T.I.S.P.
TeleTrusT Information Security Professional

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

T.I.S.P. Community Meeting 2023

Berlin, 07. - 08.11.2023

Stand der Technik in der IT-Sicherheit

Tomasz Lawicki

Capgemini, Regional Head Cybersecurity, Security Architect Director
Bundesverband IT-Sicherheit e.V. (TeleTrusT), Leiter AK "Stand der Technik"

Der Arbeitskreis "Stand der Technik"

- seit **2015**
- über **40** Personen
- **1** Ziel

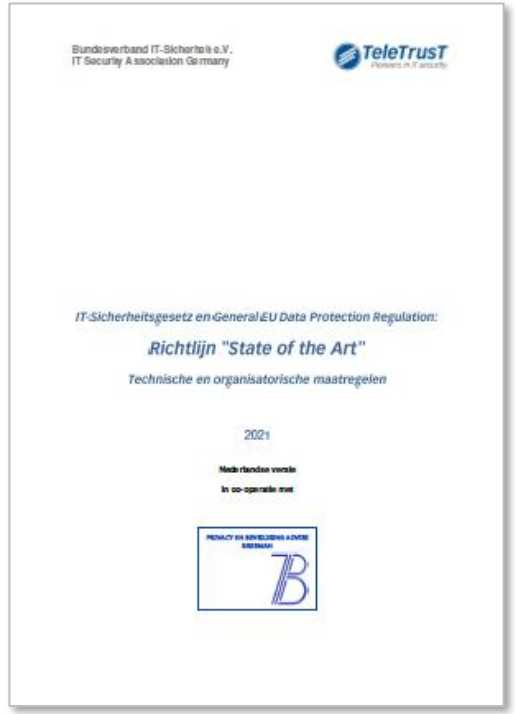
Der Arbeitskreis "Stand der Technik" wurde vom Bundesverband IT-Sicherheit e.V. (TeleTrusT) im Jahr 2015 initiiert, um den betroffenen Wirtschaftskreisen Handlungsempfehlungen und Orientierung zu geben.

Der Arbeitskreis vereint inzwischen über 40 IT-Sicherheitsexperten und IT-Sicherheitsexpertinnen, die gemeinsam technische und organisatorische Maßnahmen diskutieren, beschreiben und bewerten.

Seit 2016 frei verfügbar und international anerkannt

Bereits seit 2016 für deutsch-sprachigen Raum verfügbar.

Seit Anfang 2019 ist die Handreichung in Englisch und somit international verfügbar.



Seit Mitte 2019 wird parallel eine niederländische Version publiziert.

Handreichung zum "Stand der Technik" in der IT-Sicherheit ist frei zum Download verfügbar

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

https://www.teletrust.de/arbeitsgremien/recht/stand-der-technik/
oder
https://www.stand-der-technik-security.de

Was ist die Arbeitsgrundlage des Arbeitskreises "Stand der Technik"?

Die Pflicht "Stand der Technik" in der IT-Sicherheit einzuhalten oder zu berücksichtigen ist gesetzlich verankert.

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

ITSiG, nun ITSiG 2.0 (BSIG)
seit 2015

„§ 8a
Sicherheit in der
Informationstechnik Kritischer Infrastrukturen
(1) Betreiber Kritischer Infrastrukturen sind

"Betreiber kritischer Infrastru
verpflichtet [...] organisa
technische Vorkehrungen […]
Dabei soll der **Stand der Techn**
werden.[…]"

nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.
(2) Betreiber Kritischer Infrastrukturen

**ITSiG (erst TMG,
nun § 19 Abs. 4 TTDSG),** seit 2015

Artikel 4
Änderung des

a)
b) gegen Stö
äußer

DSGVO (GDPR)
seit 2018

Article 32
Security of processing
Taking into account the state of the art, the costs of implemen-
the nature, scope, context and purposes of processing as well
ving likelihood and severity for the rights and freedoms
the controller and the processor shall implement

sichtigung des **Stands der**
ffen der Verantwortliche und
rbeiter geeignete technische
rische Sicherheitsmaßnahmen,
dem Risiko angemessenes
utzniveau zu gewährleisten; […]"

