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

IT-Sicherheitsrechtstag 2026

Berlin, 24.09.2026

Stand der Technik: zwei Ansätze von TeleTrusT und BSI

Tomasz Lawicki, Capgemini

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

Viele Regelungen fordern ein hohes Sicherheitsniveau.

Die Herausforderung liegt in der Übersetzung abstrakter Anforderungen in konkrete, prüffähige Maßnahmen.

Regulatorische Vorgaben

- NIS2
- DORA
- DSGVO
- CRA
- AI Act
- BSIG
- TDDDG
- BSI-KritisV
- . . .

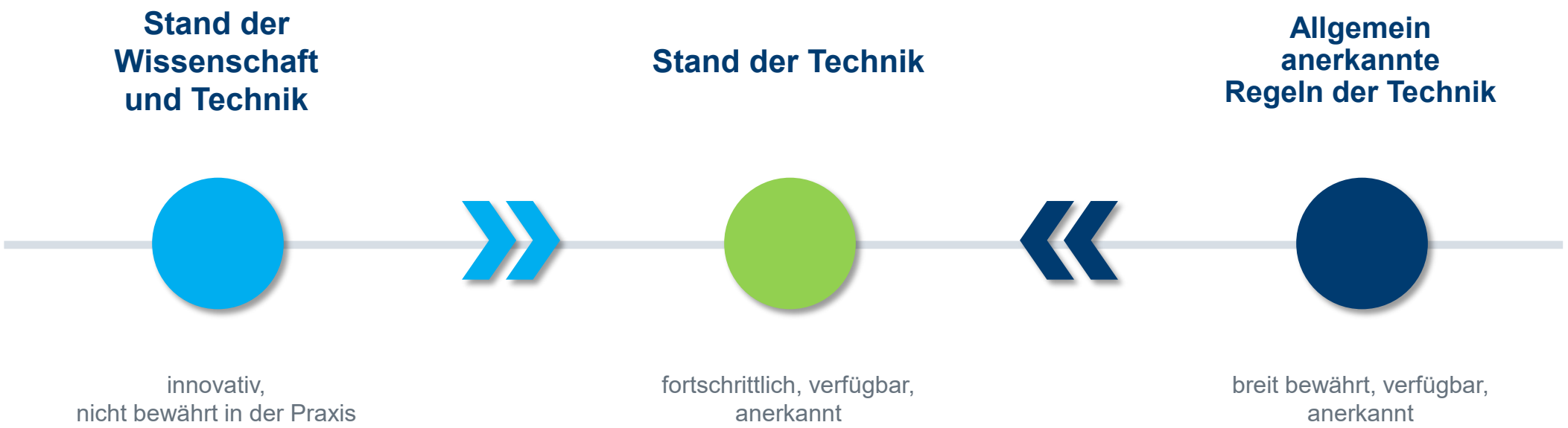
Die Unternehmen müssen Rechtsanforderungen umsetzen und dafür Nachweise liefern

Was muss konkret umgesetzt werden?

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

Stand der Technik ist ein bewegliches Ziel

Er liegt zwischen forschungsnaher Innovation und breit bewährter Standardisierung.



Technische Entwicklung • Marktbewährung • Verfügbarkeit • Anerkennung • Bedrohungslage

Der technische Fortschritt verschiebt das Schutzniveau … MFA ungleich MFA

Nicht die Anzahl der Faktoren ist entscheidend, sondern insbesondere Phishing-Resistenz, kryptografische Bindung und sichere Wiederherstellung.

Begrenztes Schutzniveau → **Fortschrittliches Schutzniveau**

01 NIEDRIG	02 NIEDRIG	03 MITTEL	04 MITTEL	05 MITTEL–HOCH	06 SEHR HOCH	07 SEHR HOCH	08 SEHR HOCH
SMS-OTP	**E-Mail-OTP**	**TOTP**	**Push-MFA**	**Number Matching**	**FIDO2 / Passkey**	**Hardware Security Key**	**Smartcard / PIV / PKI**
Code per SMS	Code per E-Mail	Authenticator-Code	Approve / Deny	Push + Nummer + Kontext	WebAuthn-basiert	FIDO2-Key + PIN/Biometrie	Zertifikat + PIN
Schwachstelle / Einordnung	**Schwachstelle / Einordnung**	**Schwachstelle / Einordnung**	**Schwachstelle / Einordnung**	**Schwachstelle / Einordnung**	**Schwachstelle / Einordnung**	**Schwachstelle / Einordnung**	**Schwachstelle / Einordnung**
SIM-Swap, SS7, Phishing	Mailkonto als Abhängigkeit	AitM / Echtzeit-Phishing	Push Fatigue, Social Engineering	Stärker, aber nicht vollständig phishing-resistent	Phishing-resistent, dienstgebunden	Phishing-resistent, physischer Besitz	High Assurance, hoher Lifecycle-Aufwand

Gleiches Sicherheitsziel, unterschiedliche Maßnahmen aufgrund unterschiedlicher Risikokontexte

Der Stand der Technik ordnet das Technologieniveau ein. Die konkrete Auswahl bleibt eine eigenständige Angemessenheitsentscheidung.

