Der moderne CISO
Cybersecurity Leadership in der digitalen Wirtschaft

Ron Kneffel

bitkom
akademie

Cyberrisiko ist Geschäftsrisiko

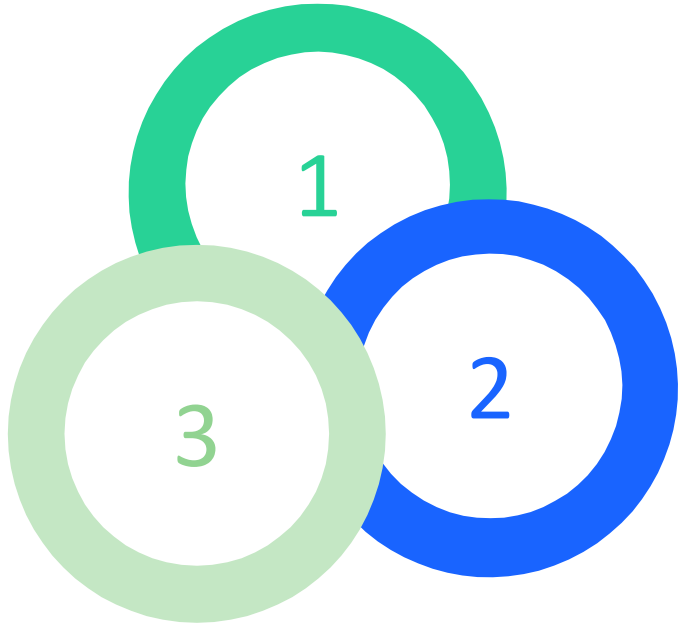
Digitale Geschäftsmodelle vergrößern die Angriffsfläche