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

**Anpassung des
IT-Sicherheitsgesetzes 2.0
gem. NIS-2-Richtlinie**

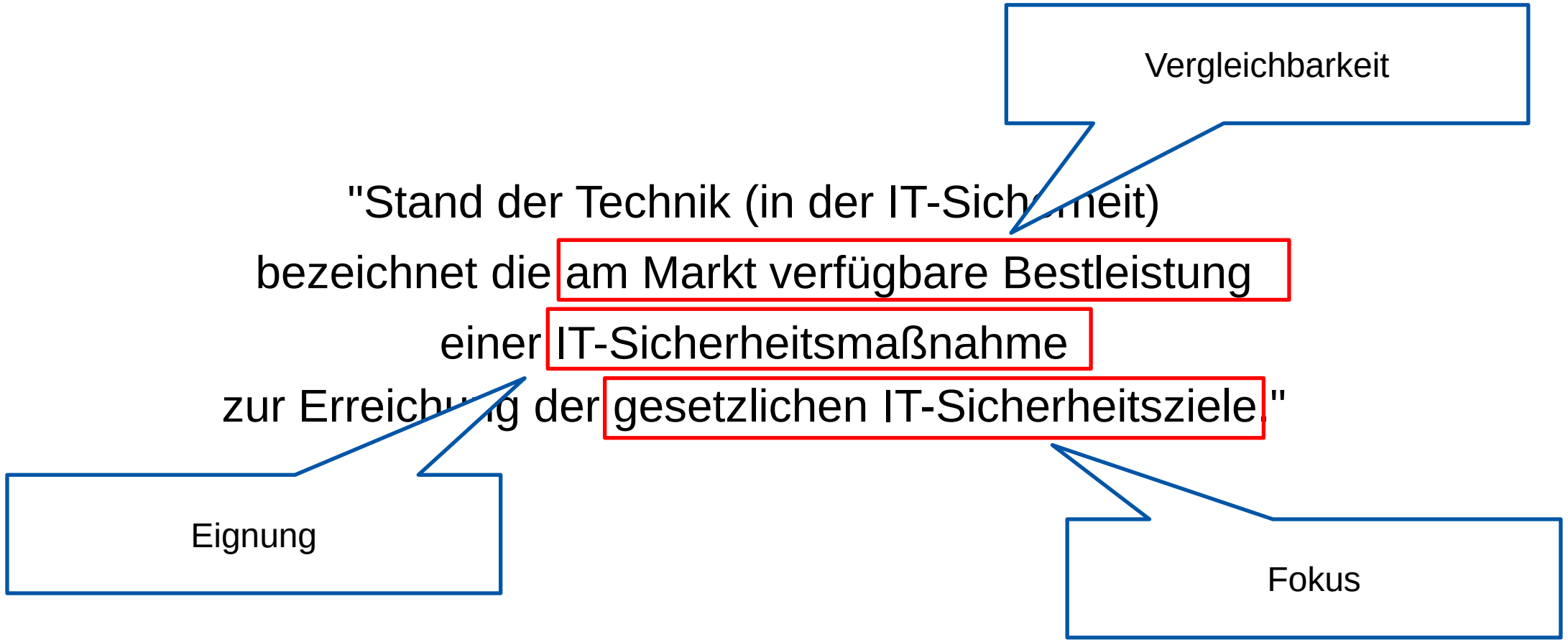
Was ist Stand der Technik in der IT-Sicherheit?

Definition aus der Handreichung

"Stand der Technik (in der IT-Sicherheit)
bezeichnet die am Markt verfügbare Bestleistung
einer IT-Sicherheitsmaßnahme
zur Erreichung der gesetzlichen IT-Sicherheitsziele."

