Cybersicherheitsmanagement vs. Cyberkriminalität: Von der Kriminalistik lernen!

Reinhold Hepp,
Polizeivizepräsident a.D.

Prof. Dr. Markus Schäffter,
Technische Hochschule Ulm

Cybersicherheitsmanagement vs. Cyberkriminalität:
Von der Kriminalistik lernen!

Dieser Vortrag besteht aus zwei konsekutiven Teilen:

- Kriminalistischer Ansatz im Risikomanagement:
  Kombination der Lageberichte zur Cybersicherheit mit Konzepten und Erfahrungen Kriminalitäts- und Sicherheitsanalyse, um IT-Risiken zu identifizieren und zu priorisieren.

- Agiler kontinuierlicher Verbesserungsprozess (A-KVP):
  Gegen die zentralen IT-Risiken wirksame Schutzmaßnahmen effizient und effektiv umsetzen durch Anwendung der positiven Ansätze des agilen Projektmanagements.

Cybersicherheitsmanagement vs. Cyberkriminalität:
Von der Kriminalistik lernen!

Einige Zahlen zur Motivation:

- 72% von 1002 von der Bitkom befragten Unternehmen wurden in den letzten 12 Monaten erfolgreich angegriffen.
- 40% von 702 von der HDI befragten KMU wurden in den letzten 12 Monaten erfolgreich angegriffen. Tendenz zu Angriffen auf kleinere KMU ist erkennbar!
- 80% der Bildungseinrichtungen waren von Ransomware betroffen, eine Zunahme um ca. +60% im Vergleich zum Vorjahr.

Quellen:
Wirtschaftsschutz 2023, Bitkom e.V.
HDI Cyberstudie 2023, HDI Deutschland AG
State of Ransomware in Education 2023 (Sophos)

Cybersicherheitsmanagement vs. Cyberkriminalität:
Von der Kriminalistik lernen!

Einschub: Das ist nichts Neues!

Common Criteria bemisst das Angriffspotenzial qualitativ & quantitativ:

als Zeit + Expertise + Wissen + Gelegenheit + Ausrüstung + Motivation,
die Täter für einen erfolgreichen Angriff aufbringen müssen!

Factor	Range	Value
Time (elapsed time)	≤ 1 day	0
	≤ 1 week	1
	≤ 2 weeks	2
	≤ 1 month	4
	≤ 2 months	7
	≤ 3 months	10
	≤ 4 months	13
Expertise	Layman	0
	Proficient	3
	Expert	6
	Multiple experts	8
	Restricted	3
	Sensitive	7
	Critical	11

Quellen: TVRA Risk Calculation Template

Cybersicherheitsmanagement vs. Cyberkriminalität:
Von der Kriminalistik lernen!

Kernaussagen aus kriminalistischer Sicht:

- Immense Schäden durch kriminelles Verhalten (Bitkom-Studie 2023):
  - 206 Mrd. Euro durch Diebstahl von IT-Ausrüstung und Daten sowie digitale und Industriespionage
  - 146 Mrd. EUR durch Cyberattacken – Phishing mit 31% an der Spitze
  - Deutlicher Anstieg von Schäden durch Ransomware
- Schäden entstehen nicht durch unzureichende Technik, sondern durch kriminelles Verhalten von Tätern!
- Zunehmende Tatbegehung durch organisierte Banden!

Cybersicherheitsmanagement vs. Cyberkriminalität:
Von der Kriminalistik lernen!

Teil 1: Kriminalprävention in der Cybersicherheit

Cybercrime: Straftaten, die sich gegen IT-Systeme, Datennetze und/oder Daten richten.

Cyberangriffe: Kriminalitätsphänomen mit enormem Schadenspotenzial

Cybersicherheitsmanagement vs. Cyberkriminalität:
Von der Kriminalistik lernen!

Entstehungsbedingungen und kriminalitätsfördernde Faktoren:

- die Tatgelegenheit: „Gelegenheit macht Diebe“
- der Tataufwand: Die Tat muss für den Täter durchführbar sein
- der Tatertrag: Kriminalität muss sich lohnen
- das Täterrisiko: Ergreifung muss unwahrscheinlich sein, bei Einbruch gibt Täter nach 3- 5 Minuten auf

Cybersicherheitsmanagement vs. Cyberkriminalität:
Von der Kriminalistik lernen!

Kernaussagen aus kriminalistischer Sicht:

- Angriffe im digitalen Raum werden zunehmen:
  - Eindeutiger Trend zum Diebstahl von Daten (kriminelle Infrastruktur zur Vermarktung) Achtung: Reputationsverlust und Sanktionen für Betroffene
  - 8 von 10 Unternehmen erwarten mehr Cyberangriffe!
    Achtung: Kriminalitätsfurcht(?) – Bedrohungsgefühl KMU
- Zunehmend Angriffe auf KMU, Kommunen, Gesundheits- und Bildungseinrichtungen (Universitäten, Hochschulen, Schulen)!

Cybersicherheitsmanagement vs. Cyberkriminalität:
Von der Kriminalistik lernen!

Kernaussagen aus kriminalistischer Sicht (Forts.):

- Tätertypen sind weit gefächert:
  - Staatlichen Akteure, organisierte Banden, Berufsverbrecher
  - Script-Kiddies und Aktivisten
  - bis hin zu Innentätern
- Ist eine täterorientierte Prävention wirkungsvoll möglich?
- Situative Prävention unverzichtbar: Tatgelegenheit erschweren, Tatertrag reduzieren und Täterrisiko erhöhen
- Ganzheitliches und bedarfsorientiertes-risikoorientiertes Schutzkonzept (nicht mit der „Schrotflinte“ bzw. „Gießkanne“): Technik – Verhalten (Stichwort Phishing) und Organisation

Cybersicherheitsmanagement vs. Cyberkriminalität:
Von der Kriminalistik lernen!

Kernaussagen aus kriminalistischer Sicht (Forts.):

- Wirkungsvolles Schutzkonzept erfordert umfassende Status Quo Feststellung:
  - Tatgelegenheit erschweren / Cyber-Resilienz erhöhen
  - Klare Managementaufträge: Verantwortung delegieren (ISB, IT-Leitung), Beschäftigte unterrichten
  - Tatertrag reduzieren: kein Lösegeld + Prävention + Notfallpläne
  - Tataufwand erhöhen: mehr Wissen, Zeit,… zur Kompromittierung

Cybersicherheitsmanagement vs. Cyberkriminalität:
Von der Kriminalistik lernen!

