UNINET it-consulting GmbH

SecurITy made in EU
Trust Seal
www.teletrust.de/itsmie

TeleTrusT Handreichung

Stand der Technik zur Umsetzung zukunftsfähiger Sicherheitskonzepte

www.uninet.at | info@uninet.at | Büro: Business Campus One, Softwarepark 32/1, 4232 Hagenberg

CYBER TRUST AUSTRIA

PARTNER BBG BUNDESBESCHAFFUNG

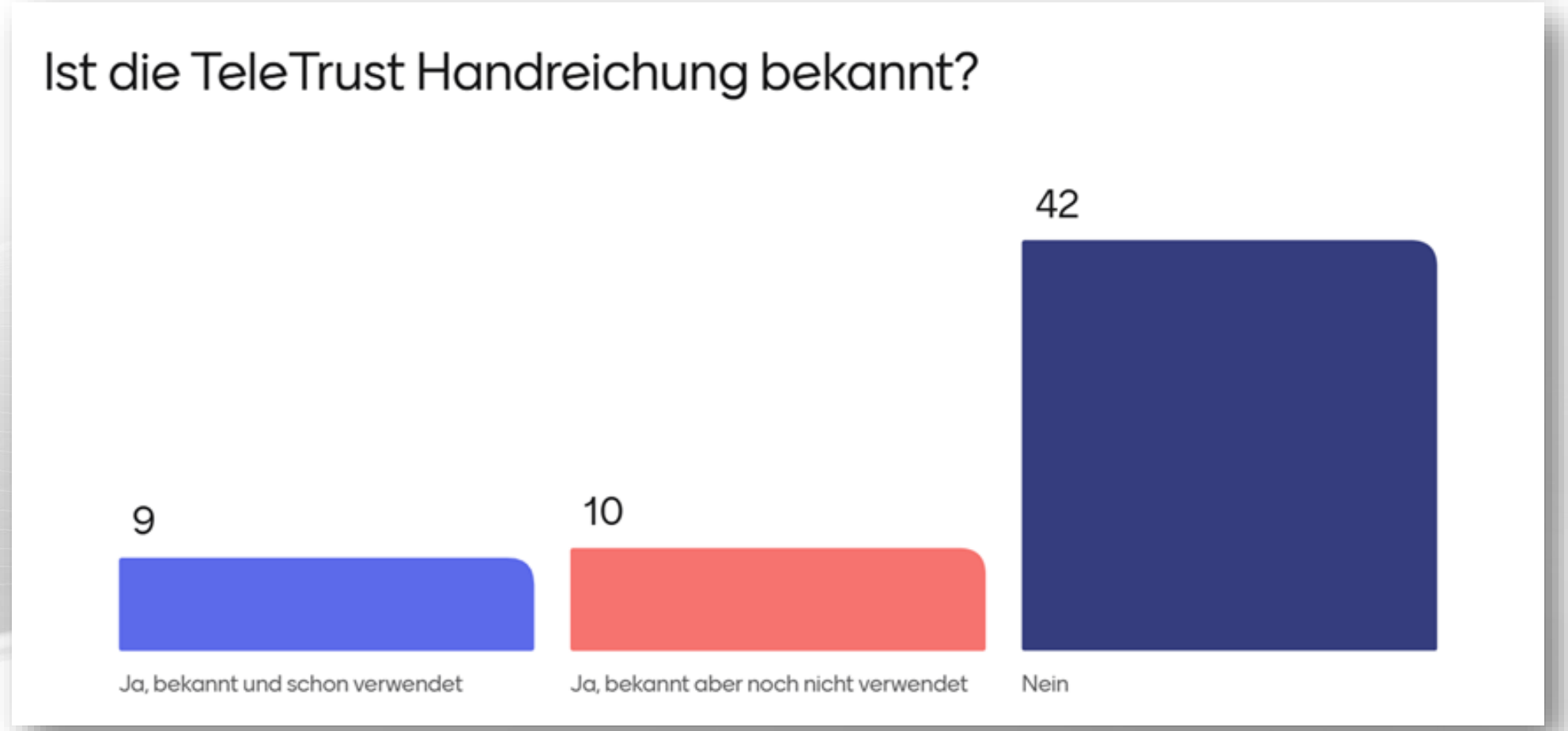
TeleTrusT, Bundesverband IT-Sicherheit e.V.