Quelle: https://www.teletrust.de/, Handreichung "Stand der Technik in der IT-Sicherheit"

Definition aus der Handreichung



Quelle: https://www.teletrust.de/, Handreichung "Stand der Technik in der IT-Sicherheit"

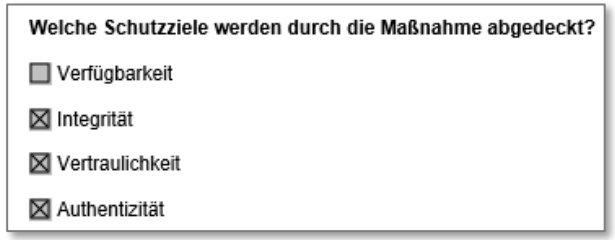
Beispiel: Integrität

Bezug	Gesetzestext	Fokus
§ 8a Abs. 1 BSIG	"Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, **Integrität**, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind."	Integrität

IT-Sicherheitsmaßnahmen
(Beispiele – Liste nicht abschließend)

- Schwachstellen- und Patchmanagement von Systemen und Anwendungen
- Dokumentation von Änderungen an Systemen
- Detektion von unberechtigten Zugriffen
- Einsatz von Maßnahmen zur Erkennung von Schadsoftware
- Schulungen zur Sensibilisierung der Mitarbeiter
- etc.

Empfehlungen in der TeleTrusT Handreichung "Stand der Technik in der IT-Sicherheit"



Wie kann der Stand der Technik in der IT-Sicherheit bestimmt werden?

Die Kalkar-Entscheidung als Grundlage

* Oft auch als "Stand der Wissenschaft und Technik" bezeichnet

Quelle: BVerfG, Beschluss vom 8. August 1978 – 2 BvL 8/77

Einordnung der Technologiestände

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

2.1 Fragen zum Grad der Anerkennung

Bewertung vom Ak SdT auszufüllen.

1) Welche Dokumentation über die Maßnahme steht öffentlich zur Verfügung?
bitte beantworten Sie die Frage, indem Sie die u.a. Kästchen ankreuzen

☐ wiss. Publikation	☐ Fachmedien	☐ Massenmedien	*1*	*3*	*5*

[bitte begründen Sie Ihre Antwort hier]

2) Nimmt die Maßnahme Bezug auf internationale oder nationale Normen?
bitte beantworten Sie die Frage, indem Sie die u.a. Kästchen ankreuzen

☐ nein, noch nicht normiert	☐ ja, eine	☐ ja, mehr als eine	*1*	*3*	*5*

[bitte begründen Sie Ihre Antwort hier]

***3)* Wurde die Maßnahme von anerkannten Gremien / Verbänden empfohlen?**
bitte beantworten Sie die Frage, indem Sie die u.a. Kästchen ankreuzen

☐ nein	☐ ja, führenden	☐ ja, vielen	*1*	*3*	*5*

[bitte begründen Sie Ihre Antwort hier]

***4)* Wird die konzeptionelle Eignung der Maßnahme regelmäßig überprüft?**
bitte beantworten Sie die Frage, indem Sie die u.a. Kästchen ankreuzen

☐ nein	☐ ja, herstellerseitig	☐ ja, unabhängige Instanz	1	3	5

[bitte begründen Sie Ihre Antwort hier]

Durchschnitt

2.2 Fragen zur Bewährung in der Praxis

Bewertung vom Ak SdT auszufüllen.

1) Wie ist der Innovationsgrad der Maßnahme einzustufen?
bitte beantworten Sie die Frage, indem Sie die u.a. Kästchen ankreuzen

☐ hoch	☐ mittel	☐ gering	*1*	*3*	*5*

[bitte begründen Sie Ihre Antwort hier]

2) Wo wurde die aktuelle Version der Maßnahme erprobt?
bitte beantworten Sie die Frage, indem Sie die u.a. Kästchen ankreuzen

☐ Laborbedingungen	☐ professioneller Einsatz	☐ Massenmarkt	1	3	5

[bitte begründen Sie Ihre Antwort hier]