Cybervorfälle beeinflussen Umsatz und Reputation

Vorstände erwarten strategische Führung durch Security

Unsere Ziele

Erwartungen an die Rolle des CISO verstehen



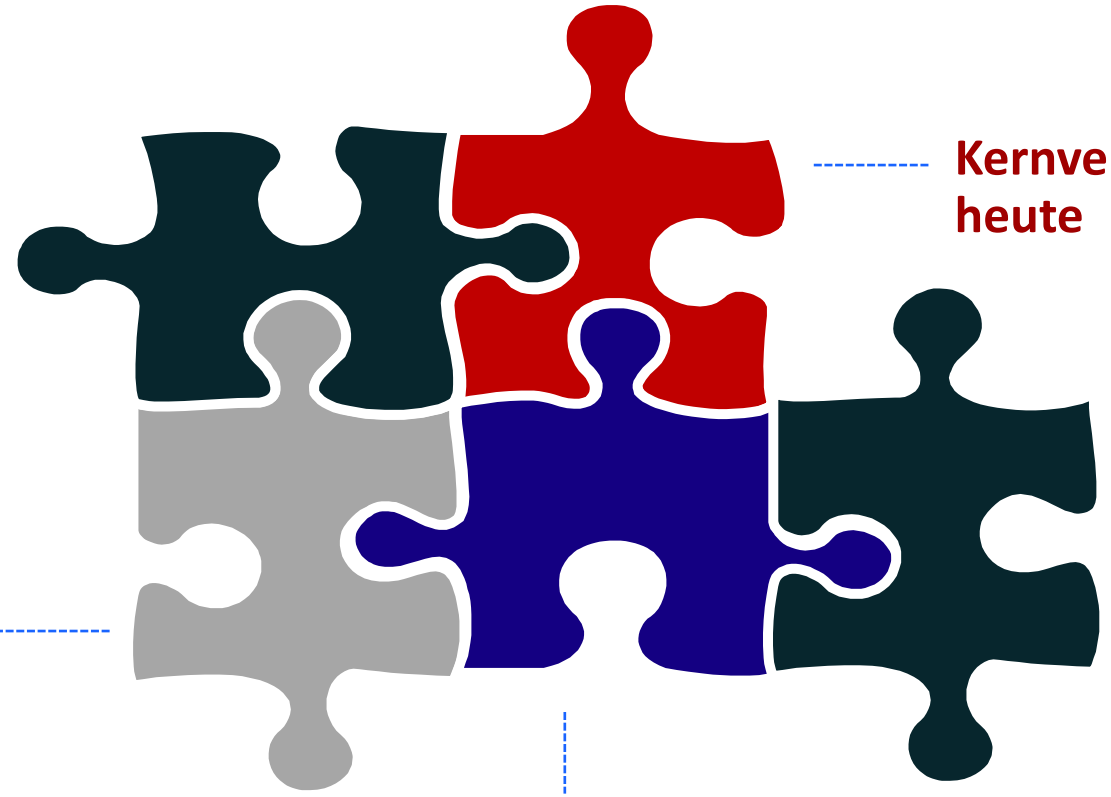
Zentrale Kompetenzen identifizieren

Impulse für die eigene Entwicklung ableiten

bitkom akademie

Agenda

Alte vs. neue CISO-Rolle



Kernverantwortlichkeiten heute

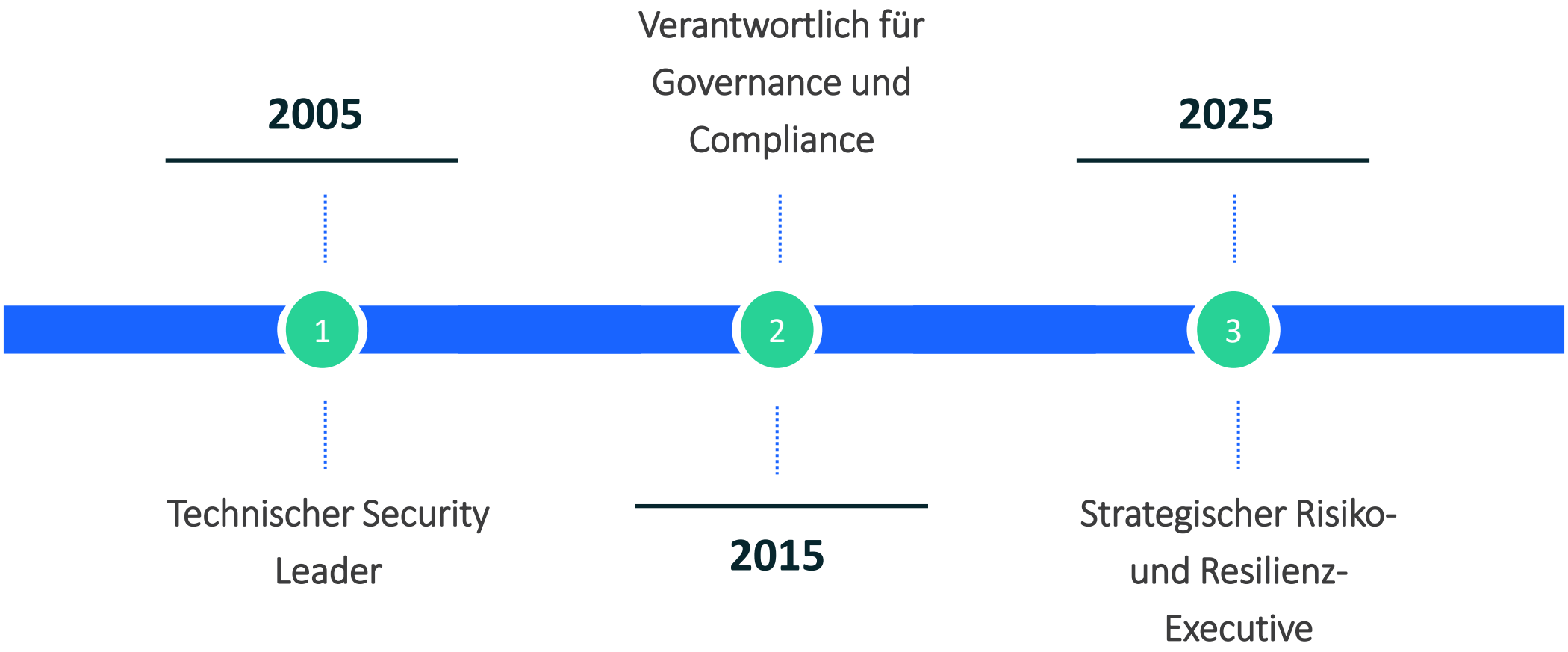
Kritische Kompetenzen & Skills

Weiterbildung & nächste Schritte

Praxisszenarien & Reflexion

bitkom akademie

Die Entwicklung der CISO-Rolle

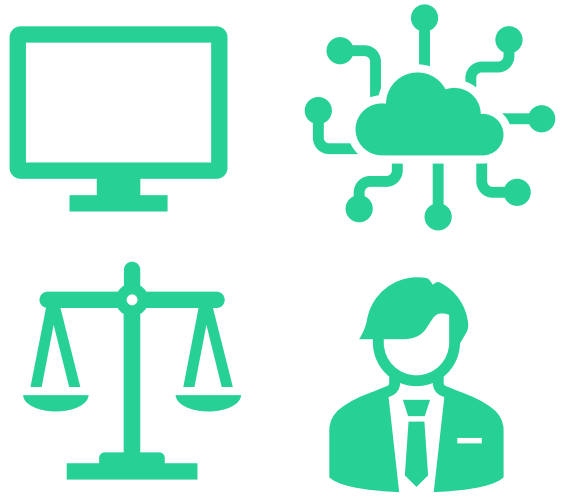


bitkom akademie

Warum sich die Rolle verändert

Digitale Transformation

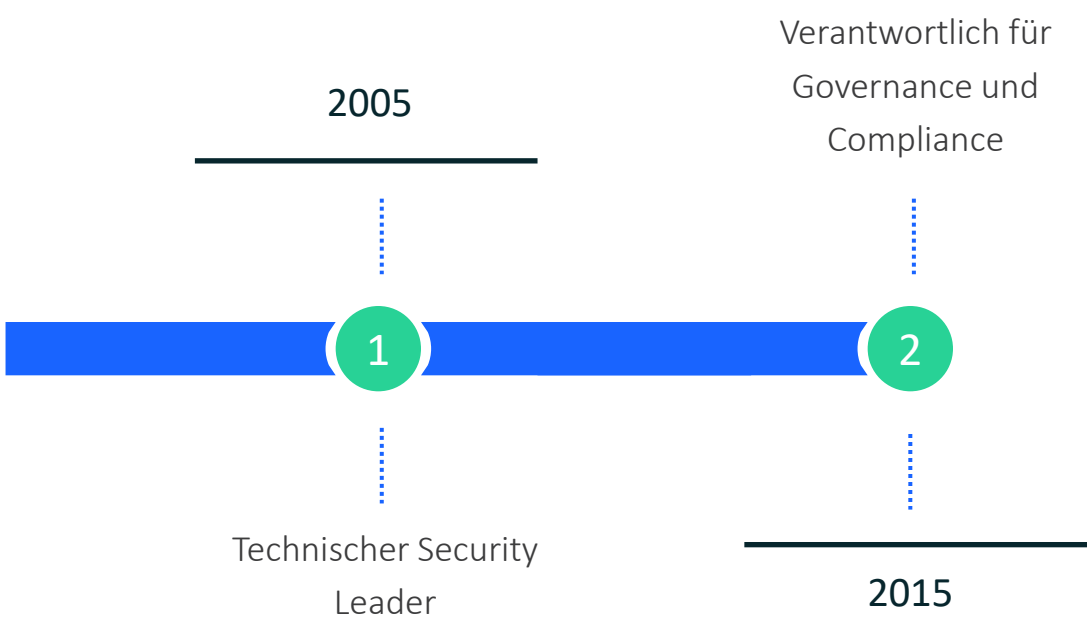
Cloud und verteilte Architekturen



Regulatorik und geopolitische Risiken

Verantwortung auf Vorstandsebene

Alte CISO-Rolle



- Starke technische Prägung
- **Zentrum:** Compliance Erfüllung

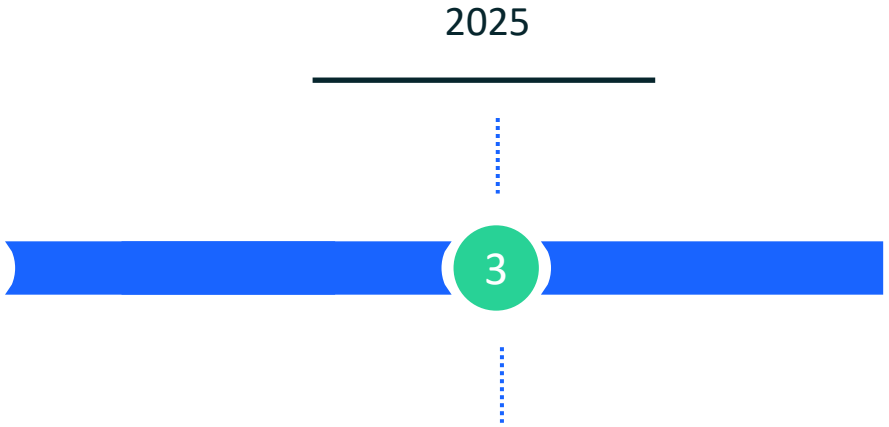
  (27001, interne Richtlinien, Maßnahmenumsetzung)

