

Informations- und Cybersicherheit

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

DAS INHALTS- VERZEICHNIS

» Hier geht's
direkt
zum Buch

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-Profile 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