Kernaussagen aus kriminalistischer Sicht (Forts.):

- Fortlaufende Kontrolle des Status Quo, kontinuierliche Anpassung an die Gefährdungslage
- Bedarfsorientierte Prävention: IT-Grundschutz/ISO 27000/KRITIS, angepasst an Bedrohungslage und an Sicherheitsniveau der Peer-Group!
- Parallel: Polizei in Bund und Ländern zerstören kriminelle Infrastrukturen, stellen kriminelle Erträge sicher

Cybersicherheitsmanagement vs. Cyberkriminalität:
Von der Kriminalistik lernen!

Fazit aus Sicht der Kriminalistik

- **Prozessevaluation**
  Umsetzung von technischen, verhaltensbezogenen und organisatorischen Schutzmaßnahmen zur gezielten Schadensprävention und zur schnellen (effizienten) und effektiven Bekämpfung von Cyberangriffen und IT-Vorfällen.

- **Wirkungsevaluation**
  Prüfen, inwieweit die umgesetzten organisatorischen Maßnahmen zu einer risikoreduzierenden Veränderung im Verhalten bzw. bei technischen Maßnahmen zu einer Verringerung des Risikos (Schadenseintritt / Schadenswirkung) führen.

Cybersicherheitsmanagement vs. Cyberkriminalität:
Von der Kriminalistik lernen!

Teil 2: Agiles Sicherheitsmanagement

Auswirkungen des Agilen Manifests auf das Sicherheitsmanagement:

- Individuen und Interaktionen sind mehr als Prozesse und Werkzeuge
  - Risiken durch gezielte Maßnahmen reduzieren, statt Katalogen blind zu folgen! Vergleiche Teil 1: Identifikation & Priorisierung!
  - Beispiele: Netzwerke segmentieren, Systemkonfigurationen sichern, Nutzende schulen = kein Selbstzweck, sondern Weg zum Ziel!
- Fortlaufende Funktionalität des Produkts
  - Schutzmaßnahmen fortlaufend an die sich ändernde Gefährdungslage anpassen!

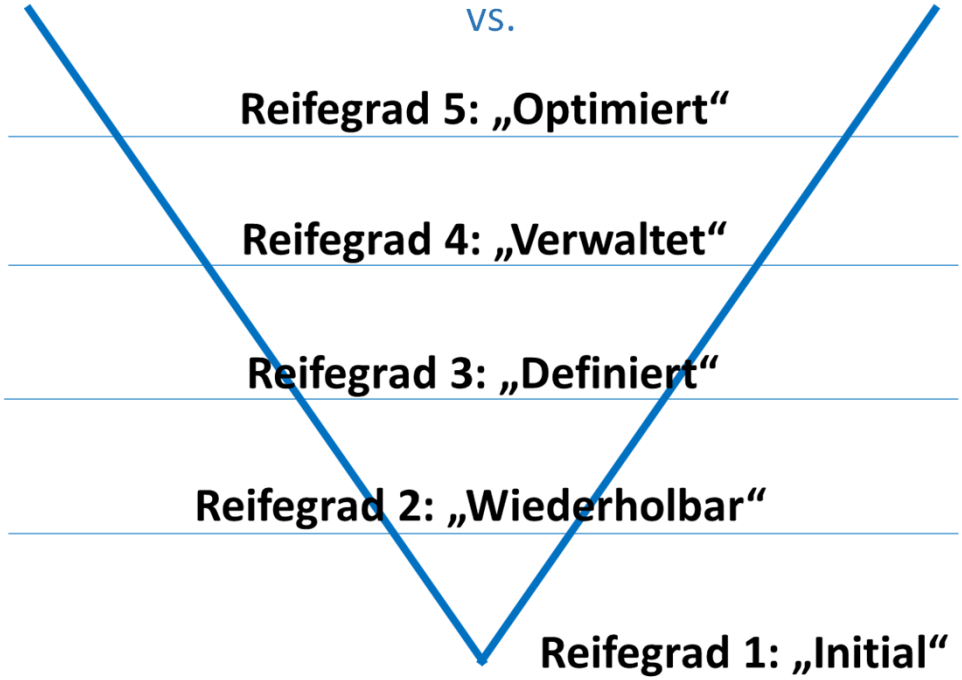
Cybersicherheitsmanagement vs. Cyberkriminalität:
Von der Kriminalistik lernen!

Agilität im Cybersicherheitsmanagement erreichen:

Entscheidend: Den Reifegrad berücksichtigen!

Reifegrad des Sicherheits-Management-systems

vs.



Reifegrad der Schutzmaßnahmen

Quellen:
Capability Maturity Model (CMM)
Autoren (V-Modell)

Cybersicherheitsmanagement vs. Cyberkriminalität:
Von der Kriminalistik lernen!

Selbsteinschätzung: Welchen Reifegrad hat Ihre Organisation?

Level 1	Level 2	Level 3	Level 4	Level 5
Initial	Wiederholbar	Definiert	Verwaltet	Optimiert
Prozesse sind undefiniert, Reaktion erfolgt jedes Mal neu	Einzelne Prozesse sind definiert, Reaktion erfolgt wiederholbar	Prozesse sind umfassend, Reaktion erfolgt standardisiert	Prozesse werden überwacht, Umsetzung wird kontrolliert	Prozesse werden kontinuierlich verbessert

Quellen:
Capability Maturity Model (CMM)

Cybersicherheitsmanagement vs. Cyberkriminalität:
Von der Kriminalistik lernen!

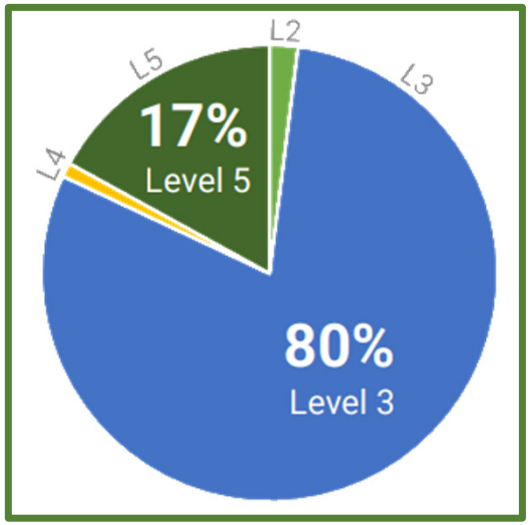
Umfrage: Welchen Reifegrad hat Ihre Organisation entweder bewusst gewählt oder bereits erreicht?