Audit

Haben wir alle Controls umgesetzt?

bitkom akademie

Neue CISO-Rolle



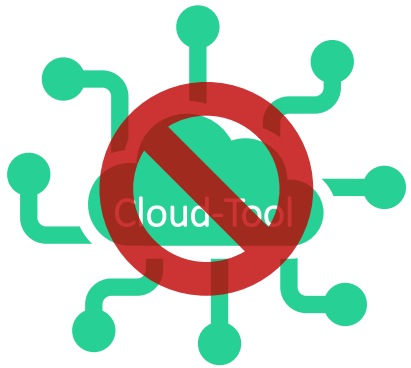
- Risikomanagement statt nur Control-Checklisten
- **Fokus:** Geschäftsrisiken

Wie tragen wir aktiv dazu bei, dass das Geschäft sicher wachsen kann?'"

bitkom akademie

Mindset-Shift

Beispiel



„Kein Bestandteil unserer Policy“

- ✓ Datenschutz
- ✓ Regulatorik
- ✓ Resilienz

bitkom akademie

Interaktive Frage

Wo steht ihr heute mit eurer Rolle?

1. *Wer erlebt die Rolle noch überwiegend technisch und operativ?*

   → *Daily Business, viele Tickets, viel operative Arbeit*

2. *Wer ist bereits strategisch unterwegs?*

   → *Steering-Runden, Board-Präsentationen, strategische Projekte*

3. *Und wer ist gerade in der Transformation?*

   → *Ein Fuß noch im Operativen, der andere schon in der Strategie*

Kernverantwortlichkeiten

Strategische Risikobewertung & Governance

Krisenführung & Notfallmanagement

Business-Alignment & Enablement

Stakeholder-Kommunikation

Kernverantwortlichkeiten: Strategische Risikobewertung & Governance

Security darf nicht nur Normen erfüllen.
Sie muss **Geschäftsrisiken sichtbar machen** und **Managemententscheidungen** unterstützen.

Was sich verändert

- Fokus auf Geschäftsrisiken statt Audit-Checklisten
- Security-Governance liefert Entscheidungs-grundlagen für den Vorstand
- Security wird Teil strategischer Unternehmens-steuerung

Beispiel

- Statt einem 20-seitigen technischen Report bekommt der Vorstand quartalsweise 3–5 Klartext-Kennzahlen:
  - *‚Top-3-Risiken für Umsatz & Reputation‘*
  - *‚MTTR bei kritischen Incidents‘*
  - *‚Status der wichtigsten Security-Initiativen'*

Kernverantwortlichkeiten: Krisenführung & Notfallmanagement

In vielen Organisationen leitet der CISO im Ernstfall den **Krisenstab** oder ist **zentrale Stimme** darin.

Erwartungen

- Klare Lagebilder
- Entscheidungsoptionen
- Priorisierung
- Ruhe unter Druck

Beispiel

- Es gibt einen Ransomware-Angriff, Teile der Produktion stehen.

  Der CISO muss in 10 Minuten erklären:

  - *Was wissen wir?*
  - *Was wissen wir nicht?*
  - *Was sind die nächsten drei Schritte?*
  - *Welche Szenarien drohen wichtigsten Security-Initiativen*

Kernverantwortlichkeiten: Business-Alignment & Enablement

Sicherheit muss **Geschäft ermöglichen**: schnellere Freigaben, sichere Digitalisierung, Unterstützung bei Produktideen.

Chancen aktiv gestalten

- Wer nur ‚Nein' sagt, wird übergangen; wer Risiken in Chancen übersetzen kann, wird Partner.

Beispiel

- Das Produktteam will ein neues Kundenportal live schalten.

  Der CISO hilft, frühzeitig
  - sichere Architektur
  - Identity- und Logging-Konzepte zu definieren

  so wird die Time-to-Market gehalten und trotzdem Security-by-Design umgesetzt.

Kernverantwortlichkeiten: Stakeholder-Kommunikation

Kommunikation mit Board, C-Suite, Mitarbeitenden und externen Partnern ist Kernaufgabe.

Risiko verstehen

- Es reicht nicht, Reports zu verschicken – es geht darum, ein gemeinsames Verständnis von Risiko und Prioritäten zu schaffen.

Beispiel

- In der Board-Sitzung erklärt der CISO
  - Nicht: **„Wir haben 1.000 offene Schwachstellen“**
  - sondern: **„Wir haben drei kritische Schwachstellen in Systemen, die 40 % unseres Umsatzes betreffen und hier ist unser Plan, wie wir das in 14 Tagen adressieren.“**

Kernverantwortlichkeiten: Reflexionsfrage

Welche dieser vier Verantwortlichkeiten prägt euren Alltag am stärksten?

- Strategische Risikobewertung & Governance
- Krisenführung & Notfallmanagement
- Business-Alignment & Enablement
- Stakeholder-Kommunikation

Welche dieser Verantwortlichkeiten fehlt in eurem Alltag fast komplett?

Kompetenzen

Neue Skill Profile

1. Management & Führung 
2. Kommunikation & Mediation 
3. Krisenmanagement & Koordination 
4. Resilienz & Belastbarkeit" 

bitkom akademie

Kompetenzen
Management & Führung

Führungskompetenz

Situation: Das Security-Team arbeitet dauerhaft im Incident-Modus.
Aktion: Der CISO definiert klare Rollen, baut Karrierepfade auf und schafft Strukturen, die nachhaltige Arbeit ermöglichen.

Verhandlungsgeschick

Situation: Security-Budget steht zur Diskussion.
Aktion: Der CISO zeigt verschiedene Budget-Szenarien und erklärt die Auswirkungen auf Geschäftsrisiken.

Lehr- und Coachingfähigkeit

Situation: Ein Team soll DevSecOps einführen.
Aktion: Der CISO begleitet den Prozess mit Workshops, Lernformaten und praktischem Feedback.

