Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

Bundesamt für Cybersicherheit BACS

Best Practices in der Cybersicherheit

Bundesamt für Cybersicherheit Schweiz

4. November 2025

Zur Person

Andreas Grünert

Experte für IT und Informationssicherheit

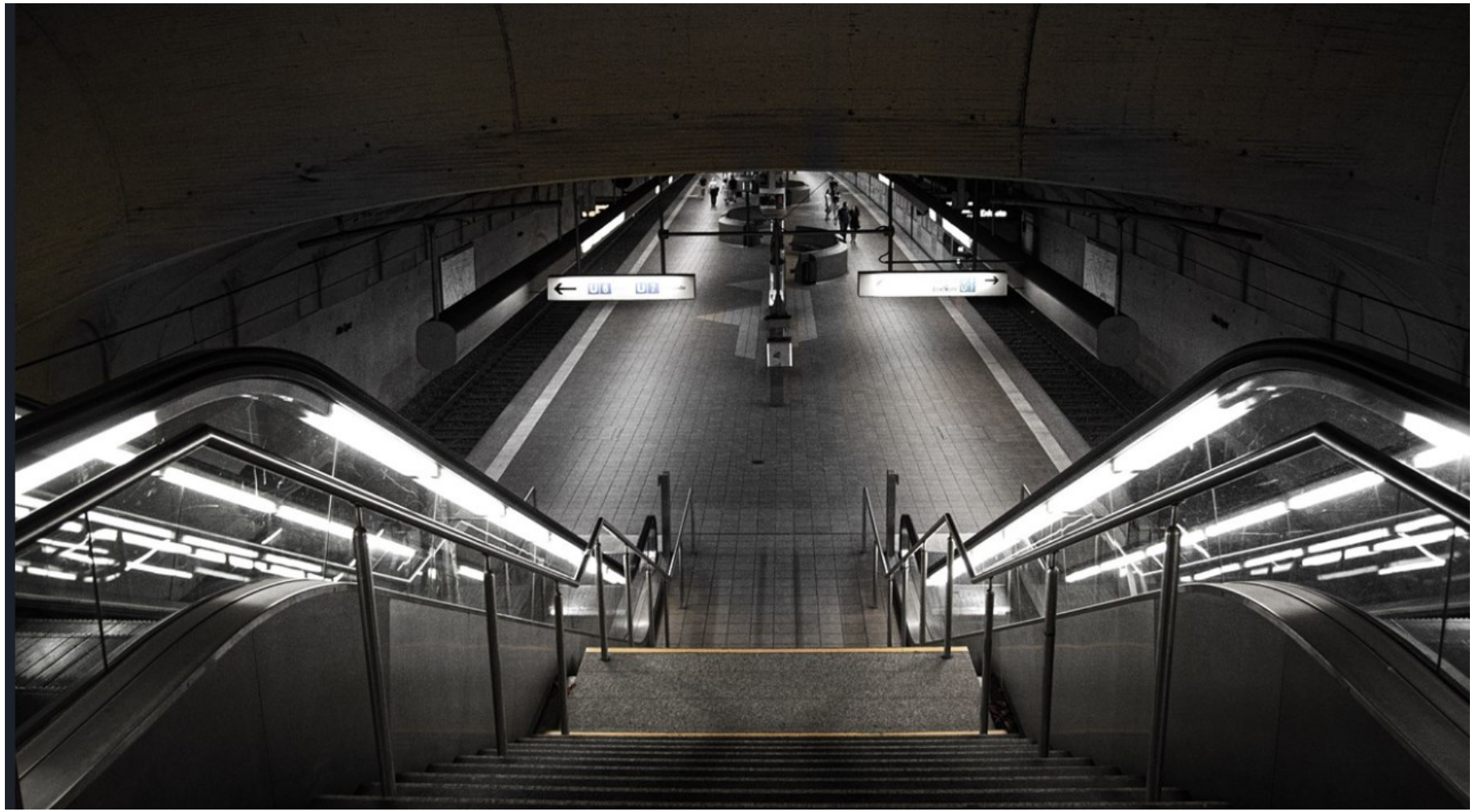
BSc IT Security BFH Biel/Bienne;
MSc Information Security ISG Royal Holloway, London; CISSP

