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

TeleTrusT meets CISO Alliance

-Workshop-

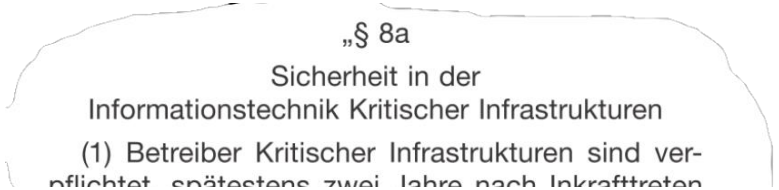
Berlin, 11.05.2023

Karsten U. Bartels, Tomasz Lawicki
Bundesverband IT-Sicherheit e.V. (TeleTrusT)

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

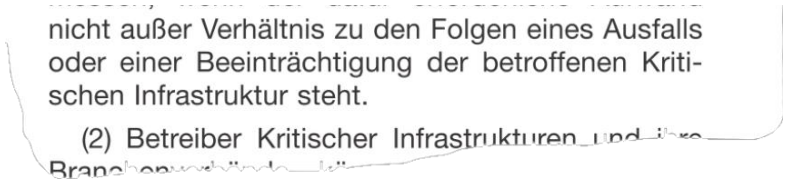
TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

ITSiG, nun ITSiG 2.0 (BSIG)
seit 2015



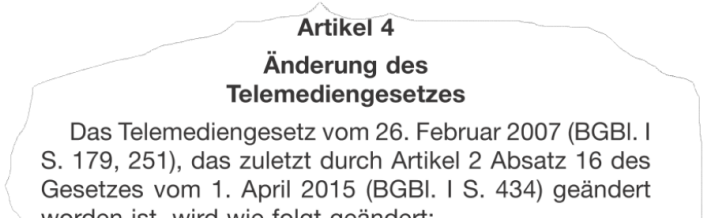
„§ 8a
Sicherheit in der
Informationstechnik Kritischer Infrastrukturen
(1) Betreiber Kritischer Infrastrukturen sind ver-

"Betreiber kritischer Infrastrukturen sind verpflichtet [...] organisatorische und technische Vorkehrungen […] zu treffen […] Dabei soll der **Stand der Technik** eingehalten werden.[…]"



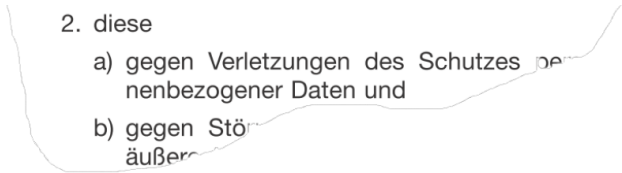
nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.
(2) Betreiber Kritischer Infrastrukturen

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



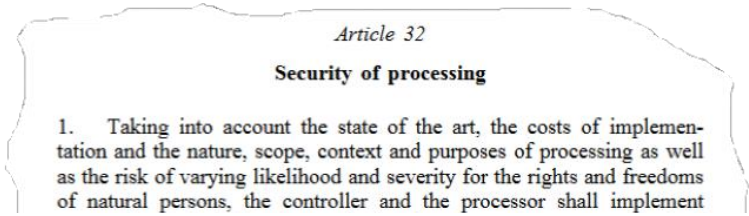
Artikel 4
Änderung des Telemediengesetzes
Das Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179, 251), das zuletzt durch Artikel 2 Absatz 16 des Gesetzes vom 1. April 2015 (BGBl. I S. 434) geändert

"Diensteanbieter haben… sicherzustellen, dass kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist […] Vorkehrungen […] müssen den **Stand der Technik** berücksichtigen.[…]"



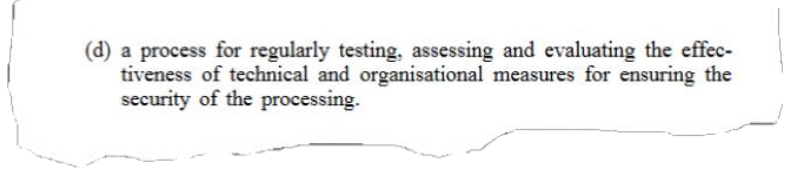
2. diese
a) gegen Verletzungen des Schutzes
nenbezogener Daten und
b) gegen Stö
äußer

DSGVO (GDPR)
seit 2018



Article 32
Security of processing
1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement

"Unter Berücksichtigung des **Stands der Technik** […] treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Sicherheitsmaßnahmen, um ein dem Risiko angemessenes Schutzniveau 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.