- Größter europäischer Kompetenzverbund für IT-Sicherheit
- Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandten Partnerorganisationen
- Laufende Publikation von Handreichungen, technische Empfehlungen und Stellungnahmen zum Themenbereich IT-Sicherheit/Security

Handreichung „Stand der Technik“

- Gründung auf Forderung des IT-Sicherheitsgesetzes (D), den „Stand der Technik“ in Unternehmen zu berücksichtigen
  - Auch DSGVO fordert „Stand der Technik“
- Seit 2016 in Deutsch, seit 2019 auch in Niederländisch und Englisch verfügbar
  - Seit 2019 Veröffentlichung in Kooperation mit ENISA
- Frei zum Download verfügbar

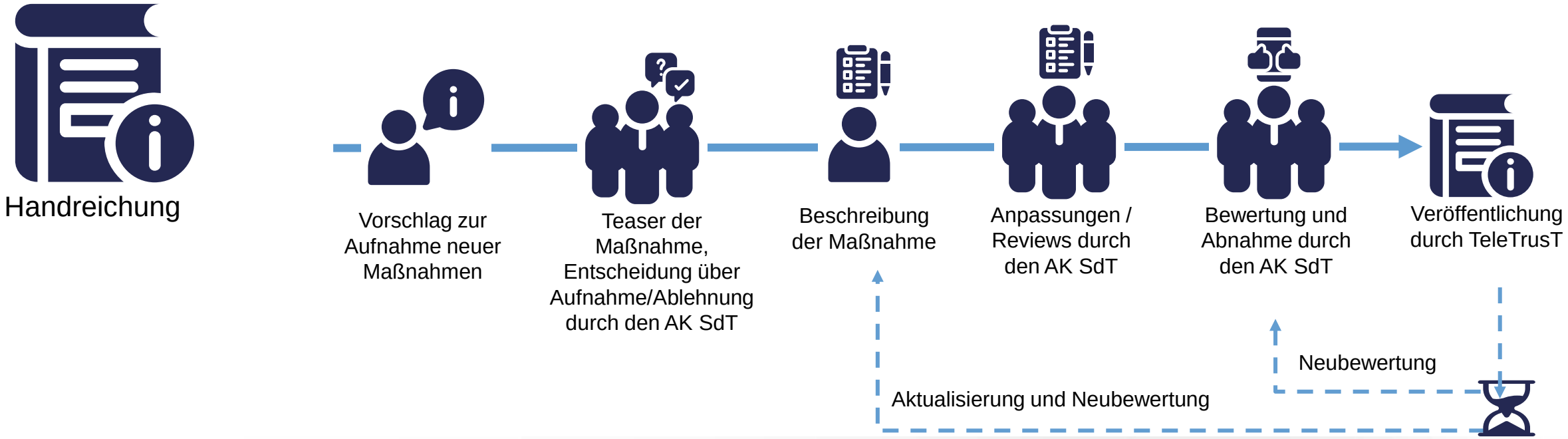