Kompetenzen
Kommunikation & Mediation

Adressatengerechte Kommunikation

- Komplexe technische Themen verständlich erklären
- Inhalte auf Management, HR und Fachbereiche zuschneiden
- Weniger Fachsprache, mehr Relevanz und klare Storyline

Konfliktlösung

- Vermittelt zwischen IT, Fachbereichen und Management
- Löst Konflikte bei Budgets, Deadlines und Anforderungen

Kompetenzen
Kommunikation & Mediation

Adressatengerechte Kommunikation Aufsichtsrat

Ausfall Onlineshop

→X Euro Umsatz

→Y Kunden

→Z Social Media Reichweite

Kompetenzen
Krisenmanagement & Koordination

Krisenführung

- Ruhe und Orientierung im Incident geben
- Klare Führung in kritischen Situationen
- Entscheidungen trotz Unsicherheit treffen

Koordinations-Skills

- CISO koordiniert Security-Themen über mehrere Bereiche hinweg
- Steuert den Informationsfluss zwischen Technik, Kommunikation, Legal, Management und Behörden

Kompetenzen
Resilienz & Belastbarkeit

Resilienz und Selbstmanagement

- Ruhe und Stabilität unter hohem Druck bewahren
- Eigene Belastung steuern und Prioritäten setzen
- Auch in langen Krisensituationen handlungsfähig bleiben

Der moderne CISO

Schnelle Selbsteinschätzung

Wählt spontan 1 bis 2 Skills, in denen ihr heute am stärksten seid:

- Führung & Teamentwicklung
- Verhandlung & Budgetsicherung
- Adressatengerechte Kommunikation
- Krisenmanagement unter Druck

Kurz nachdenken und merken:

Wo seht ihr eure größten Entwicklungsfelder?

Praxisszenarien
Szenario 1 – Breach entdeckt

- Sensible Daten wurden kompromittiert
- Teile der IT-Systeme sind aktuell nicht verfügbar

Ransomware-Attacke

Was kann und muss der CISO jetzt tun?

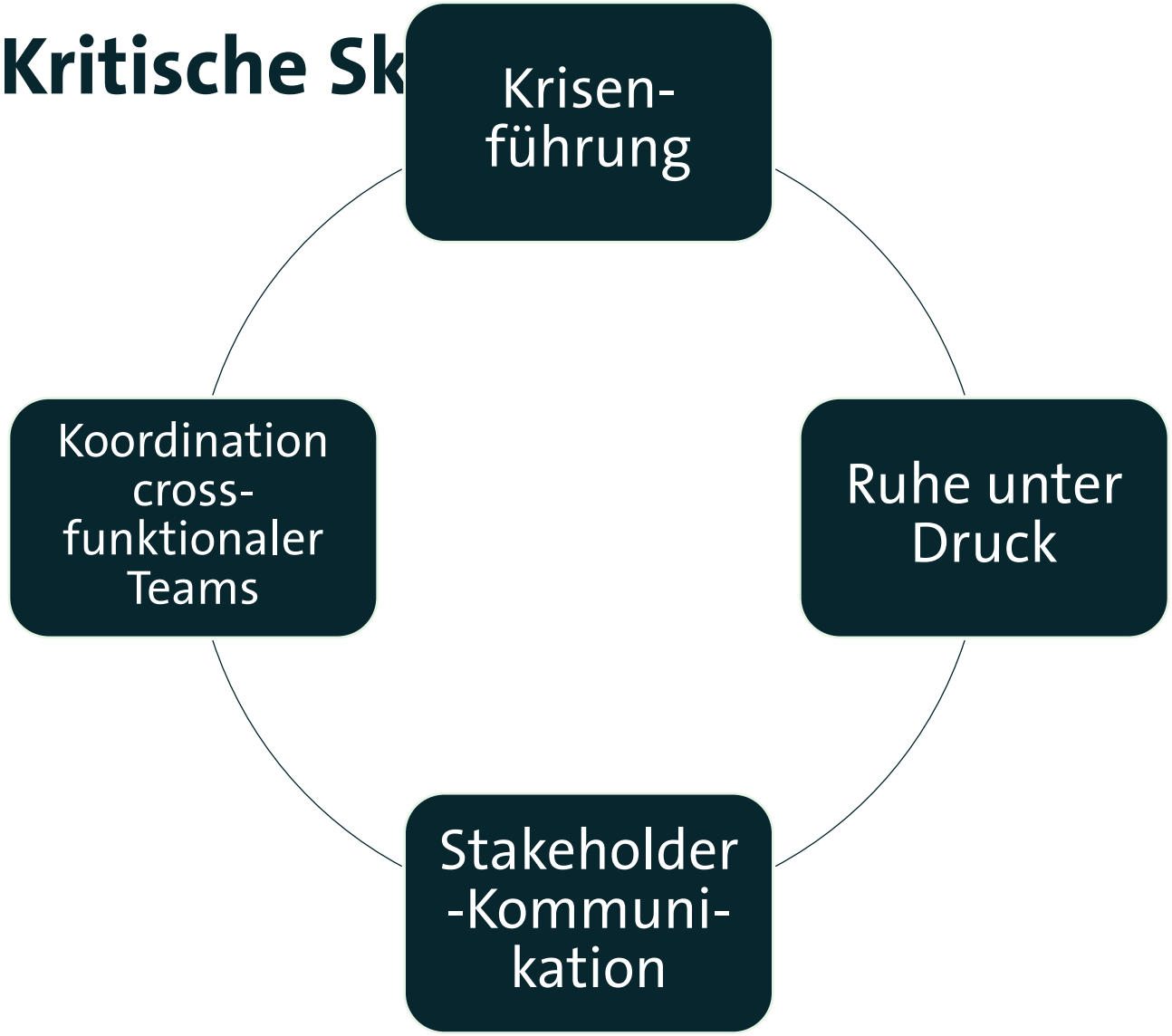
Praxisszenarien
Szenario 1 – Breach entdeckt

- Sensible Daten wurden kompromittiert
- Teile der IT-Systeme sind aktuell nicht verfügbar

Ransomware-Attacke

- **Krisenstab aktivieren** und **Verantwortlichkeiten klären**
- Vorstand, Kunden und Partner **informieren**
- **Gemeinsame Kommunikationslinie** festlegen
- Technische und organisatorische **Maßnahmen koordinieren**
- **Entscheidungen** trotz Unsicherheit **treffen**

Praxisszenarien
Szenario 1 – Kritische Sk



bitkom
akademie

Praxisszenarien
Diskussion – Breach-Erfahrungen

Welche Fehler seht ihr in der Praxis bei Breach-Situationen am häufigsten?