- 7 Jahre Verantwortlicher IT-Infrastruktur und Sicherheit bei einer Hotelkette in Südostasien
- 4 Jahre Leiter Risikomanagement für ein Bezahlsystemanbieter in Thailand, Japan und Singapore
- Seit Mai 2022 Informatiksicherheitsbeauftragter Bund im Nationalen Zentrum für Cybersicherheit (NCSC), GS-EFD
- Seit Juni 2023 Leiter Team Technologien und Security Engineering, NCSC / BACS Schweiz

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS
Bundesamt für Cybersicherheit BACS
Leiter Technologien und Security Engineering

Schwarztorstrasse 59, 3003 Bern
Tel. +41 79 707 83 37
Threema E2J2JTWD
andreas.gruenert@ncsc.admin.ch
http://www.ncsc.admin.ch

Rennen oder warten?

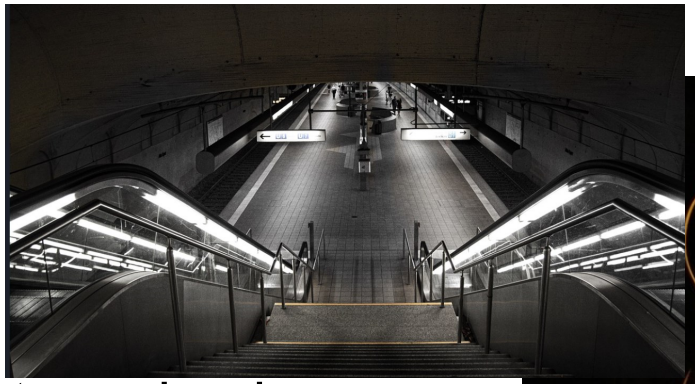


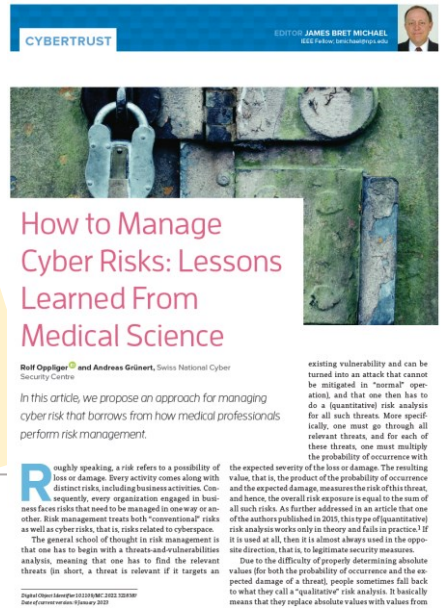
Teil 1: Einleitung

- Eine **Best Practice** ist eine bewährte Methode, Vorgehensweise oder Technologie, mit der bestimmte – meist komplexe – Ziele erreicht werden können
- Je komplexer und mehrdimensionaler diese Ziele sind, umso wichtiger sind Best Practices
- Meist basieren sie auf **heuristischen** (Lösungs-) Ansätzen und Verfahren (statt analytischen)
- Best Practices und entsprechende **Heuristiken** spielen im täglichen Leben eine grosse Rolle (Unterbewusstsein/«Bauchgefühl» statt Berechnungen)
- Viele Tätigkeiten basieren auf Methoden und Vorgehensweisen, die sich im Laufe der Zeit herausgebildet und bewährt haben

Einleitung

- Beispiele
  - Abschätzung, ob ein Zug noch erreicht werden kann
  - Abschätzung, ob bei einem Wechsel von grün auf orange bei einer Ampel beschleunigt oder gebremst werden soll
  - Schliessen der Fenster und Abschliessen der Haustüre beim Verlassen eines Hauses oder einer Wohnung (als Einbruchschutz)
  - Viele heuristische Verfahren, die in der Medizin eingesetzt werden, um die Gesundheit einer Patientin oder eines Patienten zu gewährleisten oder zu verbessern





Medizinisches Personal desinfiziert regelmässig die Hände

Bakterielle Infekte werden mit Antibiotika behandelt

Stark ansteckende Patientinnen und Patienten werden in Quarantäne gehalten

Patientinnen und Patienten mit Herzerkrankungen wird ein gesunder Lebensstil mit ausgewogener Ernährung und regelmässiger körperlicher Bewegung auferlegt