Mittelständische Produktion

Kontext	intern, verwaltete Admin-Geräte, segmentierter Zugriff
Sicherheitsziel	Administrativen Zugriff absichern
Entscheidung	MFA (TOTP)
Begründung	Begrenzte Exposition, verwaltete Admin-Geräte, Phishing-Risiko wird bewertet und dokumentiert

KRITIS-Betrieb

Kontext	externer, privilegierter Zugriff, hoher Schutzbedarf
Sicherheitsziel	Privilegierten Fernzugriff absichern
Entscheidung	MFA (FIDO2) + PAM
Begründung	Phishing-Resistenz reduziert Credential-Angriffe; PAM begrenzt Privilegien und kontrolliert Sitzungen

Beispielhafte Einordnung, keine pauschale Maßnahmenvorgabe.

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

Die entscheidende Frage lautet nicht: Was ist Stand der Technik?

Die Managementfrage ist kontextbezogen und zeitpunktabhängig.

Warum wurde genau diese Maßnahme, für dieses Risiko, in diesem Kontext, zu diesem Zeitpunkt gewählt?

- Bedrohung
- Schutzbedarf
- Technische Optionen
- Wirksamkeit
- Wirtschaftlichkeit
- Restrisiko

Nachweisbarkeit entsteht aus der nachvollziehbaren Abwägung dieser Faktoren.

BSI-Methodik: vom etablierten Grundschutz zur maschinenlesbaren Bereitstellung

Grundschutz++ liefert Methodik und Anforderungen; die Bibliothek stellt diese strukturiert bereit.

ETABLIERT

IT-Grundschutz

Methodischer Ordnungsrahmen

- **BSI-Standard 200-1**
  ISMS
- **BSI-Standard 200-2**
  Vorgehensweisen
- **BSI-Standard 200-3**
  Risikoanalyse
- **IT-Grundschutz-Kompendium**
  Anforderungen

WEITERENTWICKLUNG

Grundschutz++

Neuentwicklung des Grundschutzes

Methodik

Prozessorientierter Rahmen für Aufbau und Weiterentwicklung eines ISMS

Anwenderkatalog

Technische und organisatorische Anforderungen in standardisiertem Format

BEREITSTELLUNGSPLATTFORM

Stand-der-Technik-Bibliothek

Strukturiert und maschinenlesbar

- Kataloge und Profile
- Anforderungen und Maßnahmen
- Mappings und Zuordnungen
- Perspektivisch toolgestützte Nutzung

Mit der Stand-der-Technik Bibliothek soll schrittweise gemeinsame Referenzbasis entstehen

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

Das BSI verbindet etablierte Sicherheitsmethodik mit einer schrittweise ausgebauten Bibliothek.

FACHLICHE BASIS

Normen, Standards und Community

einschließlich Grundschutz++

BSI - LEISTUNG

Strukturieren und referenzieren

standardisiert und maschinenlesbar

ERGEBNIS

Stand-der-Technik-Bibliothek

gemeinsame, digital nutzbare Referenzbasis

Zielbild

1. **Einordnen** – Anforderungen auffinden
2. **Zuordnen** – Bezüge und Mappings nutzen
3. **Umsetzen** – Maßnahmen anschlussfähig machen
4. **Nachweisen / Prüfen** – perspektivisch toolgestützt

TeleTrusT macht aus dem Rechtsbegriff eine nachvollziehbare Orientierung

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

Der Ansatz verbindet regulatorische Einordnung, Methodik und praxisnahe Fachkapitel.