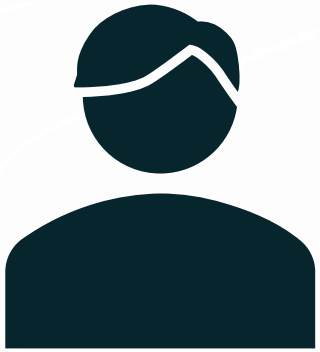
Praxisszenarien
Szenario 2 – Budget-Verhandlung

- Security-Bugdet Kürzung um 30%
- Zeitgleich: Zusätzliche Investionen durch neue Regulierung

Was kann und muss der CISO jetzt tun?

Praxisszenarien
Szenario 2 – Budget-Verhandlung

- Security-Bugdet Kürzung um 30%
- Zeitgleich: Zusätzliche Investionen durch neue Regulierung



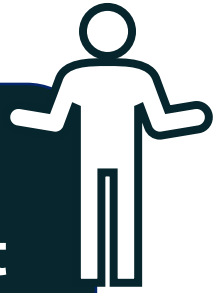
- Ein **klares Risk-Narrative** in Business-Sprache **aufbauen**
- Einen Business-Case mit **Zahlen** und **Szenarien** vorbereiten
- **Verhandeln und priorisieren**: Welche Maßnahmen sind nicht verhandelbar, wo geht stufenweise Umsetzung?
- **Kompromisse suchen**, ohne eine Schein-Sicherheit zu erzeugen

Praxisszenarien

Technologie ist nur die halbe Gleichung

Warum Kultur zählt

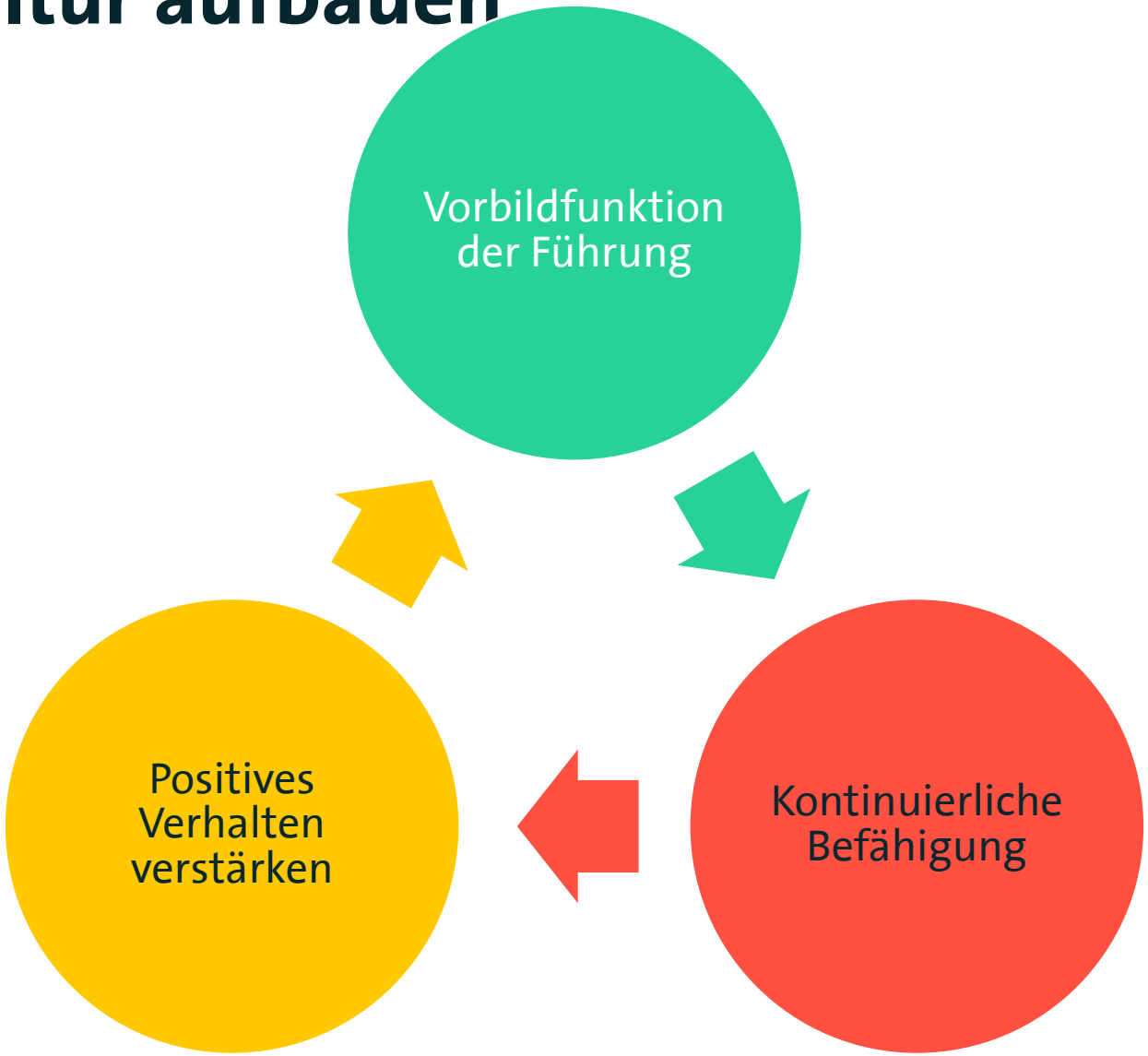
Menschliches Verhalten ist Auslöser vieler Vorfälle



Policies allein reichen nicht aus

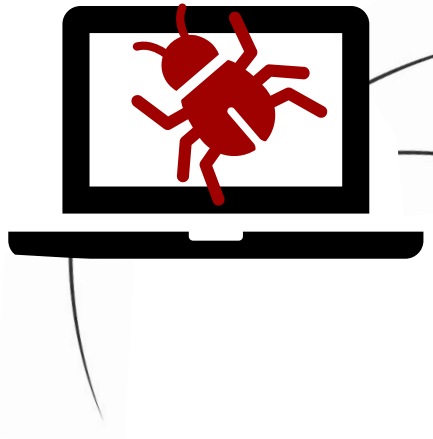
Security muss gemeinsame Verantwortung werden

Sicherheitskultur aufbauen



bitkom akademie

Praxisszenarien
Szenario 3 – Security-Kultur



Phishing-Treffer

Mitarbeitende ignorieren Security-Policies

„Security ist nicht mein Job“

Was kann und muss der CISO jetzt tun?