Einleitung

- Weil das Adjektiv «best» Optimalität suggeriert, ohne dass klar ist, nach was optimiert werden soll, wird auch etwa der Begriff **Good Practice** (anstelle von Best Practice) verwendet
- Im Gegensatz zu einer Best Practice kann sich eine Good Practice im Laufe der Zeit auch weiterentwickeln («moving target»)
- Damit ist eine Good Practice eine **Best Current Practice (BCP)**
- Dieser Begriff wird auch von der IETF verwendet (z. B. RFC 1918 ≅ BCP 5 für die Verwendung von privaten IP Adressen)
- Im folgenden werden Best | Good | Best Current Practices summarisch als **Good Practices** bezeichnet (die terminologische Feinheit bleibt aber bestehen)

Einleitung

- Aus dem Begriff der **Cybersicherheit** lassen sich viele (komplexe und mehrdimensionale) Ziele ableiten
  - Vertraulichkeit von Daten
  - Integrität von Daten und Berechnungen
  - Verfügbarkeit von Daten und anderen IT-Mitteln
  - …
- Entsprechend bieten sich Good Practices auch in der Cybersicherheit (und Resilienz) an
- Allerdings müssen diese genau spezifiziert sein
- Aussagen wie *«unsere Sicherheit basiert auf Good | Best Practices»* oder *«wir orientieren uns an Good | Best Practices»* sind belanglos (Plattitüden) und sollten vermieden bzw. präzisiert werden

Teil 2: Beispiele

- Beim BACS machen wir uns Gedanken wie wir mit Good Practices die Unternehmen und Organisationen in der Schweiz unterstützen können
  - Auf der **Managementebene** als Methoden oder (strukturierte) Vorgehens-weisen zur Stärkung der Cybersicherheit und Resilienz
  - Auf der **technischen Ebene** als technische und organisatorische Massnahmen (TOMs)
- Dazu explorieren wir mögliche Einsatzgebiete und begleitet entsprechende Piloten.
- Wir entwickeln also auch neue und innovative Ansätze, einige davon wollen wir euch heute vorstellen.
- Diese sind Good, im Sinne das sie der Cyber-sicherheit und Resilienz zudienen, nicht aber, weil sie bereits bewährte Vorgehensweisen wären. Dies wird sich erst im praktischen Einsatz zeigen.

Good Practice: Berücksichtigung der Resilienz

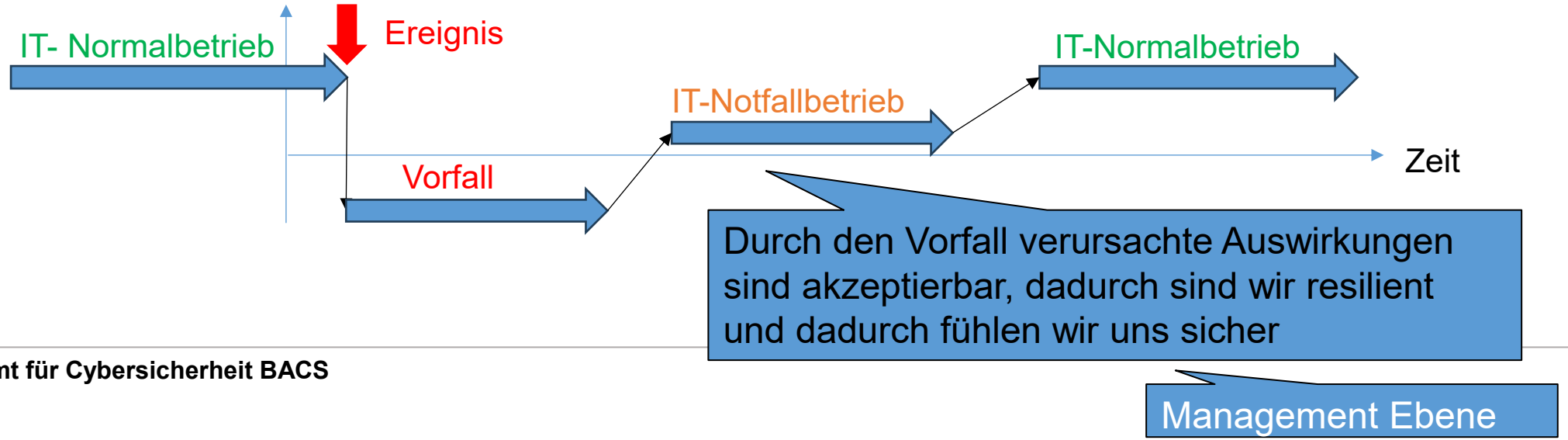
Schildkröte ≈ Sicherheit

Axolotl ≈ Resilienz

Good Practice: Berücksichtigung der Resilienz

Wir sind resilient: Wenn wir nur akzeptierbare Auswirkungen erleiden können.
Dazu gehört