Cybersicherheitsmanagement vs. Cyberkriminalität:
Von der Kriminalistik lernen!

Welchen Reifegrad haben andere Organisationen?

Von ca. 9.000 befragten Organisationen als Ziel gewählte Reifegrade :

- 80% CMMI Level 3
- 17% CMMI Level 5



Quelle: CMMI Technical Report: Performance Results, ISACA April 2023
https://cmmiinstitute.com/getattachment/738104c0-a6f0-4e1c-8bbe-35076b75f36e/attachment.aspx

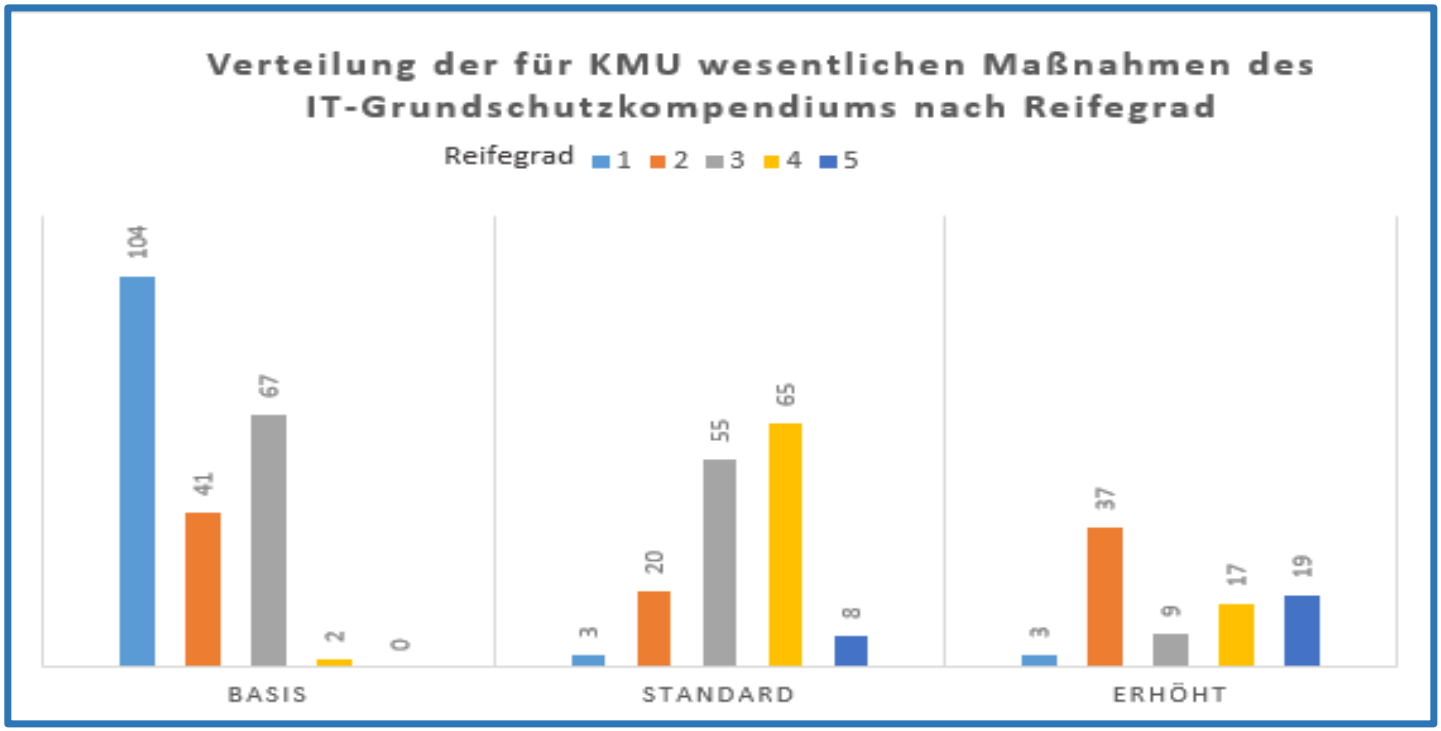
Cybersicherheitsmanagement vs. Cyberkriminalität:
Von der Kriminalistik lernen!

Welche Reifegrade verlangt/erreicht der IT-Grundschutz?

Reifegrad	Tätigkeiten/Kriterien
1 Initial	ausführen, durchführen, umsetzen, einrichten, berücksichtigen, prüfen, testen, informieren, sicherstellen. Anleitungen/Checklisten/Methodiken werden angewendet, aber nicht systematisch.
2 Wiederholbar	wiederholt, regelmäßig, systematisch, untersuchen, zeitnah, identifizieren, festlegen, korrelieren, Verantwortliche benennen, Handbücher, Leitfäden, Anleitungen erstellen, Abläufe definieren.
3 Definiert	regeln, dokumentieren, protokollieren, nachweisen, einstufen, freigeben, Konzepte/Richtlinien erstellen, Prinzipien anwenden, Vereinbarungen treffen.