Praxisszenarien
Szenario 3 – Security-Kultur

Phishing-Treffer

Mitarbeitende ignorieren Security-Policies

„Security ist nicht mein Job“

- Befähigende **Security-Trainings** entwickeln
- **Anreize** für sicheres Verhalten setzen
- Positive Verhaltensänderung **belohnen**
- Führungskräfte als **Security-Vorbilder** einbinden
- Fokus auf **Enablement** statt Bestrafung

Praxisszenarien
Szenario 2 – CFO überzeugen

Wie erklärt man in 2 Minuten, warum diese 30 % Kürzung ein Problem ist?

Dont

- Reine Pflichtschulungen ohne Praxisbezug
- Mitarbeitende nur für Fehler sanktionieren
- Security als Kontrolle oder Hindernis darstellen
- Führungskräfte nicht einbinden

Do

- Schulungen entwickeln, die Mitarbeitende befähigen
- Anreize für sicheres Verhalten schaffen
- Positive Verhaltensänderungen belohnen
- Führungskräfte als Vorbilder einbinden
- Beispiel: Risiko-Profil mit aktuellem Budget vs. nach Kürzung

Praxisszenarien
Erfahrungsaustausch – Kulturwandel

Welche Hebel nutzt ihr in euren Organisationen, um Security- Kultur zu verändern?

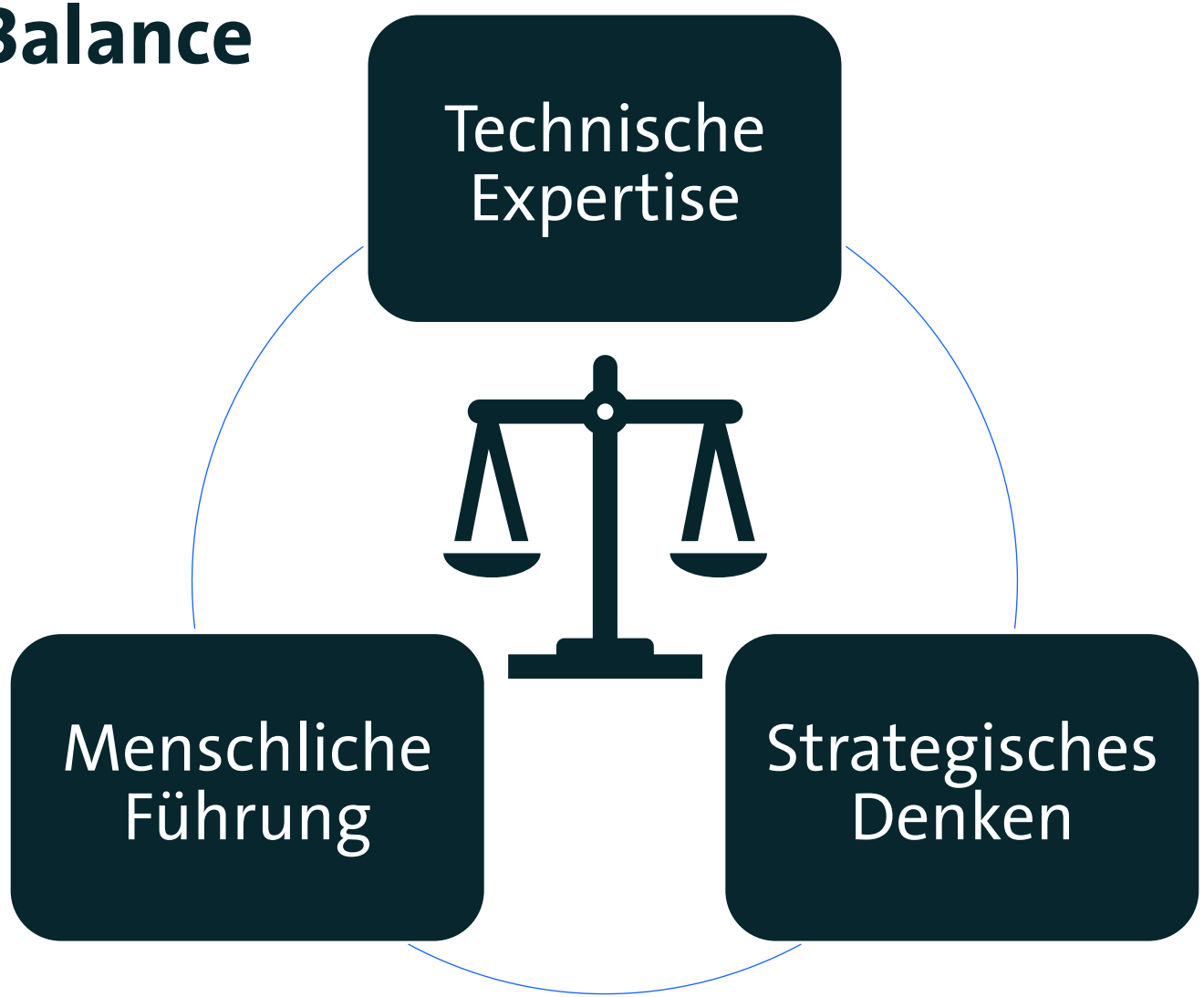
Wo stoßt ihr an Grenzen? Was funktioniert nicht, obwohl ihr es versucht habt?

