Status der Überarbeitung der TR-03174
- Sichere Anwendungen im Finanzwesen -

Bundesamt
für Sicherheit in der
Informationstechnik

Agenda

- Zur Person
- Referat D24 Gesundheits- und Finanzwesen
- Warum eine Überarbeitung der TR-03174?
- Aufgaben zur Zielerreichung
- Fragen und Diskussion

Bild: © AdobeStock/Liudmyla

Zur Person / Vorstellung

Bild: © AdobeStock/Azazul

Zur Person

Andreas Schwiemann, Referent im BSI Referat D24, „Gesundheits- und Finanzwesen“

- Ausbildung zum Informatikkaufmann (Sparkasse Bonn)
- Master in Finanzmanagement und Unternehmensführung (Hochschule Koblenz)
- CISA, CRISC, CISM, COBIT, ITIL und weitere Zertifizierungen
- Service-Manager (prosystemsIT / Wincor-Nixdorf)
- Informationssicherheitsbeauftragter (Sparkasse KölnBonn)
- IT-Revisor (Debeka-Versicherung)
- Abteilungsleiter IT, Organisation und Digitalisierung (Stadtverwaltung Andernach)
- Seit 2025 Referent beim Bundesamt für Sicherheit in der Informationstechnik

Referat D24 Gesundheits- und Finanzwesen

Referat D24 „Gesundheits- und Finanzwesen“

Referat des Bereichs „Digitalisierung“ des BSI

Kleines Team zu Finanzen mit folgenden Themenschwerpunkten:

- Staat und Verwaltung (z.B. EU, Bundesbank, verschiedene Ministerien und Bundesanstalten, Landes- und Kommunalverwaltungen)
- Banken, Sparkassen, Finanzdienstleister, Verbände, etc. sowie zugehörige IT-Dienstleister
- (End-)Kundinnen und (End-)Kunden (Infos, Verbraucherschutz, etc.)

Wir sind Kompetenzstelle für Cybersicherheit im Finanzwesen.
Wir unterstützen und beraten auf dem aktuellen Stand der Technik.
Wir können auf ca. 1.800 Expertinnen und Experten zurückgreifen.

TR-03174 – Historie und Überarbeitung

Warum eine TR für das Finanzwesen?

Ist die bestehende Regulatorik nicht ausreichend?

- Durch MaRisk, PSD2, technische Standards (RTS), DORA, etc. sind die Vorgaben im europäischen Finanzwesen umfangreich. Der Sicherheitsstandard ist hoch.

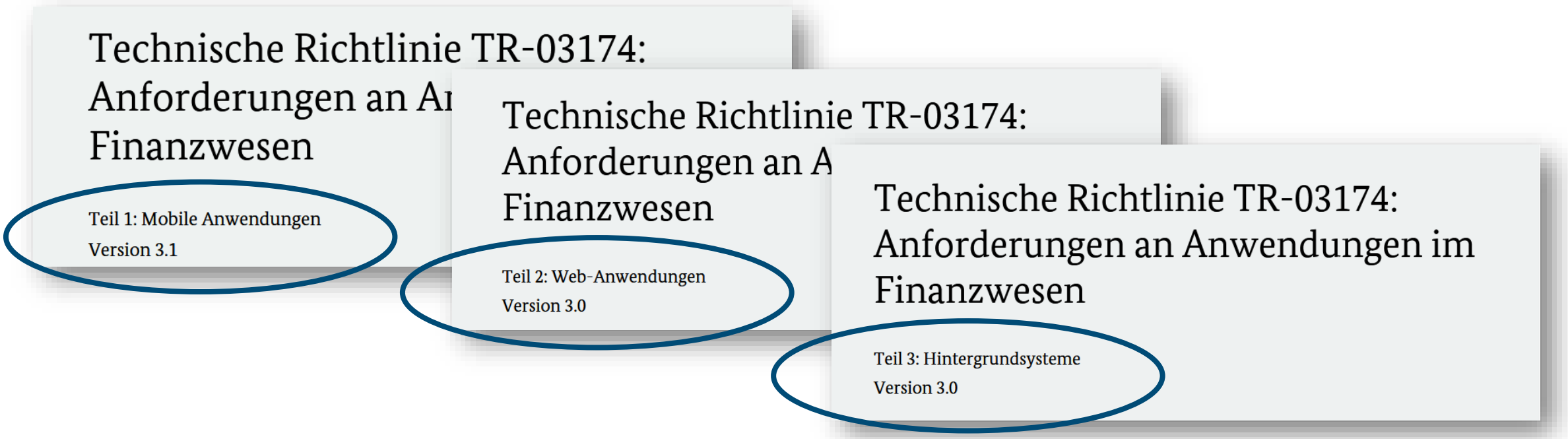
- Die Regulatorik berücksichtigt nicht alle technischen Aspekte einer IT-Infrastruktur. Hier kann das BSI zur Unterstützung herangezogen werden

- Das Finanzwesen ist (weiterhin) im Fokus der Cyberkriminalität (Auszug BSI Lagebild 2025: „*In den vergangenen 12 Monaten hat der größte Anteil der Betroffenen Cyberkriminalität in Form von Betrug im Allgemeinen erfahren (43 %). Die Gruppe der Betrugsfälle umfasste dabei den Betrug beim Online-Banking (11 %), …“)*

- Bei Vorfällen ist die Meinung des BSI zur Sicherheit im Finanzwesen sehr gefragt

Was ist bzw. sind die TR-03174? Kurze Historie

Die TR-03174 ist eine dreiteilige Technische Richtlinie zu Anwendungen im Finanzwesen



- Ursprung der TR ist die „TR-03161 Anforderungen an Anwendungen im **Gesundheitswesen**“. Diese wurde an das **Finanzwesen** angepasst.
- Fokus liegt auf der sicheren Planung, Auditierung und Nutzung der Anwendungen im Finanzwesen.

