

Informations- und Cybersicherheit

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

» Hier geht's
direkt
zum Buch

DAS VORWORT

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.

Kapitel 1

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

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 Anmeldeöglichkeiten unter:



www.cycademy.de/ciso-masterclass