Umfrage



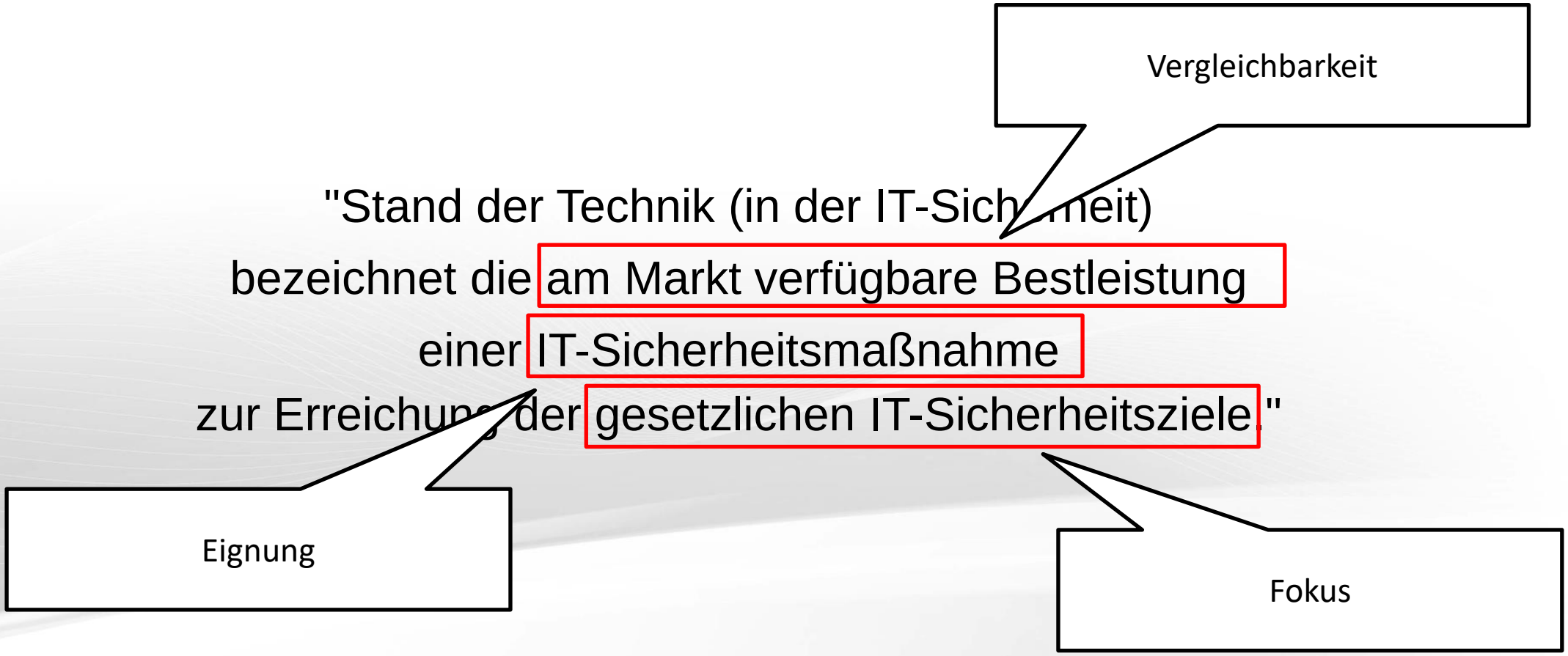
Entwicklungsprozess der Handreichung

- Arbeitskreis „Stand der Technik“
  - Gründung 2015
  - Über 40 Personen in Deutschland und Österreich (Regionalstelle Hagenberg)

Prozess Entwicklung der Handreichung und Qualitätssicherung



Was ist der Stand der Technik?



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

Wie kann der Stand der Technik bestimmt werden?

- Drei-Stufen-Theorie nach Kalkar-Entscheidung als Grundlage

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

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

Wie kann der Stand der Technik bestimmt werden?

