 Just-in-Time-Zugriffsmodellen 294

K

Key-Encapsulation Mechanism 631
 Key Performance Indicators 357
 Key Risk Indicators 173
 Kommunikation 90
 Kontextanalyse 123
 Kontinuierliche Fortbildung 559
 Kontinuierliche Verbesserung 480

KQL 437
 KRITIS-VO 207, 216, 512
 Krypto-Agilität 637
 Künstliche Intelligenz 393, 569

L

Large Language Models 614
 Lateral Movement 322
 Least Privilege 239
 Leitbild 122
 LLM 394
 Logaggregation 407
 Logging Coverage 315
 Loss Event Frequency 168
 Loss Exceedance Curve 172
 Loss Magnitude 168, 171

M

Make-or-Buy 387, 391
 Malware-Evasion 577
 Managed 135
 Maturity Assessments 126
 Maturity Roadmapping 134
 Mean Time to Detect 381
 Membership Inference 583
 Mikrosegmentierung 240
 MISP 506
 MITRE ATT&CK 371, 410, 435
 MITRE ATT&CK TTP Coverage 440
 MITRE SOC-CMM 385, 399
 MLDSA 631
 ML-KEM 631
 ML-Modelle 570
 Model Inversion 583
 MTTC 481
 MTTD 409, 481
 MTTR 316
 Multi-Cloud 295
 Multi-Factor Authentication 310
 Multi-Faktor-Authentifizierung 333

N

Netzwerkperimeter 237
 Never trust, always verify 273
 NIS2 207, 213
 NIS2-Richtlinie 470
 NIST AI Risk Management Framework 601
 NIST CSF 2.0 151, 155
 NIST Cybersecurity Framework 197
 NIST HQC 633
 NIST SP 800-34 528
 NIST SSDF 365
 Notfallpläne 540

O

OAuth 311
 Operational Security 68
 Operational Technology (OT) 34, 452
 Operative CTI 489
 organisatorische Anbindung 81
 OSCP 560
 OSEP 560
 OSINT 498
 OT-Security Monitoring 397
 OWASP SAMM 365

P

Paket. Siehe Package
 PAM 271
 PAM-Reifegrade 283
 Passwörter 321
 PBAC 238
 PDP 241
 PEP 241
 Perimeterbasierte Sicherheitsansätze 237
 Phishing 575
 Phishing Detection 425
 Phishing-Resistente MFA 333
 Playbooks 465
 Policy-Based Access Control 278
 Policy Drift Rate 316

Post-Quantum-Crypto (PQC)-Readiness Assessment 629
 Post-Quantum Kryptographie 629
 Predictive Threat Intelligence 569
 Primary Loss 169
 Privacy-by-Design 32
 Privileged Access Management 272, 280
 Privileged Identity Management 306
 Privilege Escalation 322
 Processing and Exploitation 493

Q

Qualifizierungsstrategien 555
 Quartalsreporting 141
 Quarterly Security Business Reviews 41
 Quick Wins 137

R

RACI-Matrix 192
 RASP 345
 RBAC 238, 306
 Repeatable 135
 Reporting-Frameworks 133
 Reputationsschutz 122
 Resilienz 121
 Restore-Tests 540
 Return on Security Investment 386, 389
 Risikoorientierung 555
 Risikosteuerung 184
 Roadmap-Entwicklung 130
 Role-Based Access Control 277, 310
 Rollenbündelung 84
 Rotation by Default 325
 RPO 526
 RSA 629
 RTO 526
 Rule Fidelity Rate 439
 Runtime Application Self-Protection 350

S

SaaS Security 310
 SaaS Security Posture Management 312

SAST 345
 SBOM 345
 SCA 345
 Schulungen 555
 SCIM 311
 Secondary Loss 169
 Secrets 321
 Secrets Management 332
 Secure Coding Guidelines 357
 Secure Design Reviews 560
 Security-as-Code 395
 Security Business Reviews 133
 Security-by-Default 80
 Security-by-Design 292, 346
 Security Culture 72
 Security Engineering 66
 Security-Funktion 61
 Security-Governance 103
 Security Information and Event Management 34, 406
 Security Office 62
 Security Operations Center 371
 Security Orchestration, Automation and Response 34, 423
 Security-Strategie 121
 Security-Teams 86
 Segregation of Duties 273
 Shared Accounts 332
 Shared Responsibility 292
 Shift Left 360
 Sicherheitsorganisation 61
 Sicherheitsstrategie 37
 SIEM Maturity Model 415
 Sigma 437
 Single Sign-On 310
 SLH-DSA 632
 SOAR 262, 405, 593
 SOC 2 32
 Software Bill of Materials 33, 354
 Software Composition Analysis 352
 Software Defined Perimeter 247
 Software Development Lifecycle 359

SSO 274
 Stakeholder-Management 59, 87
 Stakeholder-Matrix 88
 Starke Authentifizierung 333
 Static Application Security Testing 347
 Steuerungsarchitektur 125
 STIX 504
 STIX/TAXII 437
 Strategische CTI 489
 Suspicious API Activity 426

T

Tabletop Exercises 482, 560
 Tabletop-Übungen 465
 Taktische CTI 490
 TAXII 505
 Technische CTI 490
 Third Party Risk Management 225
 Third-Party Software Policy 357
 Threat Actor Profiling 499
 Threat Event Frequency 170
 Threat Hunting 435, 444
 Threat Intelligence 597
 Threat Intelligence Platforms 507
 Threat Landscape Briefings 383
 Threat-led SOC 395
 Time-Bound Access 333
 Time-to-Remediate 201
 TISAX 32, 207, 210, 511
 TLS 1.3 633
 TLS-Handshake 629
 Tokens 321
 Total-Cost-of-Ownership 390

TPRM-Lifecycle 226
 Transparenz 98
 TTP-Mapping 499
 TTP-Orientierung 436
 TTPs 435

U

UEBA 405, 591
 Use Case Coverage 381
 User and Entity Behavior Analytics 419

V

Vertrauen 32, 122
 Voice-Cloning 573
 Vulnerability 171

W

Wiederanlaufstrategien 526
 Wiederherstellungszeit 550

Y

YARA 437

Z

zentrale Governance 105
 zentrale Kontrollbibliothek 191
 zentrales Modell 103
 Zero Trust 297
 Zero Trust-Architektur 237
 Zero Trust Maturity Model 252
 Zielbilddefinition 127
 ZTA Roadmap 252