3) Existieren vergleichbare Maßnahmen am Markt?
bitte beantworten Sie die Frage, indem Sie die u.a. Kästchen ankreuzen

☐ nein	☐ wenige	☐ viele	1	3	5

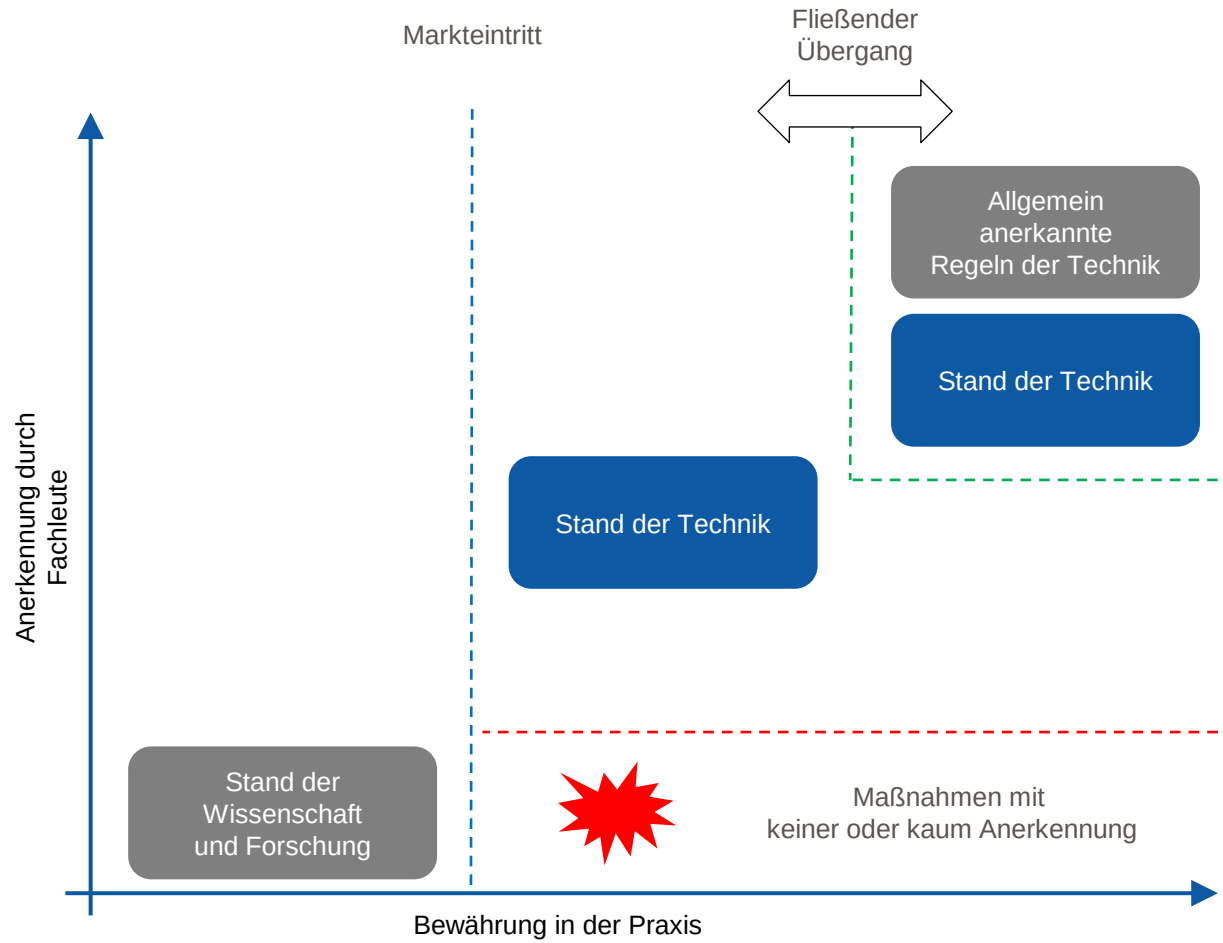
[bitte begründen Sie Ihre Antwort hier]