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

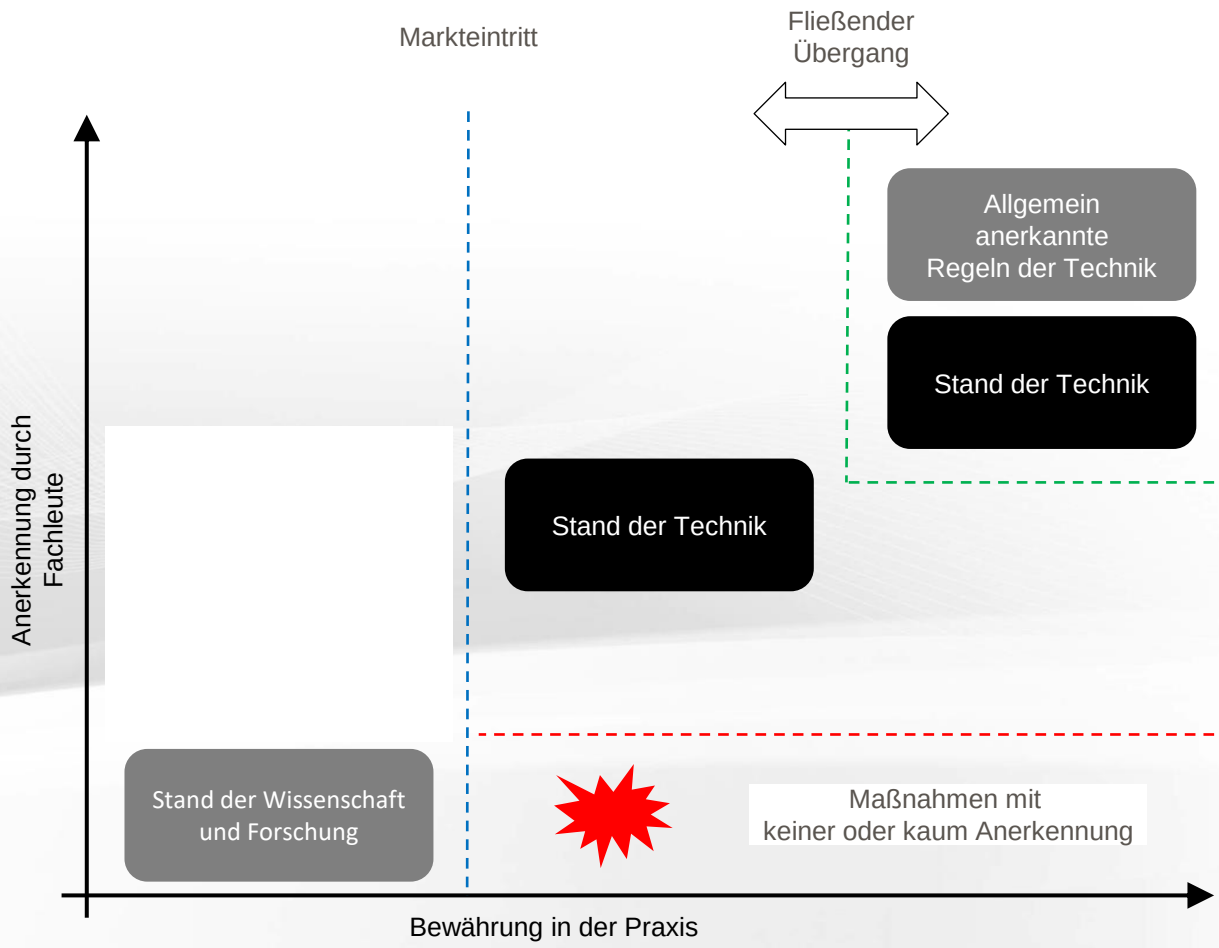
[bitte begründen Sie Ihre Antwort hier]

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

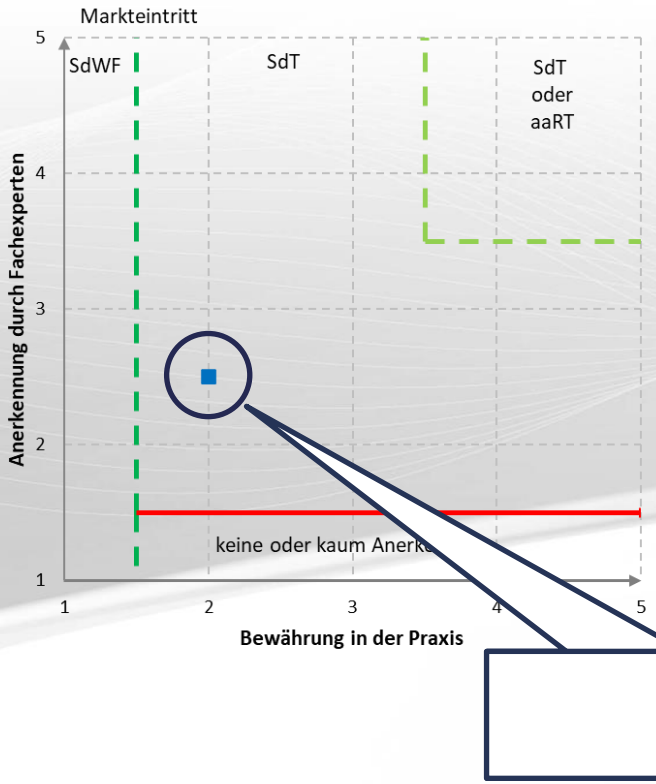
[bitte begründen Sie Ihre Antwort hier]