Der CISO der Zukunft

Security als strategische Funktion

- ✓Cyber-Resilienz als **Wettbewerbsvorteil**
- ✓Security in **Unternehmensstrategie** eingebettet
- ✓CISO als **vertrauenswürdiger** Berater

Leadership-Balance

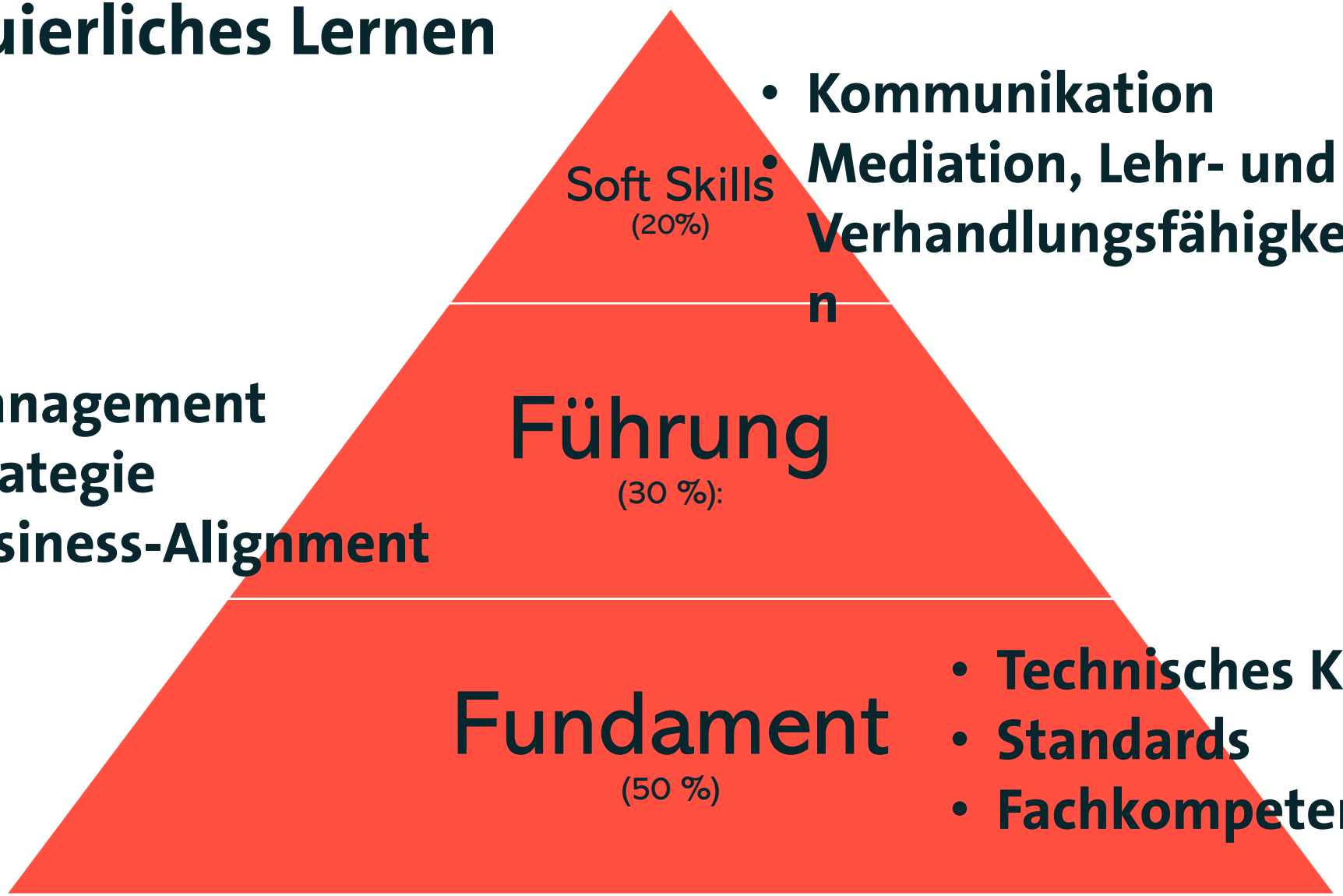


bitkom akademie

Kontinuierliches Lernen

- Technologie entwickelt sich rasant
- Leadership-Herausforderungen wachsen
- Peer-Netzwerke werden wichtiger

Kontinuierliches Lernen



- Kommunikation
- Mediation, Lehr- und Verhandlungsfähigkeiten

- Management
- Strategie
- Business-Alignment

- Technisches Know-how
- Standards
- Fachkompetenz

bitkom akademie

Der moderne CISO

Ehrliche Selbstreflexion

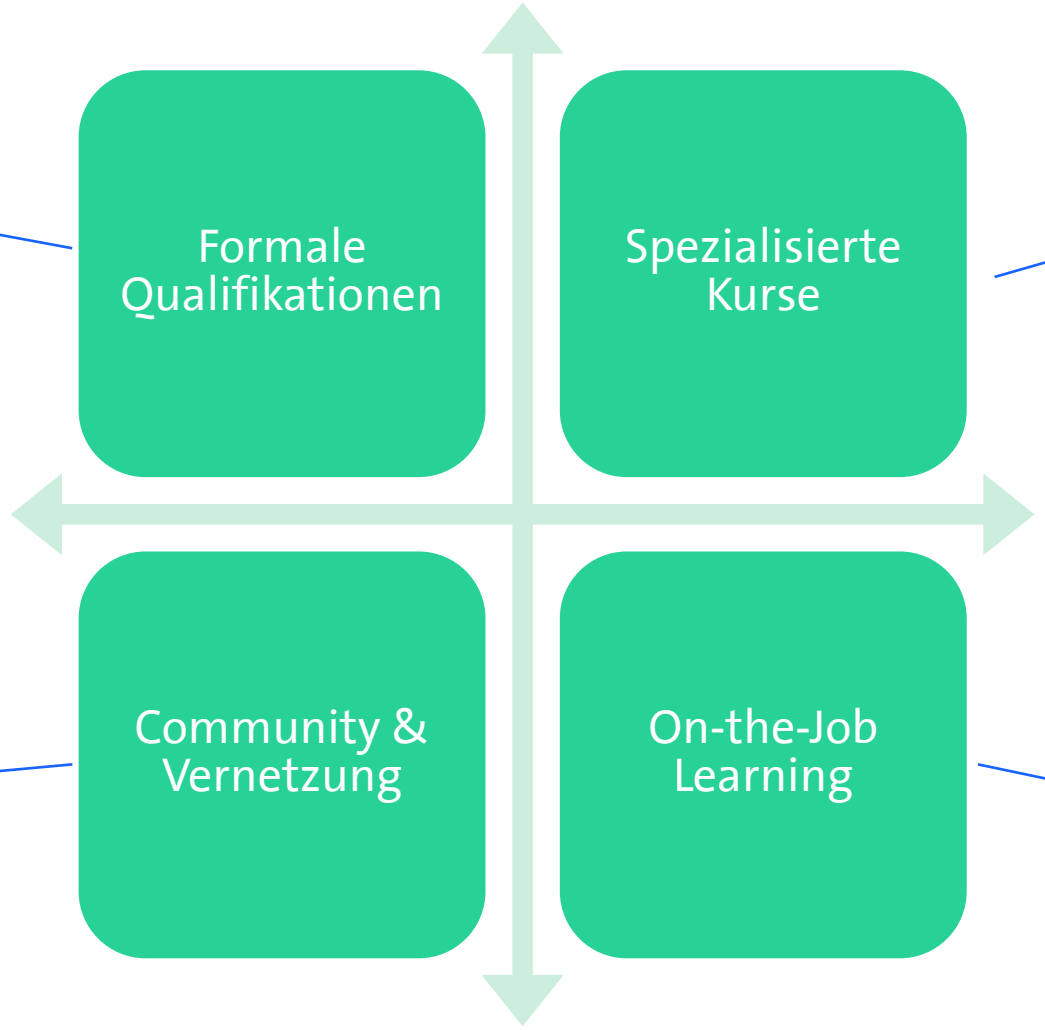
Wie viel Prozent eurer Energie und Zeit steckt heute in...