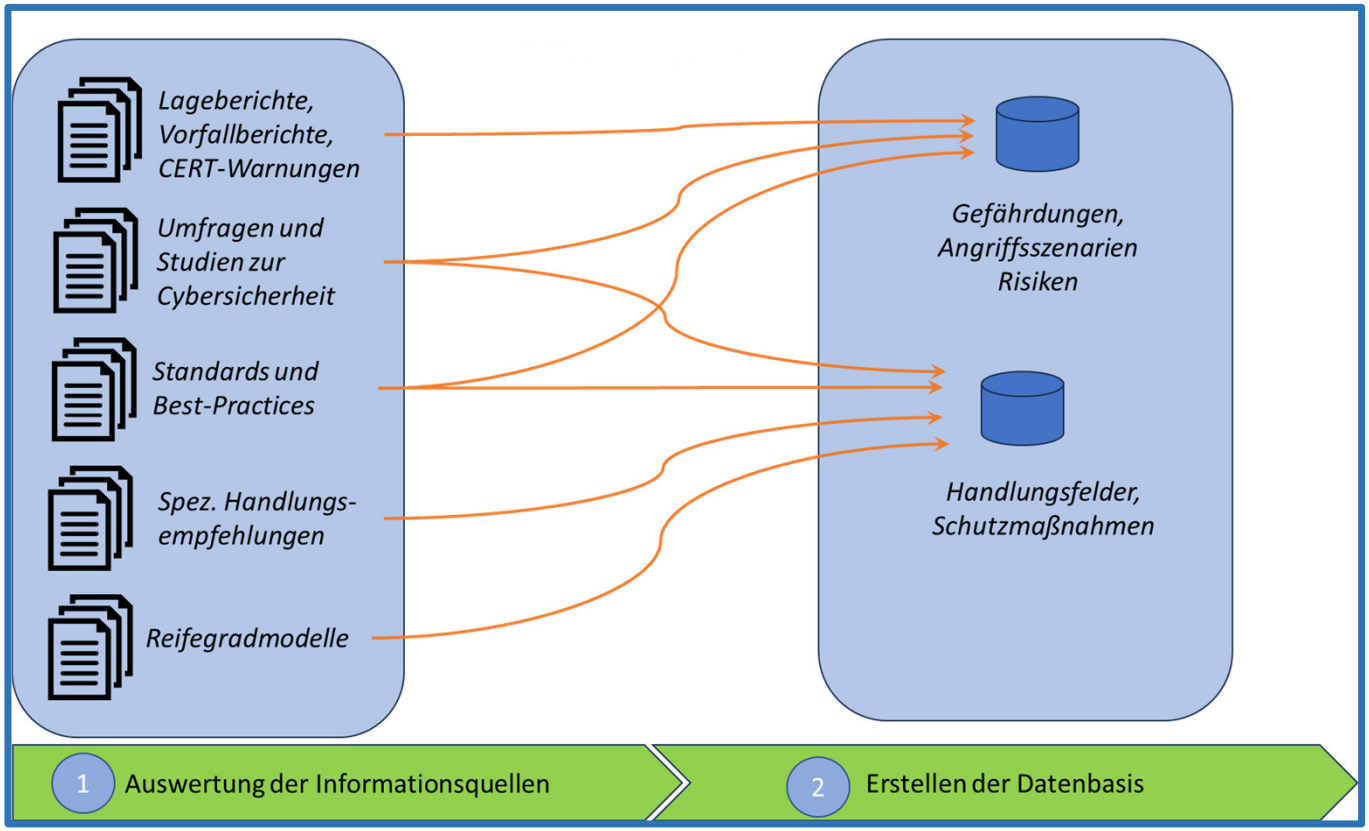
Cybersicherheitsmanagement vs. Cyberkriminalität:
Von der Kriminalistik lernen!

Reifegrade von 450 für KMU (besonders) relevante IT-Grundschutzmaßnahmen



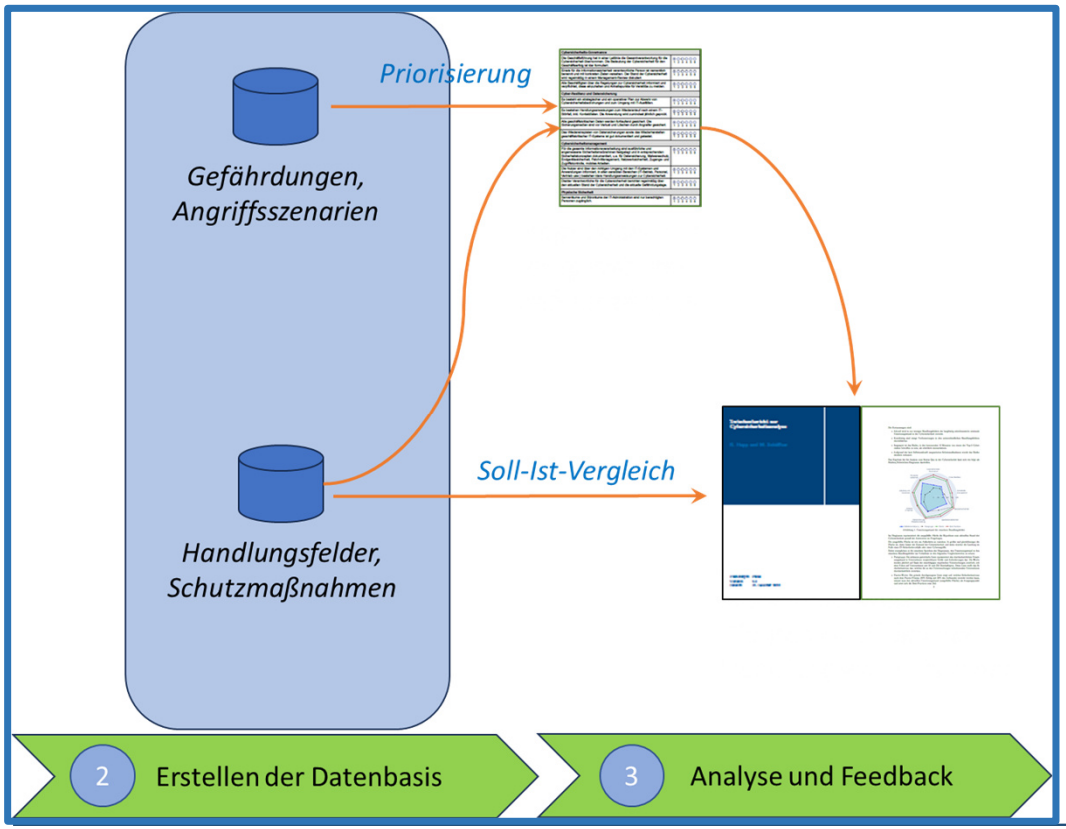
Cybersicherheitsmanagement vs. Cyberkriminalität:
Von der Kriminalistik lernen!

Unser Lösungsansatz: Sicherheitsanalyse auf Basis einer Meta-Studie



Cybersicherheitsmanagement vs. Cyberkriminalität:
Von der Kriminalistik lernen!