Durchschnitt

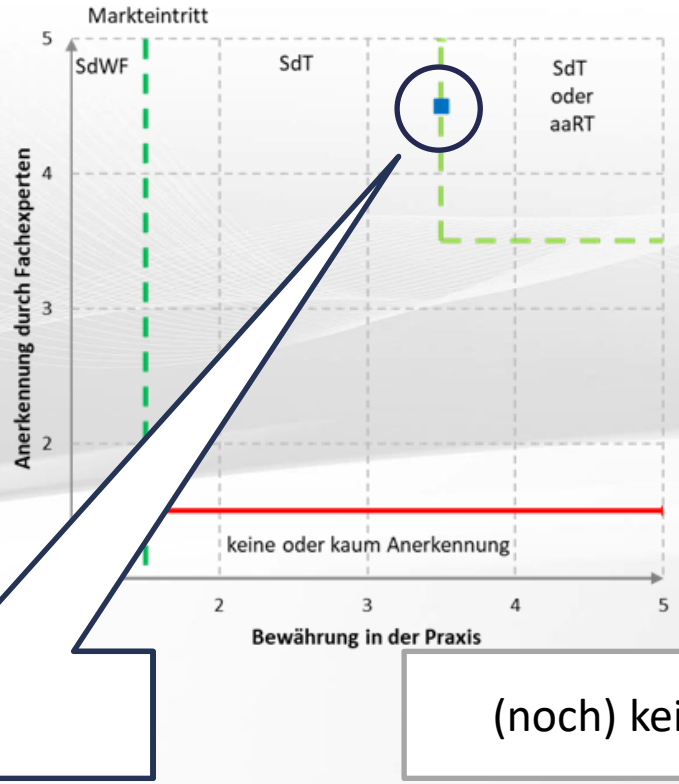


Wie kann der Stand der Technik bestimmt werden?

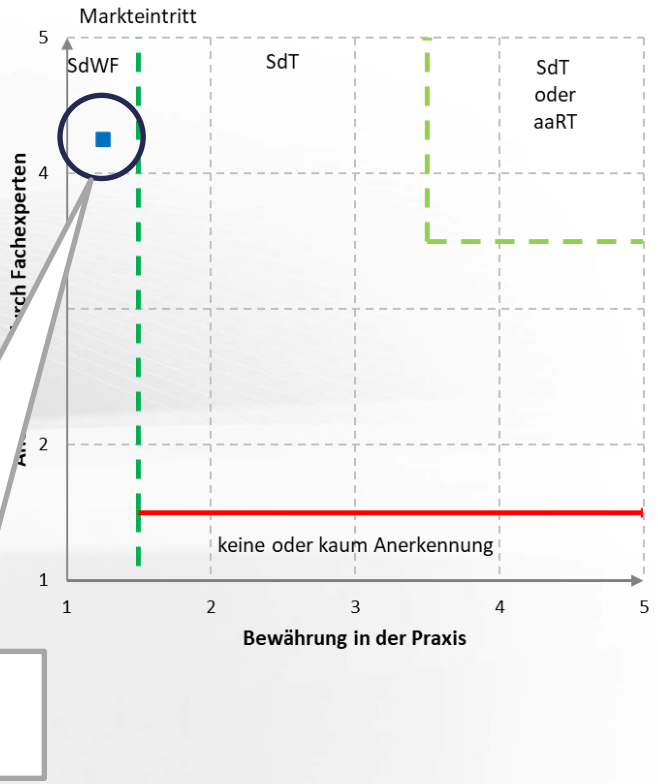
Endpoint Detection & Response Plattform



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

Inhalte Handreichung

- Vielzahl an technischen und organisatorischen Maßnahmen (TOMs)

Technische Maßnahmen

- Authentifizierungsmethoden und –Verfahren
- Bewertung und Durchsetzung starker Passwörter
- Multifaktor-Authentifizierung
- Kryptographische Verfahren
- Verschlüsselung von Festplatten
- Verschlüsselung von Dateien und Ordnern
- Verschlüsselung von E-Mails
- Sicherung des elektronischen Datenverkehrs mit PKI
- Einsatz von VPN (Layer 3)
- Verschlüsselung auf Layer 2
- Cloudbasierter Datenaustausch
- Datenablage in der Cloud
- Nutzung von mobilen Sprach- und Datendiensten
- Kommunikation mittels Instant Messenger
- Management mobiler Geräte
- Routersicherheit
- Netzwerküberwachung mittels Intrusion Detection System
- Schutz des Web-Datenverkehrs
- Schutz von Webanwendungen
- Fernzugriff auf Netzwerke / Fernwartung
- Serverhärtung
- Endpoint Detection & Response Plattform
- Internetnutzung mit Web-Isolation
- Angriffserkennung und Auswertung (SIEM)
- Vertrauliche Datenverarbeitung
- Sandboxing zur Schadcode-Analyse
- Cyber Threat Intelligence
- Absicherung administrativer IT-Systeme
- Überwachung von Verzeichnisdiensten und identitätsbasierte Segmentierung
- Netzwerksegmentierung und Separierung