- Das Kennen der akzeptierbaren Auswirkungen.
- Das Verhindern, dass Vorfälle dazu führen können, dass die akzeptierbaren Auswirkungen überschritten werden
- Das Vorbereiten und Sicherstellen von entsprechenden Reaktionsfähigkeiten.

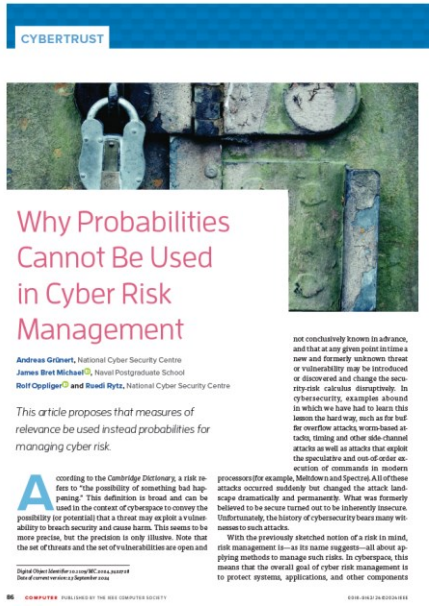


Good Practice: Methode anstatt Rahmenwerk

- Es gibt viele Rahmenwerke zur Cybersicherheit
- Die Rahmenwerke geben nur partiell (methodisch) vor wie sie umgesetzt werden sollen
- Sie beinhalten immer eine Art analytische, probabilistische Risikoidentifizierung. Dadurch werden die akzeptierbaren Auswirkungen immer im Kontext einer (nicht beurteilbaren) Wahrscheinlichkeit berücksichtigt, dies ist ein Wiederspruch zur Notwendigkeit die akzeptierbaren Auswirkungen zu kennen.
  - Wir können daraus auch schliessen: Wahrscheinlichkeiten helfen Versicherungsgesellschaften bei der Berechnung von Prämien, nicht aber Unternehmen bei der Ermittlung von akzeptierbaren Auswirkungen.