Unser Lösungsansatz: Umfassendes Feedback

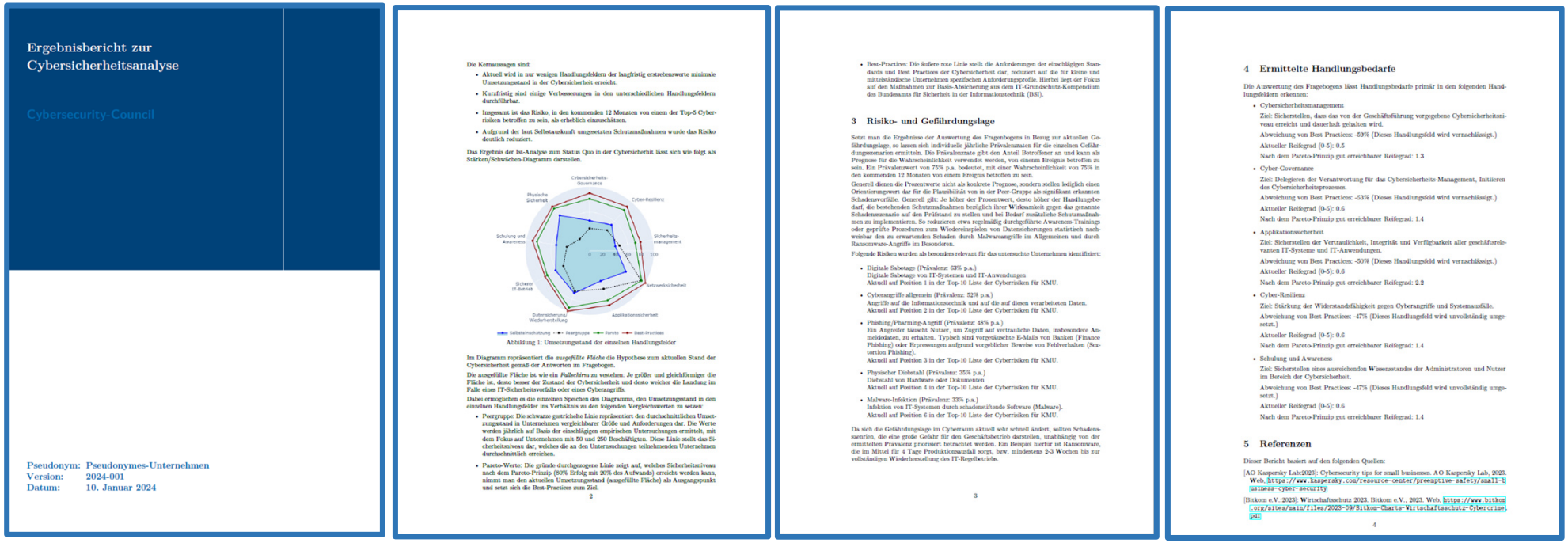


Feedback:

- Einschätzung des Umsetzungsstands
- Reifegrad der Organisation
- Stärken/Schwächen-Diagramm
- Risiko- und Gefährdungslage
- Handlungsempfehlungen:
  konkret / basierend auf Risikolage (vgl. Teil 1)

Cybersicherheitsmanagement vs. Cyberkriminalität:
Von der Kriminalistik lernen!

Unser Lösungsansatz: Zielgerichteter (kurzer) Bericht



Ergebnisbericht zur Cybersicherheitsanalyse

Cybersecurity Council

Pseudonym: Pseudonymes-Unternehmen
Version: 2024-001
Datum: 10. Januar 2024

Die Kernaussagen sind:

- Aktuell wird in nur wenigen Handlungsfeldern der langfristig erstrebenswerte minimale Umsetzungsstand in der Cybersicherheit erreicht.
- Kurzfristig sind einige Verbesserungen in den unterschiedlichen Handlungsfeldern durchführbar.
- Insgesamt ist das Risiko, in den kommenden 12 Monaten von einem der Top-5 Cyberrisiken betroffen zu sein, als erheblich einzuschätzen.
- Aufgrund der laut Selbstauskunft umgesetzten Schutzmaßnahmen wurde das Risiko deutlich reduziert.

Das Ergebnis der Ist-Analyse zum Status Quo in der Cybersicherhit lässt sich wie folgt als Stärken/Schwächen-Diagramm darstellen.

Abbildung 1: Umsetzungstand der einzelnen Handlungsfelder

Im Diagramm repräsentiert die *ausgefüllte Fläche* die Hypothese zum aktuellen Stand der Cybersicherheit gemäß der Antworten im Fragebogen.

Die ausgefüllte Fläche ist wie ein *Fallschirm* zu verstehen: Je größer und gleichförmiger die Fläche ist, desto besser der Zustand der Cybersicherheit und desto weicher die Landung im Falle eines IT-Sicherheitsvorfalls oder eines Cyberangriffs.

Dabei ermöglichen es die einzelnen Speichen des Diagramms, den Umsetzungstand in den einzelnen Handlungsfelder ins Verhältnis zu den folgenden Vergleichswerten zu setzen:

- Peergruppe: Die schwarze gestrichelte Linie repräsentiert den durchschnittlichen Umsetzungstand in Unternehmen vergleichbarer Größe und Anforderungen dar. Die Werte werden jährlich auf Basis der einschlägigen empirischen Untersuchungen ermittelt, mit dem Fokus auf Unternehmen mit 50 und 250 Beschäftigten. Diese Linie stellt das Sicherheitsniveau dar, welches die an den Untersuchungen teilnehmenden Unternehmen durchschnittlich erreichen.
- Pareto-Werte: Die gründe durchgezogene Linie zeigt auf, welches Sicherheitsniveau nach dem Pareto-Prinzip (80% Erfolg mit 20% des Aufwands) erreicht werden kann, nimmt man den aktuellen Umsetzungsstand (ausgefüllte Fläche) als Ausgangspunkt und setzt sich die Best-Practices zum Ziel.

2

- Best-Practices: Die äußere rote Linie stellt die Anforderungen der einschlägigen Standards und Best Practices der Cybersicherheit dar, reduziert auf die für kleine und mittelständische Unternehmen spezifischen Anforderungsprofile. Hierbei liegt der Fokus auf den Maßnahmen zur Basis-Absicherung aus dem IT-Grundschutz-Kompendium des Bundesamts für Sicherheit in der Informationstechnik (BSI).

3 Risiko- und Gefährdungslage

Setzt man die Ergebnisse der Auswertung des Fragenbogens in Bezug zur aktuellen Gefährdungslage, so lassen sich individuelle jährliche Prävalenzraten für die einzelnen Gefährdungsszenarien ermitteln. Die Prävalenzrate gibt den Anteil Betroffener an und kann als Prognose für die Wahrscheinlichkeit verwendet werden, von einem Ereignis betroffen zu sein. Ein Prävalenzwert von 75% p.a. bedeutet, mit einer Wahrscheinlichkeit von 75% in den kommenden 12 Monaten von einem Ereignis betroffen zu sein.