Weitere Gesetze und Novellierungen folgten bereits oder sind in Vorbereitung

Der "Stand der Technik" im Gesetz (DE/ EU)

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

Pflicht, Verbrauchern IT-Sicherheits-Updates zur Verfügung zu stellen (§ 327 f BGB)

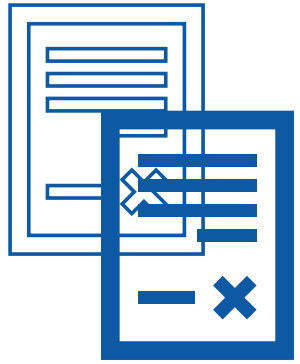
Geschäftsgeheimnisschutz-Gesetz (GeschGehG)

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

EU Cyber Resilience Act-Entwurf

Stand der Technik im Vertrag

Der Stand der Technik von IT-Sicherheitsleistungen
- als Hauptleistung oder Nebenleistung.



Fragen, die aus der Gesetzgebung entstanden

- Was ist Stand der Technik in der IT-Sicherheit?
- Wie kann ich den Stand der Technik in der IT-Sicherheit bestimmen?
- Wie kann ich den Stand der Technik in der IT-Sicherheit einhalten?
- Wie gut ist meine Infrastruktur aufgestellt?
- Was muss ich tun?
- Was wird es mich kosten?
- etc.

Der Arbeitskreis "Stand der Technik"

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.

Die Kalkar-Entscheidung als Grundlage

* auch als "Stand der Wissenschaft und Technik" bezeichnet

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

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

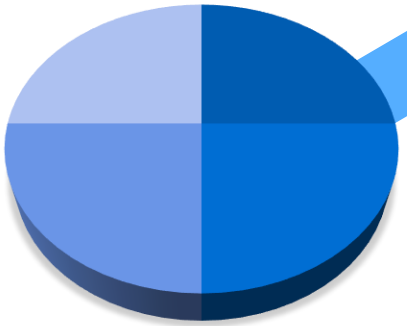
Kriterien zur Einordnung der Technologiestände

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

Allgemeine Anerkennung durch führende Fachleute

Stand der Dokumentation

Normenbezug



Empfehlung anerkannter Gremien

Prüfung konzeptioneller Eignung

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

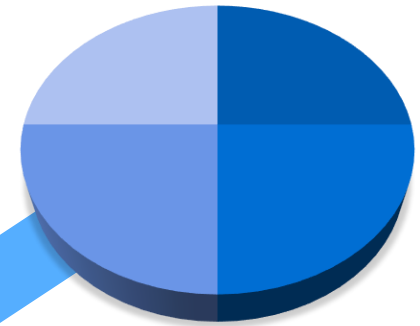
Bewertung vom AK SdT auszufüllen.

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					

Bewährung in der Praxis

Grad der Innovation

Stand der Erprobung



Vergleichbarkeit am Markt

Intervall der Aktualisierung

Einordnung der Technologiestände

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

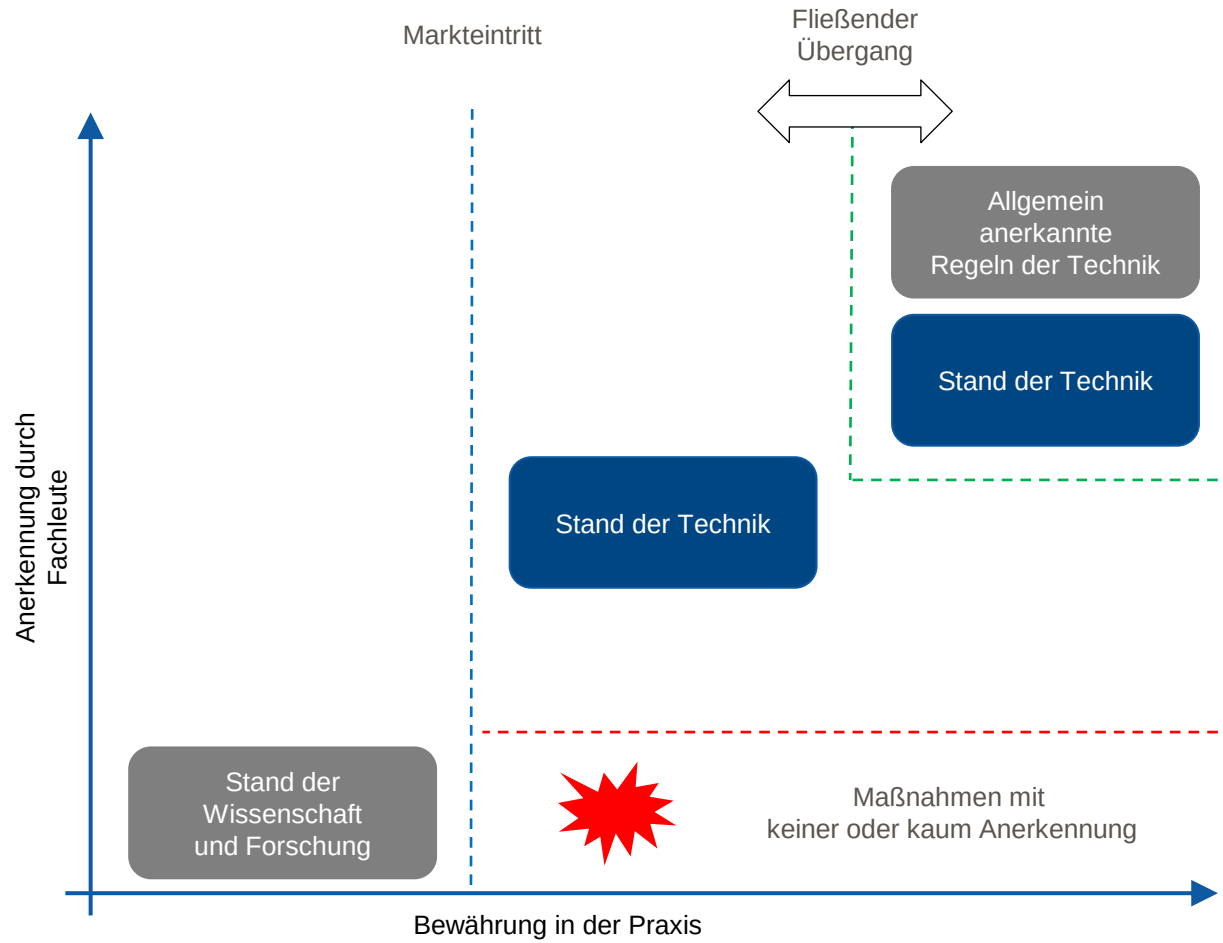
[bitte begründen Sie Ihre Antwort hier]