ISO 27001

IEC 62443
u.A. Part 3-2 / 4-1

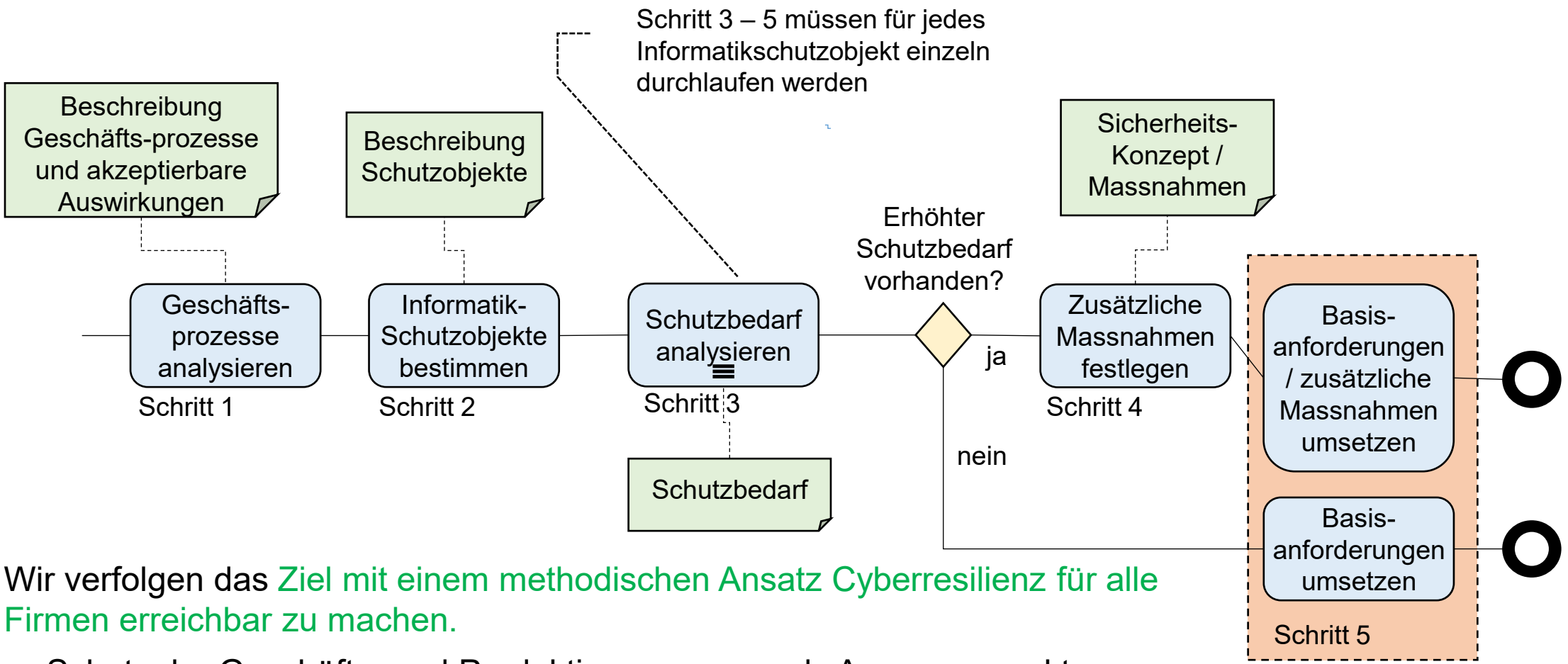

CYBERTRUST

Why Probabilities Cannot Be Used in Cyber Risk Management

Andreas Grünert, National Cyber Security Centre
James Bret Michael, Naval Postgraduate School
Rolf Oppliger and Ruedi Rytz, National Cyber Security Centre

This article proposes that measures of relevance be used instead probabilities for managing cyber risk.

Good Practice: Methode statt Rahmenwerk



Wir verfolgen das Ziel mit einem methodischen Ansatz Cyberresilienz für alle Firmen erreichbar zu machen.

- Schutz der Geschäfts- und Produktionsprozesse als Ausgangspunkt
- Verzicht auf wahrscheinlichkeitsbasierte Risikoanalysen
- Rund 20 Basisanforderungen die immer und verbindlich umzusetzen sind

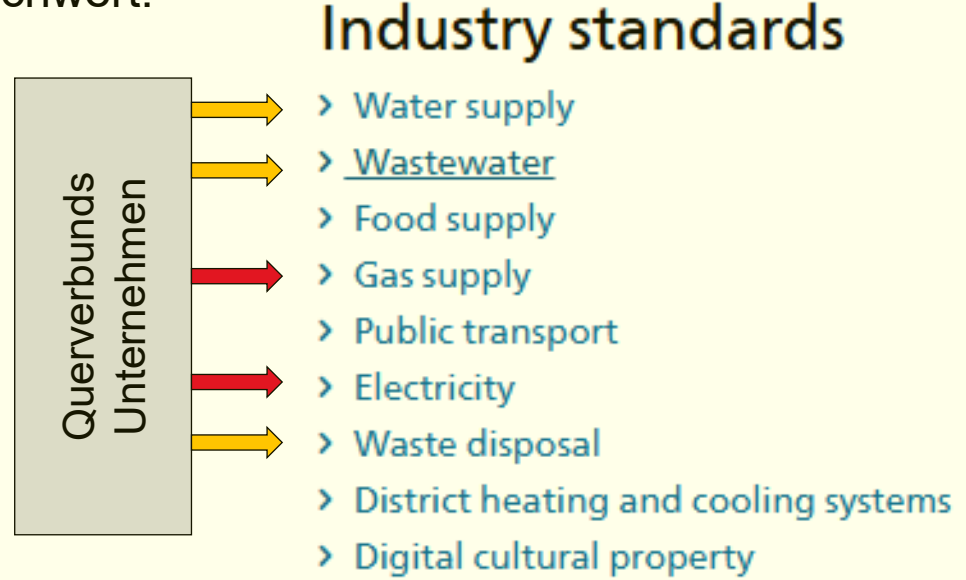
Management Ebene

Good Practice: Eine Methode für alle, Schwellenwerte pro Sektor / Branche

Eine Methode, aber auch,

- Branchenspezifische / Kontextspezifische Schwellenwerte (in Absprache mit den Aufsichtsbehörden oder Regulatoren).
- sektorspezifische empfohlene Massnahmen bei erhöhtem Schutzbedarf.