Generell dienen die Prozentwerte nicht als konkrete Prognose, sondern stellen lediglich einen Orientierungswert dar für die Plausibilität von in der Peer-Gruppe als signifikant erkannten Schadensvorfälle. Generell gilt: Je höher der Prozentwert, desto höher der Handlungsbedarf, die bestehenden Schutzmaßnahmen bezüglich ihrer Wirksamkeit gegen das genannte Schadensszenario auf den Prüfstand zu stellen und bei Bedarf zusätzliche Schutzmaßnahmen zu implementieren. So reduzieren etwa regelmäßig durchgeführte Awarenes-Trainings oder geprüfte Prozeduren zum Wiedereinspielen von Datensicherungen statistisch nachweisbar den zu erwartenden Schaden durch Malwareangriffe im Allgemeinen und durch Ransomware-Angriffe im Besonderen.

Folgende Risiken wurden als besonders relevant für das untersuchte Unternehmen identifiziert:

- Digitale Sabotage (Prävalenz: 63% p.a.)
  Digitale Sabotage von IT-Systemen und IT-Anwendungen
  Aktuell auf Position 1 in der Top-10 Liste der Cyberrisiken für KMU.
- Cyberangriffe allgemein (Prävalenz: 52% p.a.)
  Angriffe auf die Informationstechnik und auf die auf diesen verarbeiteten Daten.
  Aktuell auf Position 2 in der Top-10 Liste der Cyberrisiken für KMU.
- Phishing/Pharming-Angriff (Prävalenz: 48% p.a.)
  Ein Angreifer täuscht Nutzer, um Zugriff auf vertrauliche Daten, insbesondere Anmeldedaten, zu erhalten. Typisch sind vorgetäuschte E-Mails von Banken (Finance Phishing) oder Erpressungen aufgrund vorgeblicher Beweise von Fehlverhalten (Sextortion Phishing).
  Aktuell auf Position 3 in der Top-10 Liste der Cyberrisiken für KMU.
- Physischer Diebstahl (Prävalenz: 35% p.a.)
  Diebstahl von Hardware oder Dokumenten
  Aktuell auf Position 4 in der Top-10 Liste der Cyberrisiken für KMU.
- Malwaro-Infektion (Prävalenz: 33% p.a.)
  Infektion von IT-Systemen durch schadenstiftende Software (Malware).
  Aktuell auf Position 6 in der Top-10 Liste der Cyberrisiken für KMU.

Da sich die Gefährdungslage im Cyberraum aktuell sehr schnell ändert, sollten Schadensszenarien, die eine große Gefahr für den Geschäftsbetrieb darstellen, unabhängig von der ermittelten Prävalenz priorisiert betrachtet werden. Ein Beispiel hierfür ist Ransomware, die im Mittel für 4 Tage Produktionsausfall sorgt, bzw. mindestens 2-3 Wochen bis zur vollständigen Wiederherstellung des IT-Regelbetriebs.

3

4 Ermittelte Handlungsbedarfe

Die Auswertung des Fragebogens lässt Handlungsbedarfe primär in den folgenden Handlungsfeldern erkennen:

- Cybersicherheitsmanagement
  Ziel: Sicherstellen, dass das von der Geschäftsführung vorgegebene Cybersicherheitsniveau erreicht und dauerhaft gehalten wird.
  Abweichung von Best Practices: -59% (Dieses Handlungsfeld wird vernachlässigt.)
  Aktueller Reifegrad (0-5): 0.5
  Nach dem Pareto-Prinzip gut erreichbarer Reifegrad: 1.3
- Cyber-Governance
  Ziel: Delegieren der Verantwortung für das Cybersicherheits-Management, Initiieren des Cybersicherheitsprozesses.
  Abweichung von Best Practices: -53% (Dieses Handlungsfeld wird vernachlässigt.)
  Aktueller Reifegrad (0-5): 0.6
  Nach dem Pareto-Prinzip gut erreichbarer Reifegrad: 1.4
- Applikationssicherheit
  Ziel: Sicherstellen der Vertraulichkeit, Integrität und Verfügbarkeit aller geschäftsrelevanten IT-Systeme und IT-Anwendungen.
  Abweichung von Best Practices: -50% (Dieses Handlungsfeld wird vernachlässigt.)
  Aktueller Reifegrad (0-5): 0.6
  Nach dem Pareto-Prinzip gut erreichbarer Reifegrad: 2.2
- Cyber-Resilienz
  Ziel: Stärkung der Widerstandsfähigkeit gegen Cyberangriffe und Systemausfälle.
  Abweichung von Best Practices: -47% (Dieses Handlungsfeld wird unvollständig umgesetzt.)
  Aktueller Reifegrad (0-5): 0.6
  Nach dem Pareto-Prinzip gut erreichbarer Reifegrad: 1.4
- Schulung und Awareness
  Ziel: Sicherstellen eines ausreichenden Wissensstandes der Administratoren und Nutzer im Bereich der Cybersicherheit.
  Abweichung von Best Practices: -47% (Dieses Handlungsfeld wird unvollständig umgesetzt.)
  Aktueller Reifegrad (0-5): 0.6
  Nach dem Pareto-Prinzip gut erreichbarer Reifegrad: 1.4

5 Referenzen

Dieser Bericht basiert auf den folgenden Quellen:

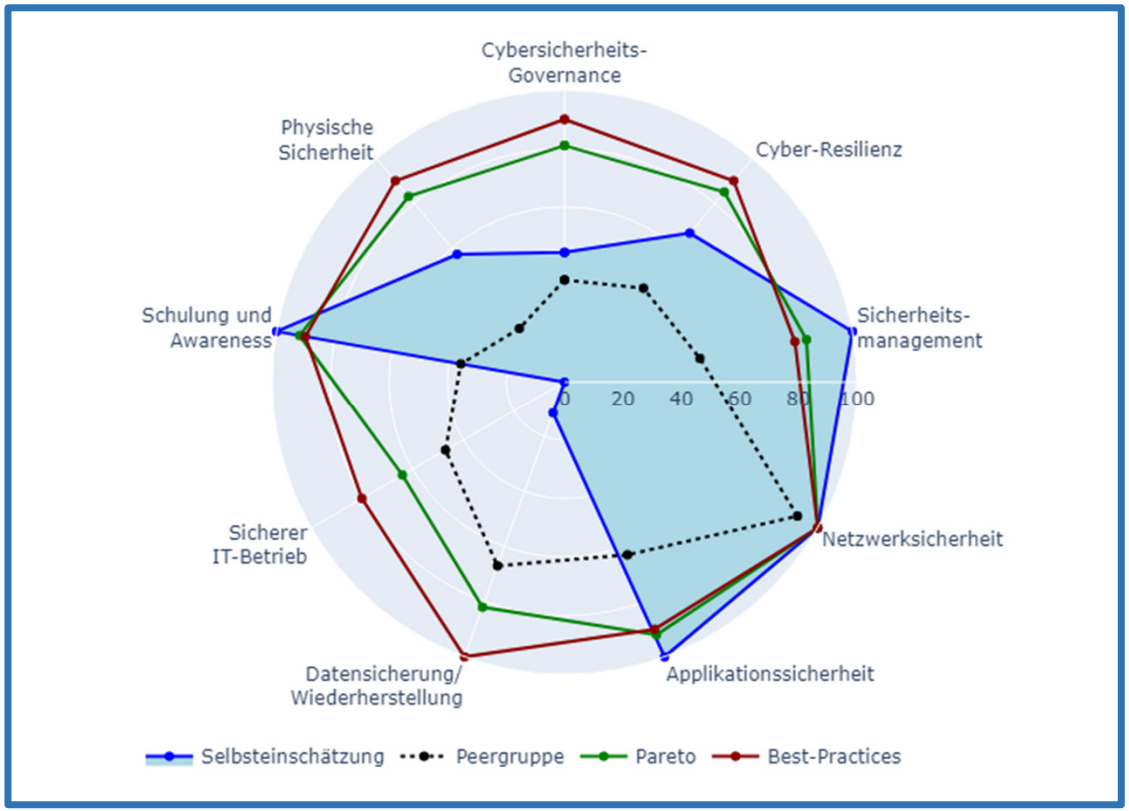
[AO Kaspersky Lab:2023]: Cybersecurity tips for small businesses. AO Kaspersky Lab, 2023. Web, https://www.kaspersky.com/resource-center/preemptive-safety/small-business-cyber-security