Organisatorische Maßnahmen

- Standards und Normen
- Prozesse
- Sichere Softwareentwicklung
- Schwachstellen- und Patchmanagement
- Management von Informationssicherheitsrisiken
- Personenzertifizierung
- Umgang mit Dienstleistern
- Informationssicherheitsmanagementsystem (ISMS)
- Absicherung privilegierter Accounts
- Dark Web Monitoring
- Software Bill of Materials (SBOM)

Umsetzung mithilfe der Handreichung

Beispiel: Netzwerksegmentierung und Separierung

- Unterteilung eines Netzwerks in mehrere Segmente
- Kommunikation erfolgt eingeschränkt über Zonengrenzen (Boundary Protections) mit einer Prüfung/Überwachung des Netzwerkverkehrs
- Einschränkung vieler Risiken (z.B. Bedrohungen durch Schadsoftware)

- **Verbundene Bedrohung(-en)**
  - Laterale Bewegung von Angreifern im Netzwerk (Network Lateral Movement)
  - Ungehinderte Verbreitung von Schadsoftware in Netzwerken
  - Bedrohungen durch Insider
  - Unzulässiger oder böswilliger Datenverkehr wird nicht identifiziert
  - Ausnutzung von Zugangsmöglichkeiten zu vernetzten Systemen
  - Verlust der Verfügbarkeit, Integrität und Vertraulichkeit einer großen Anzahl an Systemen, wenn diese in einem flachen Netzwerk betrieben werden
  - …

Umsetzung mithilfe der Handreichung

Beispiel: Netzwerksegmentierung und Separierung

- **Beschreibung der Maßnahme**
  - Vorgehensweise zur Trennung von Netzwerken (logisch oder physisch, auf Basis des Schutzbedarfs etc.)
  - Datenverkehr zwischen Netzwerkzonen (Firewalls/IPS/ACT, Whitelisting etc.)
  - Prinzip Defense-in-Depth
  - Schutz- und Härtungsmaßnahmen pro Zone
  - Verhinderung von Split-Tunneling
  - Administrative Systeme in dedizierten Netzwerken
  - …