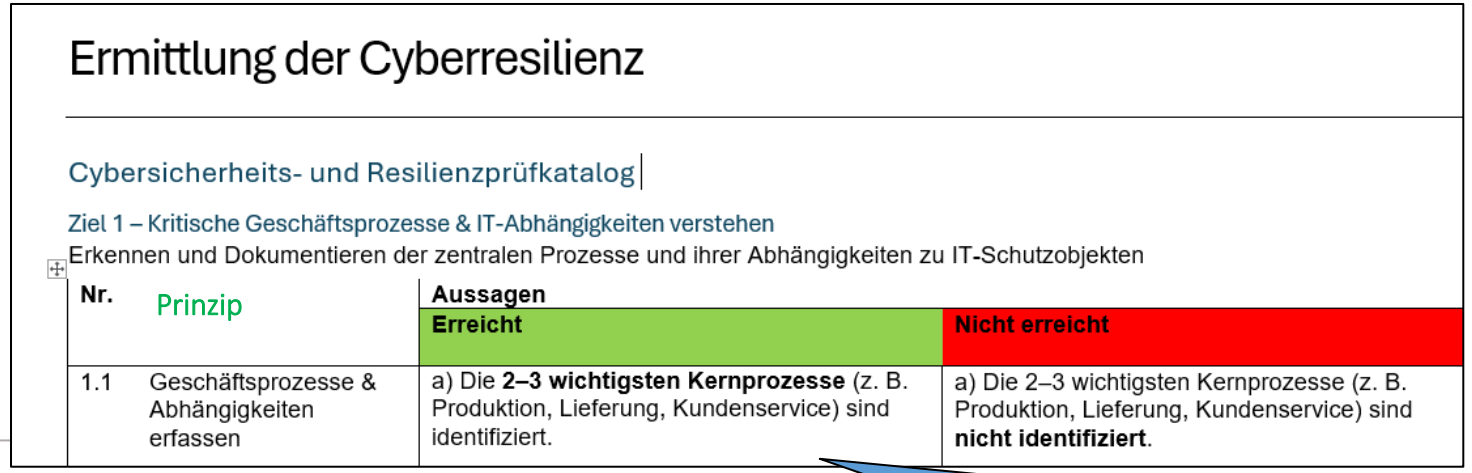
Heute gibt es in der Schweiz unterschiedliche Standards (und Methoden) für verschiedene Branchen, was eine einheitliche Umsetzung der Cybersicherheit erschwert.



Good Practice: Transparentes Cyberresilienz-Assessment

Das BACS entwickelt zurzeit auch eine Methode für das Assessment und Benchmarking.
Diese hat zum Ziel Resilienz prüfbar, vergleichbar und teilbar zu machen

- Hypothese: Resilienz ist erreicht wenn **6 Prüfzeile** und **20 Prinzipien** erreicht werden.
- Eine Organisation prüft und entscheidet anhand von Aussagen pro **Geschäftsprozess, Aufgabe oder Produktionsprozess**, ob diese Prinzipien erreicht oder nicht erreicht werden.
- Resilienz (für einen Prozess) ist also nur dann erreicht wenn **alle Prinzipien** erreicht werden.