[Bitkom e.V.:2023]: Wirtschaftsschutz 2023. Bitkom e.V., 2023. Web, https://www.bitkom.org/sites/main/files/2023-09/Bitkom-Charts-Wirtschaftsschutz-Cybercrime.pdf

4

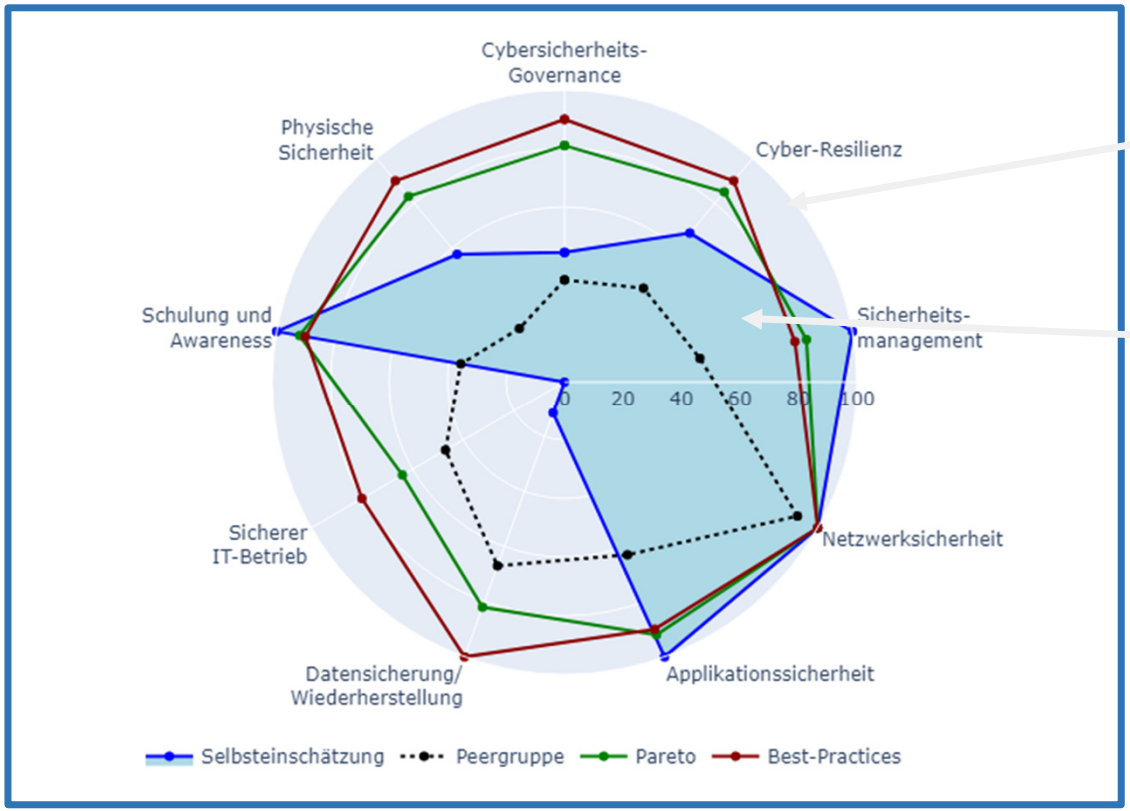
Cybersicherheitsmanagement vs. Cyberkriminalität:
Von der Kriminalistik lernen!

Ein wesentlicher Bestandteil: das Stärken-Schwächen-Diagramm!



Cybersicherheitsmanagement vs. Cyberkriminalität:
Von der Kriminalistik lernen!

Ein wesentlicher Bestandteil: das Stärken-Schwächen-Diagramm!