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



Inhalte der Handreichung "Stand der Technik" in der IT-Sicherheit

Ausschnitt

Technische Maßnahmen

- Cloudbasierter Datenaustausch
- Datenablage in der Cloud
- Durchsetzung starker Passwörter
- Endpoint Detection & Response Platform
- Fernzugriff auf Netzwerke/Fernwartung
- Internetnutzung mit Web-Isolation
- IDS/ IPS
- Kommunikation mittels Instant-Massenger
- Kryptografische Verfahren
- Management mobiler Geräte
- Multifaktor-Authentifizierung
- Nutzung von mobilen Sprach- und Datendiensten
- PKI
- Router-Sicherheit
- Schutz des Web-Datenverkehrs
- Schutz von Web-Anwendungen
- Serverhärtung
- Verschlüsselung von Dateien und Ordnern
- Verschlüsselung von E-Mails
- Verschlüsselung von Festplatten
- VPN (Layer3 / Layer2)

Exkurs

Anwendungs-beispiele

Ausschnitt

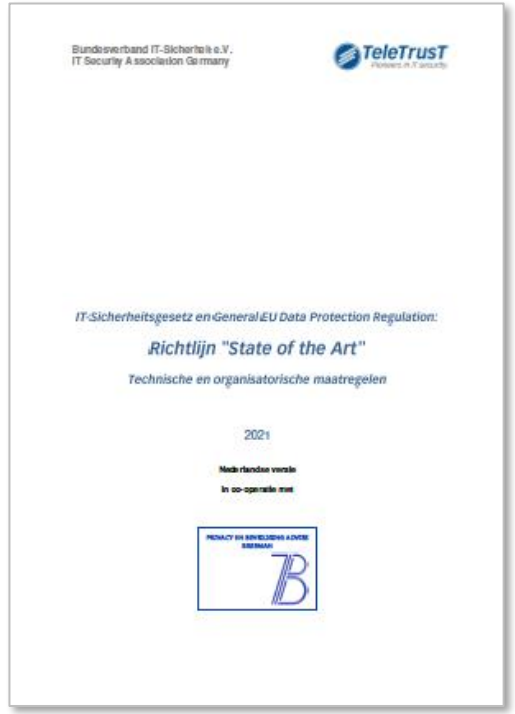
Organisatorische Maßnahmen

- Anforderungsmanagement
- Audits und Zertifizierung
- Dokumentations- und Kommunikationsmanagement
- IT-Servicemanagement
- Management der Erfolgskontrolle
- Management der Erklärung zur Anwendbarkeit
- Management der Informationssicherheits-Leitlinie
- Management des Geltungsbereichs
- Management von Informationssicherheitsrisiken
- Prozesszertifizierung
- Ressourcenmanagement
- Schwachstellen - und Patchmanagement
- Sichere Softwareentwicklung
- Sicherheitsorganisation
- Standards und Normen
- Verbesserungsmanagement (kontinuierlicher Verbesserungsprozess)
- Wissens- und Kompetenzmanagement

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