Ermittlung der Cyberresilienz

Cybersicherheits- und Resilienzprüfkatalog

Ziel 1 – Kritische Geschäftsprozesse & IT-Abhängigkeiten verstehen

Erkennen und Dokumentieren der zentralen Prozesse und ihrer Abhängigkeiten zu IT-Schutzobjekten

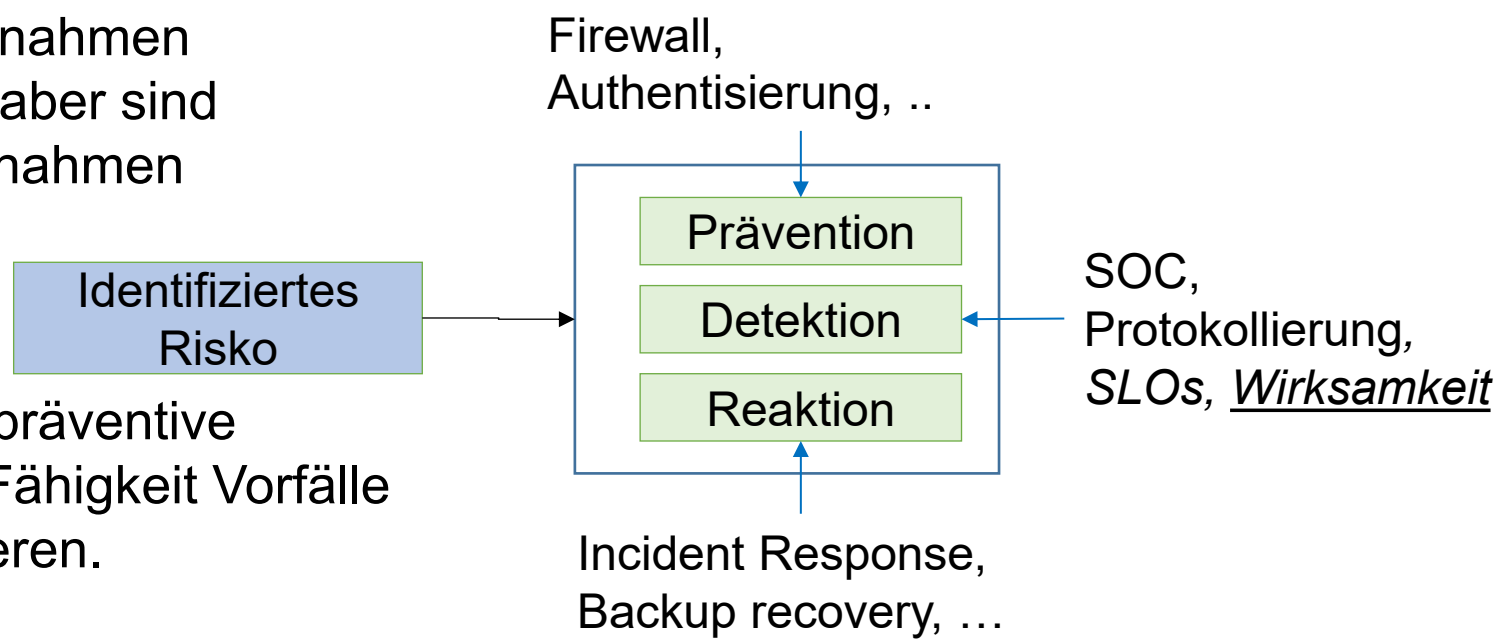
Nr.	Prinzip	Aussagen	
		Erreicht	Nicht erreicht
1.1	Geschäftsprozesse & Abhängigkeiten erfassen	a) Die **2–3 wichtigsten Kernprozesse** (z. B. Produktion, Lieferung, Kundenservice) sind identifiziert.	a) Die 2–3 wichtigsten Kernprozesse (z. B. Produktion, Lieferung, Kundenservice) sind **nicht identifiziert**.

Management Ebene

Good Practice: Protect, Detect, Respond für jedes Risiko

Diese Good Practice hat zum Ziel die Auswahl und Priorisierung von Präventiv, Erkennenden und Reagierenden Massnahmen zu verbessern.

- **PDR**: Für alle relevanten IT-Risiken sollen wenn möglich präventive Massnahmen ergriffen werden, in jedem Fall aber sind erkennende reagierende Massnahmen umzusetzen.