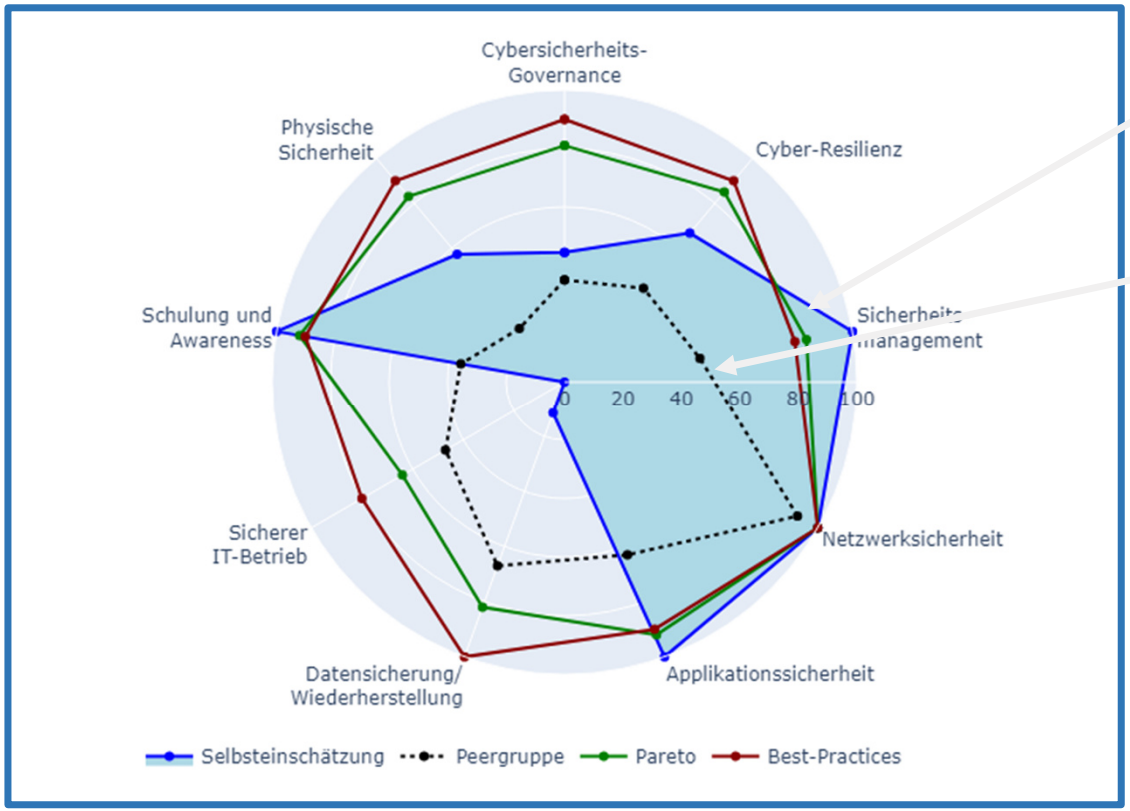
Kreislinie: 100%-Erfüllung Anforderungen des IT-Grundschutzes (Standard)

Ausgefüllte Fläche: Umsetzungsstand nach Auswertung des Fragebogens (Vorsicht: Selbstauskunft!)

Metapher: Fallschirm, schützt vor hohen Stürzen!

Cybersicherheitsmanagement vs. Cyberkriminalität:
Von der Kriminalistik lernen!

Ein wesentlicher Bestandteil: das Stärken-Schwächen-Diagramm!



Ausgefüllte Fläche:
Umsetzungsstand in der Organisation

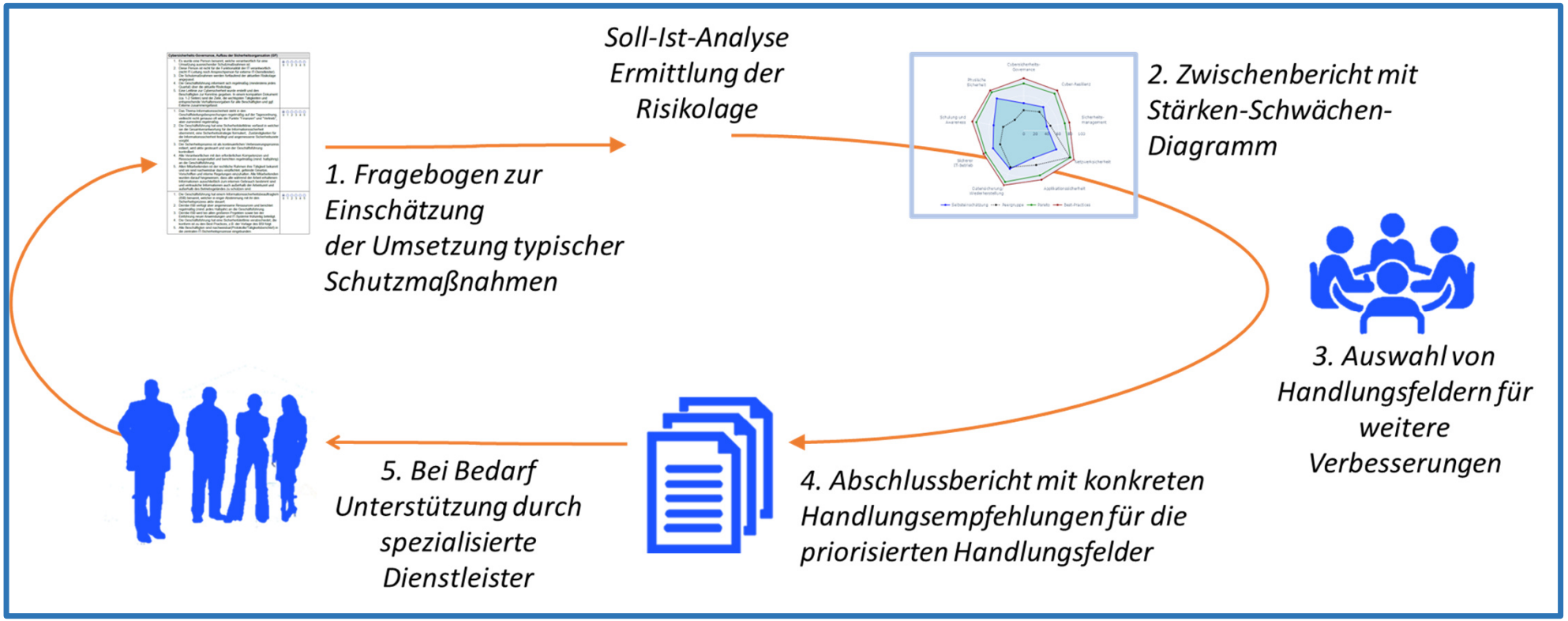
Gestrichelte Linie:
Umsetzungsstand der Peer-Gruppe
(hier: KMU mit vglb. #Mitarbeitenden)

Rote Linie:
Anforderungen IT-Grundschutz für
KMU (Studien, Empfehlungen)

Grüne Linie:
Erreichbar gemäß Pareto-Prinzip

Cybersicherheitsmanagement vs. Cyberkriminalität:
Von der Kriminalistik lernen!

Unser Lösungsansatz: Agiles Management durch fortgesetzte Analyse



Cybersicherheitsmanagement vs. Cyberkriminalität:
Von der Kriminalistik lernen!

Herzlichen Dank für Ihre Aufmerksamkeit!

Reinhold Hepp

Polizeivizepräsident a.D., z. Zt. Ministerium des Innern, für Digitalisierung und Kommunen Baden-Württemberg

Reinhold.Hepp@web.de

Dr. Markus Schäffter

Professor für Informationssicherheit & Datenschutz
Technische Hochschule Ulm

Markus.Schaeffter@thu.de