- Technische Arbeit & Operatives?
- Führung & strategisches Management?
- Kommunikation & Stakeholder-Arbeit?

Passt das zu den Anforderungen an eure Rolle?

Weiterbildung & lebenslanges Lernen

Solides technisches und konzeptionelles Fundament:
CISSP, CISM oder CCSK



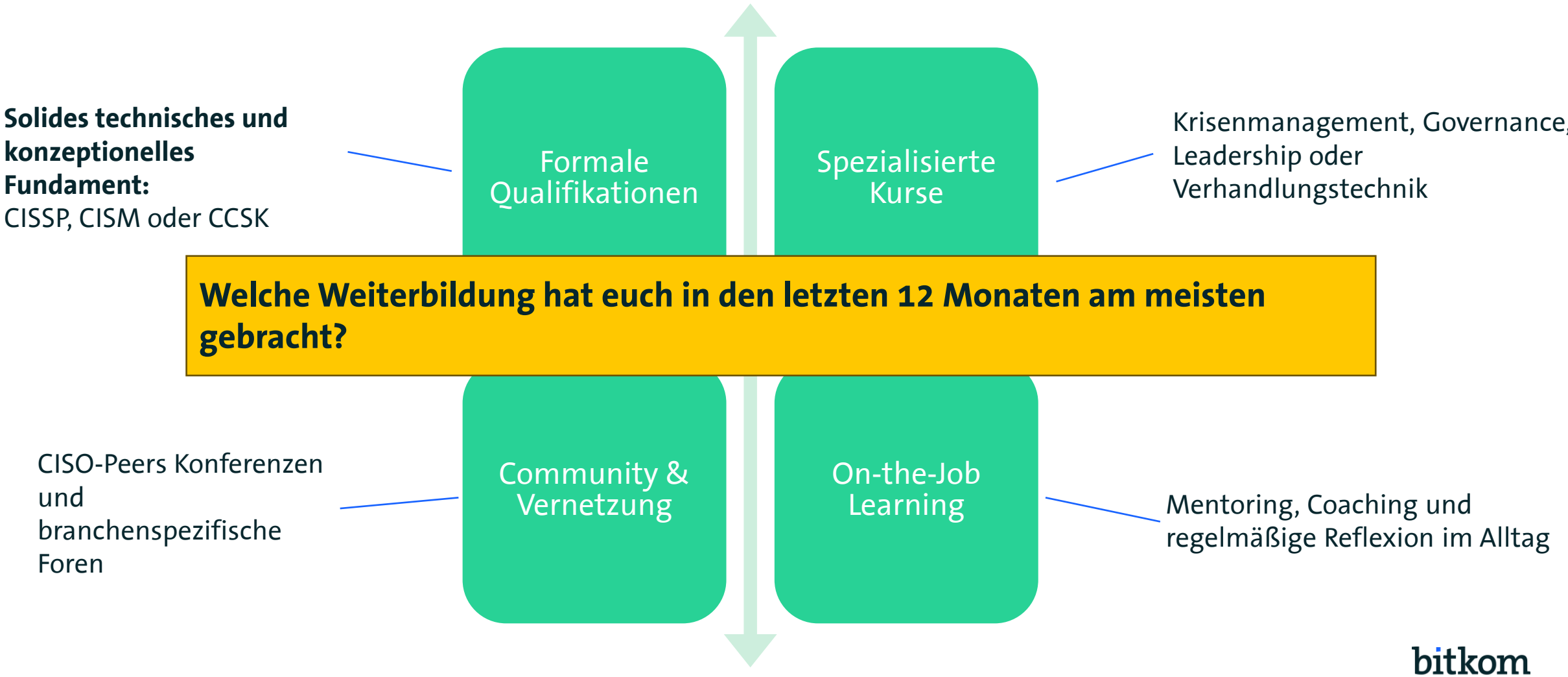
Krisenmanagement, Governance, Leadership oder Verhandlungstechnik

CISO-Peers Konferenzen und branchenspezifische Foren

Mentoring, Coaching und regelmäßige Reflexion im Alltag

bitkom akademie

Weiterbildung & lebenslanges Lernen



bitkom akademie

Deine nächsten Schritte

1. **Selbsteinschätzung:** In welchen Skills bin ich stark, wo schwach?
2. **Fokus:** Welche 2–3 Kompetenzen möchte ich in den nächsten 12 Monaten gezielt entwickeln?
3. **Aktionen:** Welche konkreten Schritte leite ich ab?
    a. Kurs buchen
    b. Mentor suchen
    c. Regelmäßiges Feedback im Management einholen
4. **Reflexion:** Mindestens quartalsweise schauen: Was hat sich verändert?

    Was hat funktioniert, was nicht?

Persönlicher Aktionsplan

Beispiele

- *Mit CFO oder CIO über deren Sicht auf Security sprechen*
- *CISO-Peer oder Mentor für Sparring suchen*
- *2 Tage für eigene Weiterbildung im Kalender blocken*
- *Nach dem nächsten größeren Projekt: Feedback zu eurer Kommunikation einholen*

Key Takeaways

**Security ist heute Business-Thema,
nicht nur IT-Thema.**

Soft Skills und Führung sind kritische Erfolgsfaktoren

Lebenslanges Lernen ist Grundvoraussetzung

Der moderne CISO

Fragen & Diskussion

- Wie erlebt ihr die CISO-Rolle in euren Organisationen?
- Was sind eure größten Herausforderungen aktuell?
- Wo wünscht ihr euch mehr Unterstützung?

CISO Excellence Programm

20. Mai – 12. Juni 2026

bitkom akademie