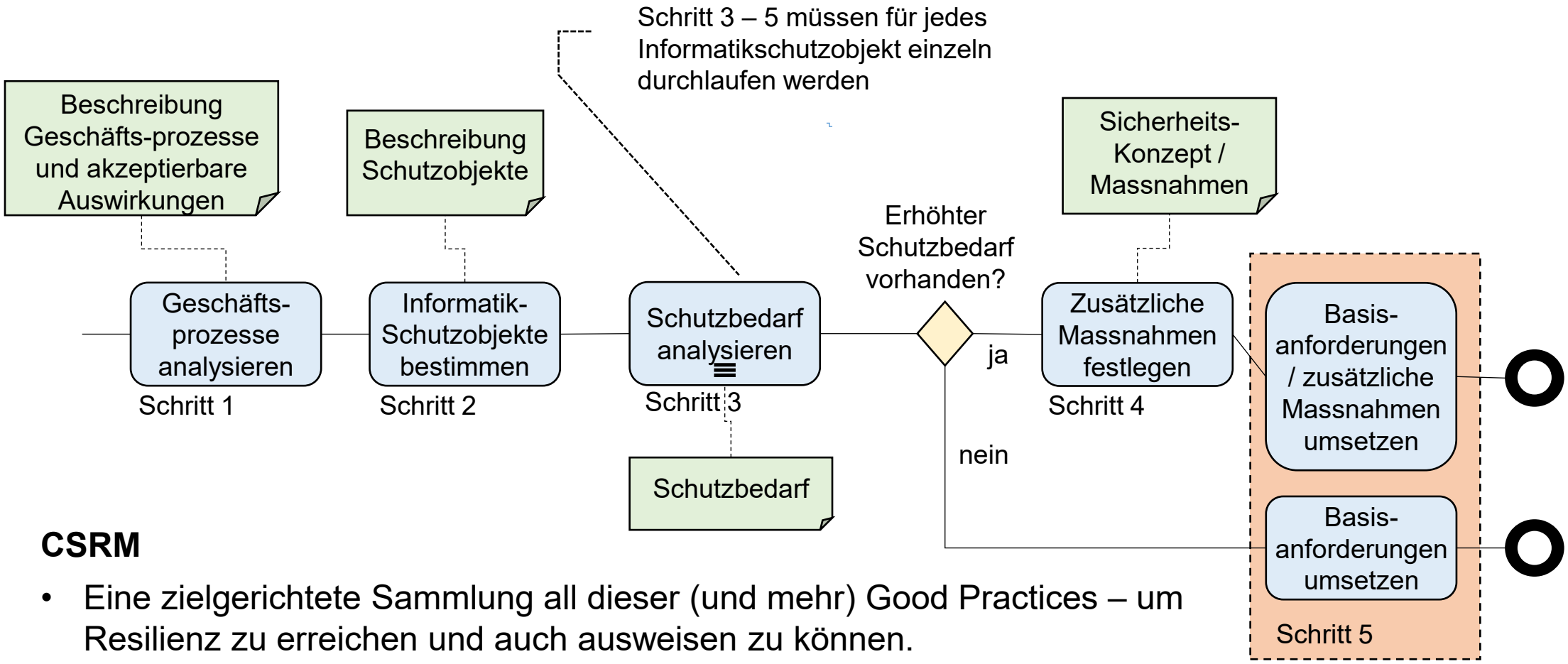


Die Good Practice verbindet das präventive Verhindern von Vorfällen mit der Fähigkeit Vorfälle zu Erkennen und darauf zu reagieren.

Weitere (alt) bekannte Good Practices

- Least Privilege
- Security by Default
- Netzwerk Segmentierung
- Nur Zugriff übers Internet ermöglichen, wenn ein öffentlicher Zugriff notwendig ist. (Reduzierung der Angriffsfläche)
- Überwachung mithilfe von ShadowServer (oder ähnlichem)
- Canaries zur automatisierten Benachrichtigung bei einer Kompromittierung
- Änderungen an den Sicherheitseinstellungen physischer Geräte muss eine interaktive Bestätigung (z. B. das Drücken einer Taste) erfordern
- ISMS Umsetzung mithilfe eines (online) Kalender der regelmässig durchzuführenden Aktivitäten beschreibt
- Von aussen nach innen: zuerst werden die Massnahmen umgesetzt, mit denen der Schutz im Hinblick auf Zugriffe und eine Kompromittierung von aussen erreicht wird, bevor die Massnahmen umgesetzt werden, die auf einen internen Schutz abzielen

BACS Cybersicherheit und -Resilienz Methode (CSRM)



CSRM

- Eine zielgerichtete Sammlung all dieser (und mehr) Good Practices – um Resilienz zu erreichen und auch ausweisen zu können.

Q&A

Diskussion