Arbeitskreis „Stand der Technik“

Rechtliche Grundlagen
erklärend

Bewertungs-Methode
transparent

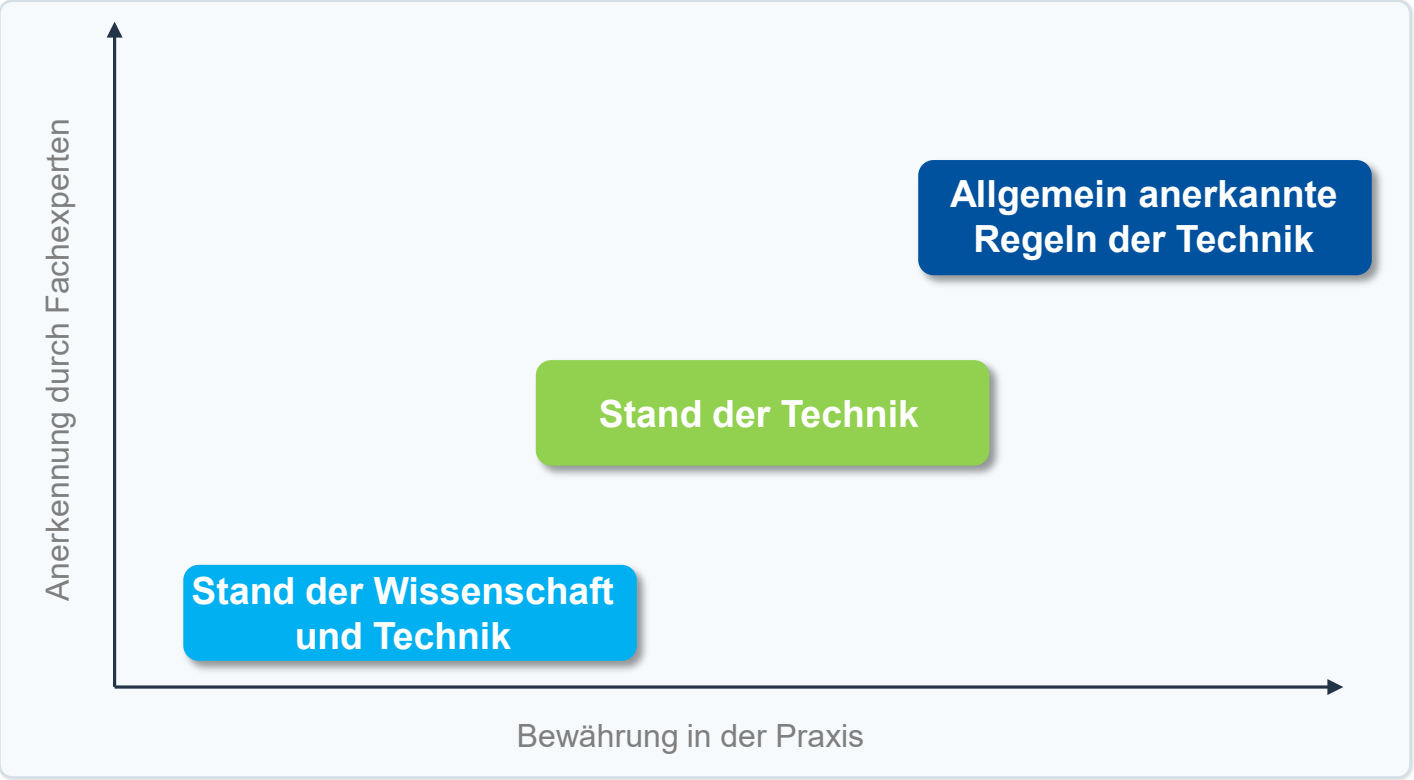
Fachkapitel
praxisnah

Orientierungs-grundlage (Handreichung)
menschenlesbar

Fachliche Einordnung + verständliche Erläuterung + Fachverband-Wissen

Anerkennung, Bewährung und transparente Bewertung machen die Einordnung belastbar

Die Methode ordnet Maßnahmen entlang zweier Dimensionen ein.



Kriterienbeispiele

- Dokumentation
- Normenbezug
- Empfehlung anerkannter Gremien
- unabhängige Prüfung
- Innovationsgrad
- Erprobung
- Marktalternativen
- Aktualisierungsintervall

Transparenz ist Teil des Ergebnisses: Warum wurde so eingeordnet?

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

Die Unterschiede und Gemeinsamkeiten auf einen Blick

Kriterium	BSI Stand-der-Technik-Bibliothek	TeleTrusT Handreichung “Stand der Technik”
Institution	Bundesbehörde / gesetzlicher Auftrag	Fachverband / Expertenkreis / Wirtschaft, Verwaltung und Wissenschaft
Primärformat	Maschinenlesbarer Ansatz	Menschenlesbare Handreichung
Schwerpunkt	Maschinenlesbare Strukturierung	Fachliche Orientierung
Stärke	Skalierung + Wiederverwendung	Kontext + Verständlichkeit
Beste Nutzung	Perspektivisch: Toolunterstützung + Überwachung	Begründung + Kommunikation
Grenze	Im Aufbau; Inhalte werden sukzessive erweitert, Keine Einzelfallbewertung	keine Einzelfallbewertung

Im weiteren Ausbau

Gemeinsame Orientierung trotz unterschiedlicher Rollen

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

1 Gemeinsamer Themenraum

BSI und TeleTrusT befassen sich mit Sicherheitsmaßnahmen und deren Einordnung.

2 Unterschiedliche Bewertung möglich

Eine Maßnahme kann aufgrund verschiedener Kriterien, Quellen oder Zeitstände unterschiedlich bewertet werden.

3 Regelmäßiger Austausch

Transparente Kriterien und fachlicher Dialog schaffen Anschlussfähigkeit und einen möglichst breiten Konsens.

Ziel ist ein möglichst breiter Konsens.
Verbleibende Abweichungen müssen transparent und nachvollziehbar sein.

Vom Stand der Technik zur belastbaren Sicherheitsentscheidung

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

Orientierung

Technisches Niveau einordnen

Welche fortschrittlichen, verfügbaren und fachlich tragfähigen Lösungen existieren heute?

Sicherheitsentscheidung

Angemessenheit bestimmen und nachweisen

Welche dieser Optionen brauchen wir für unser konkretes Risiko und unseren konkreten Nutzungskontext?

BEWERTEN › BEGRÜNDEN › DOKUMENTIEREN › AKTUALISIEREN

Orientierung zum technischen Niveau kommt von außen.
Auswahl, Nachweisführung und regelmäßige Überprüfung bleiben bei der Organisation.

Q & A