4) Wie oft wird die Maßnahme herstellerseitig konzeptionell aktualisiert?
bitte beantworten Sie die Frage, indem Sie die u.a. Kästchen ankreuzen

☐ häufiger als 1/Jahr	☐ jährlich	☐ seltener	1	3	5

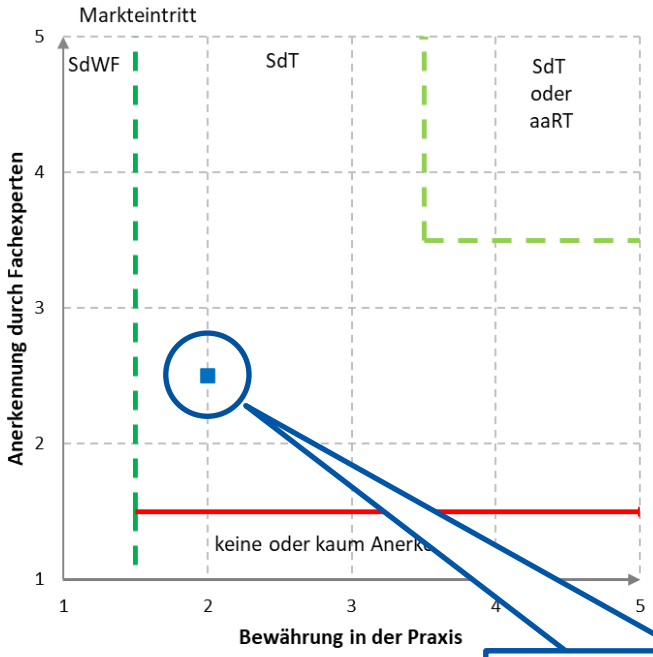
[bitte begründen Sie Ihre Antwort hier]