- **Schutzziele**

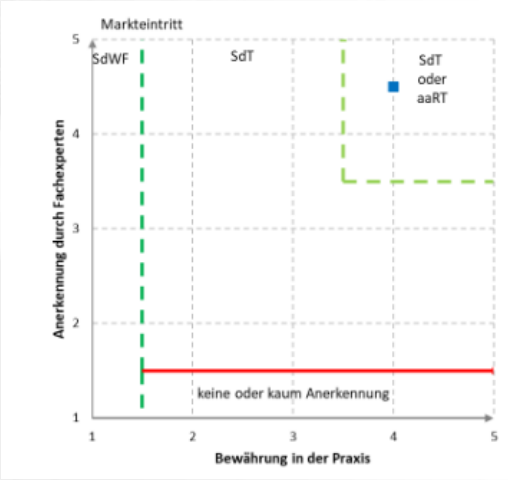
  ☒ Verfügbarkeit

  ☒ Integrität

  ☒ Vertraulichkeit

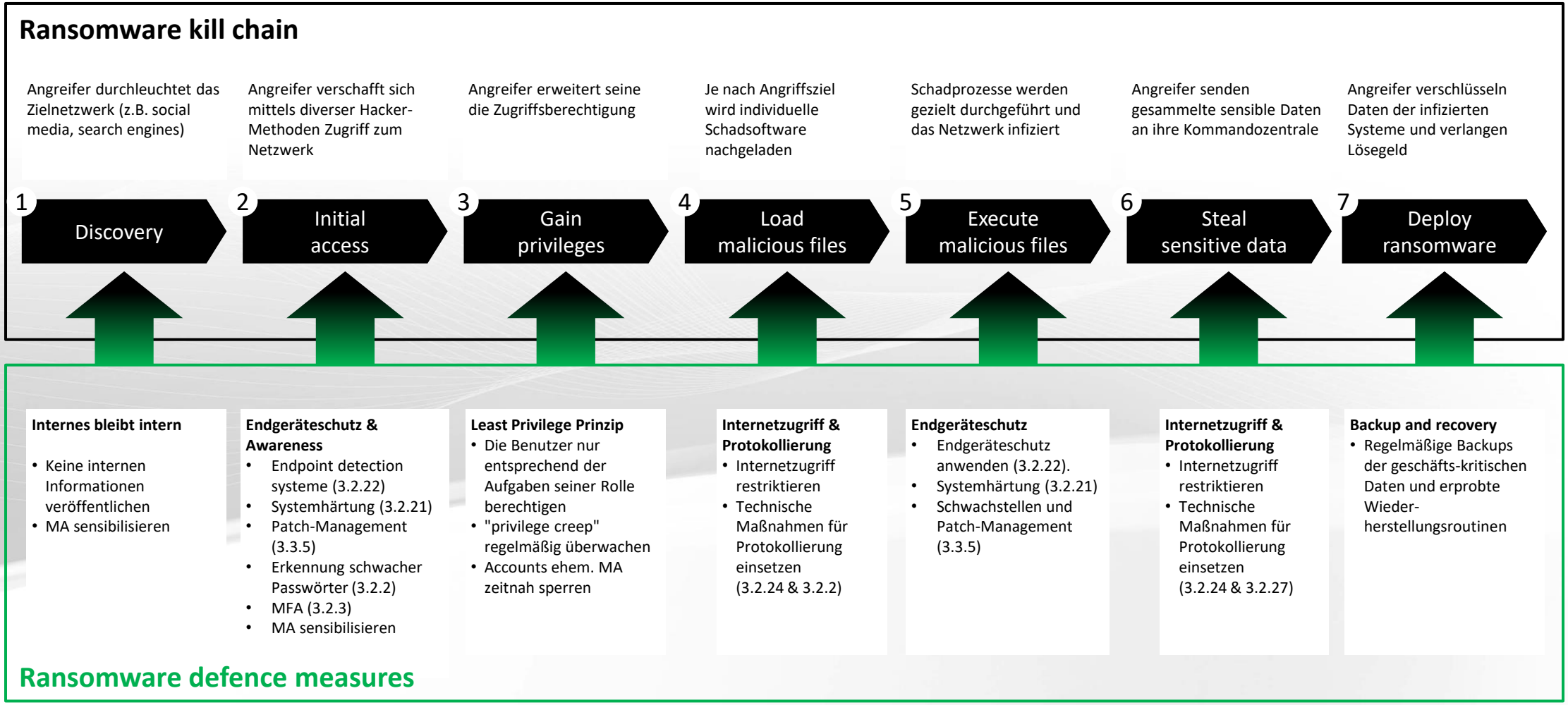
  ☐ Authentizität

- **Empfohlene Standards zur Umsetzung der Maßnahme**
  - BSI IT-Grundschutz-Kompendium, NET.1.1 „Netzwerkarchitektur und Design“
  - ISO/IEC 27002:2022, Controls 8.20, 8.21. 8.22
  - IEC 62443-3-3:2013



Mehr Einblick: **Workshop „Anwendbarkeit der TeleTrusT Handreichung zum „Stand der Technik“ in der Praxis**

Beispiel: Maßnahmen gegen Ransomware



Roadmap und zukünftige Entwicklungen

- Keine dedizierte Roadmap
  - Idee: Handreichung laufend aktualisieren, um Aktualität zu gewährleisten

- Neue Version der Handreichung im Sommer 2025
  - Vielzahl neuer Themen, u.a.
    - » IT-Asset-Management
    - » Incident Management
    - » Geschäftskontinuitätsmanagement (BCM)
    - » Notfall- und Krisenmanagement
  - Zusätzliche Exkursthemen
    - » Mapping zu ISO/IEC 27001:2022
    - » Auswirkung von KI auf Informationssicherheit
    - » Absicherung der Lieferkette

KONTAKT

UNINET it-consulting GmbH

www.uninet.at, info@uninet.at

Büro:

Business Campus ONE

Softwarepark 32/1

4232 Hagenberg, Österreich

Firmenrechtlicher Sitz

Fichtenstraße 20, 4020 Linz, Österreich

FN 299242m LG Linz, ATU63752406

BBG Lieferant für IT-Consulting und IT-Sachverständige

Vertragsnummer: 3602.04434