Durchschnitt

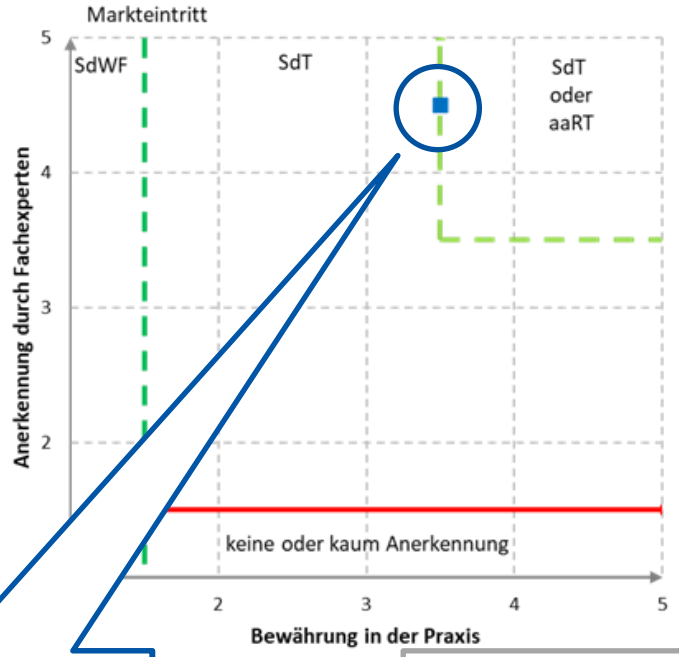


Beispiel: Einordnung von Maßnahmen

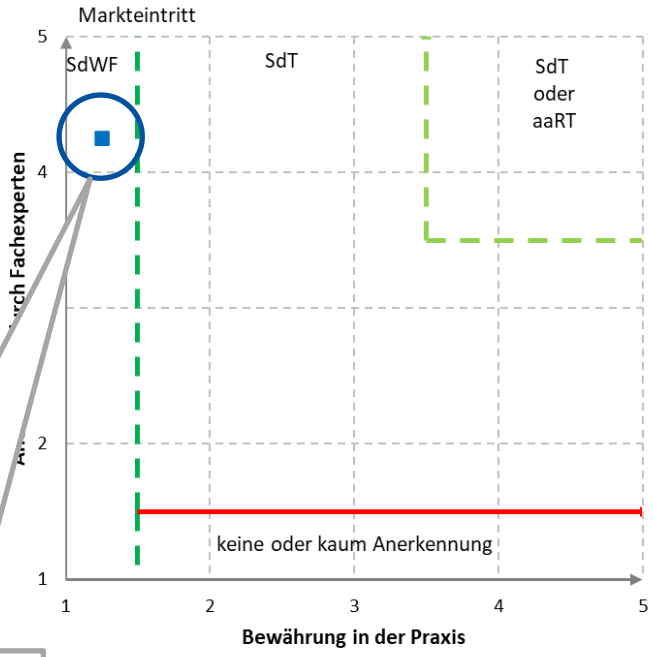
Endpoint Detection & Response Plattform



Multi-Faktor-Authentifizierung



Post-Quanten-Kryptographie (konstruiert)



SdT

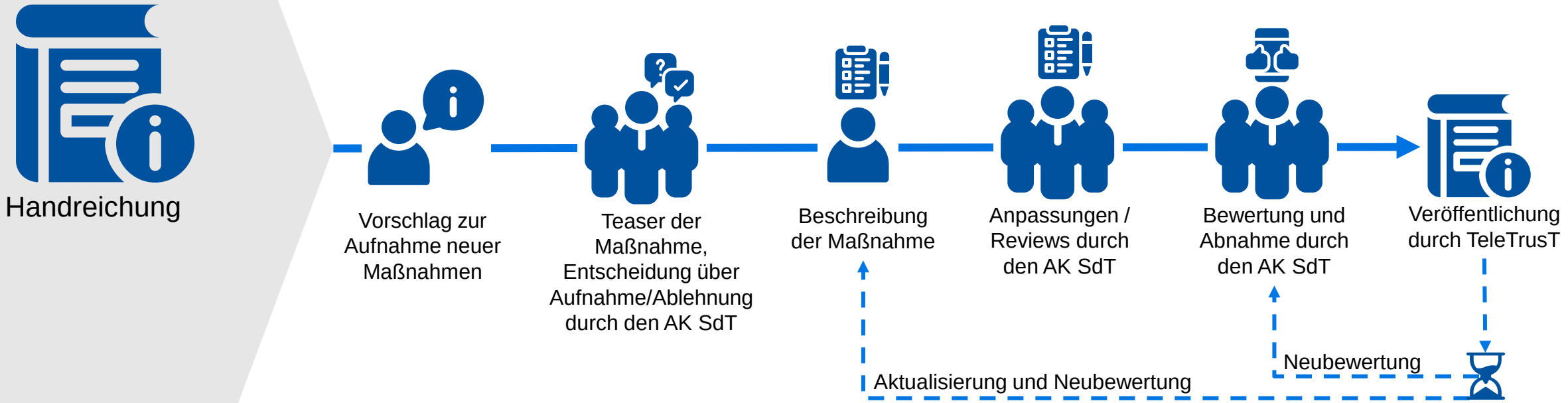
(noch) kein SdT

SdWF = Stand der Wissenschaft und Forschung

SdT = Stand der Technik

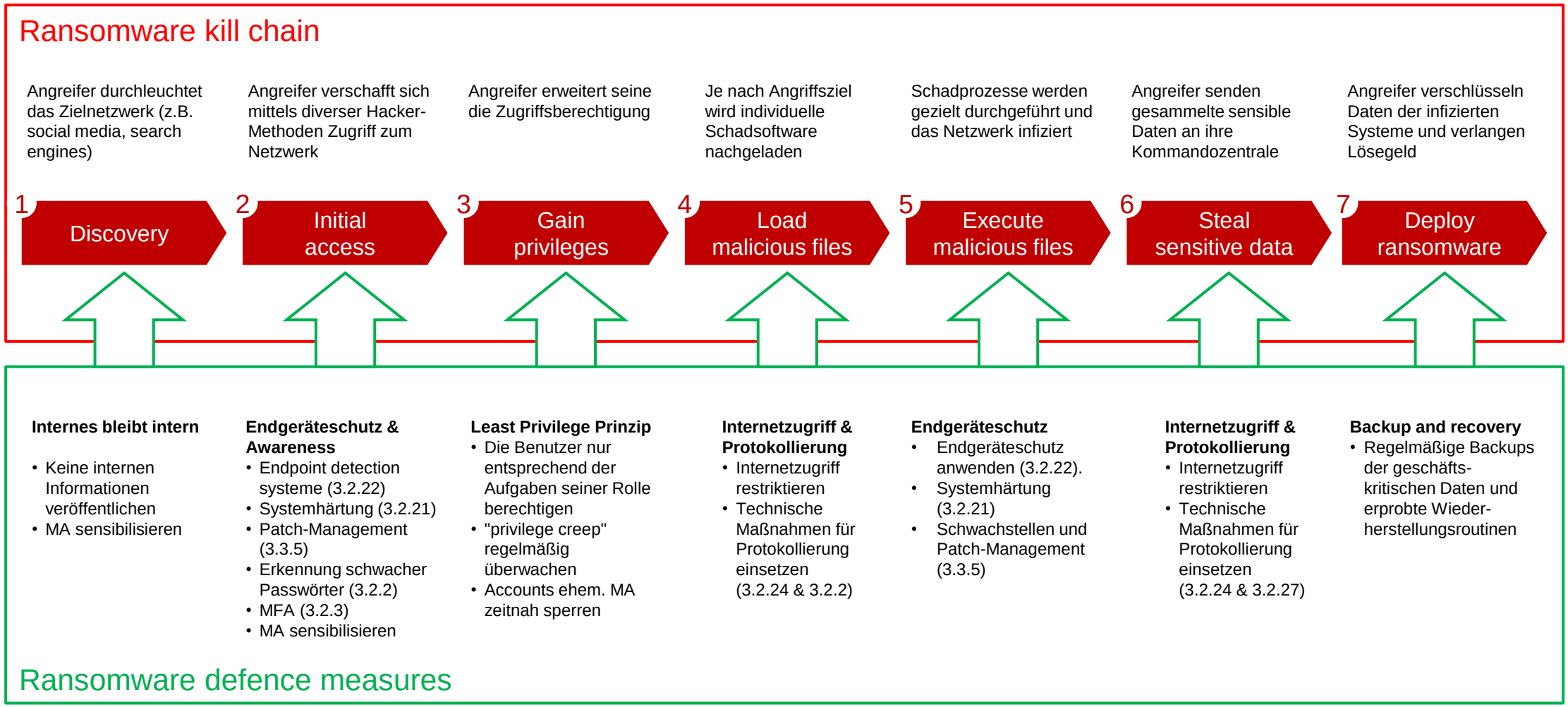
aaRT = allgemein anerkannten Regeln der Technik

Die Einordnung der Sicherheitsmaßnahmen folgt einem festgelegten Prozess.



Wie kann die Handreichung unterstützen?

Beispiel: Maßnahmen gegen Ransomware-Angriffe



Wie stelle ich sicher, dass meine Sicherheitsmaßnahmen dem Stand der Technik entsprechen?

3 Tipps zum Stand der Technik in der IT-Sicherheit

- Systeme und Anwendungen auf dem aktuellen Software-Stand halten
- Regelmäßig eigene Sicherheitsmaßnahmen gegen aktuelle Angriffsvektoren überprüfen und bei Bedarf anpassen dabei technische Entwicklung am Markt beobachten und Empfehlungen berücksichtigen
- Eigene Sicherheitsmaßnahmen und ihren Zustand dokumentieren

Q & A