Warum eine Überarbeitung der TR-03174?

Um Korrekturen durchzuführen und die Ausrichtung zu verändern!

- **Fehlende Referenzen auf Quellen**
  => Es befinden sich Verweisfehler im Dokument

- **Restanten aus der TR-03161 (Gesundheit), fehlender Finanzbezug**
  => Verweise auf z.B. Krankenkassen und die TR-03161

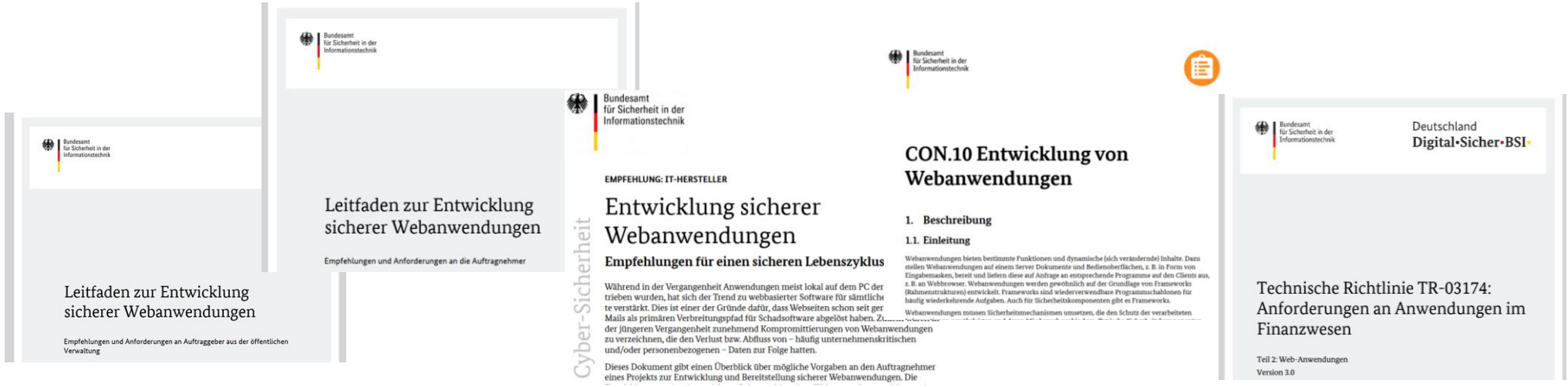
- **Gegensätzliche Vorgaben aus BSI-Grundschutz und TR-03174**
  => Unterschiede IT-Grundschutz und TR, z.B. bei der Verschlüsselung von Backups

- **Kritik der Deutschen Kreditwirtschaft bzw. BaFin an Formulierung und Inhalt**
  => Konkretisierung der EBA-Vorgaben nicht Aufgabe des BSI, falsche Zielsetzung der TR
  => Gegensätze zwischen PSD 2 und TR-03174 bzw. TR geht über regulatorische Anforderungen hinaus

Warum eine Überarbeitung der TR-03174?

Um den Nutzen zu erhöhen!

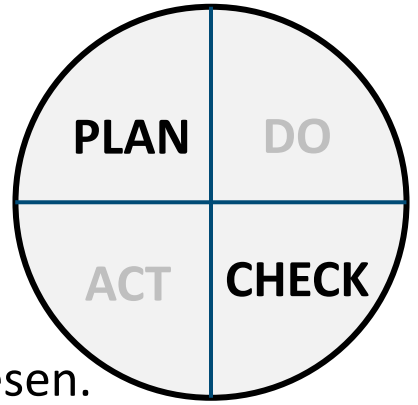
- **Hat ein App- bzw. Softwareentwickler die Aufgabe, sich mit den regulatorischen Standards auseinanderzusetzen, hat er eine gewaltige Aufgabe vor sich:**
  - Regulatorische Texte (PSD 2 + DORA)
  - Sowie verschiedene technische Richtlinien und Leitfäden der EBA bzw. BaFin
- **Hinzu kommen die drei Teile der TR-03174 (wenn diese alle benötigt werden): 176 Seiten**
- **Und ggf. weitere Bausteine, Leitlinien, Technische Richtlinien (z.B. TR-02102), etc. des BSI bzw. der ISO**



TR-03174 – Ziel und Umsetzung

Idee Zielsetzung

Was soll mit der TR erreicht werden?



- **Ziel:** Die TR-03174 ist Empfehlung und Hilfestellung, insb. für die sichere
  - Planung und
  - Prüfung

  von Mobilen Anwendungen, Web-Anwendungen und Backend-Systemen im Finanzwesen.

  Durch Umsetzung der TR werden die Empfehlungen des BSI zur Informationssicherheit eingehalten und die Besonderheiten des Finanzwesens berücksichtigt.

  ABER die Umsetzung der TR garantiert nicht die Einhaltung der kompletten Regulatorik. Es handelt sich um eine technische Ergänzung!

Aufgaben zur Zielerreichung

Was ist zu tun?

Aufgaben zur Zielerreichung:

1. Abgleich der Inhalte der TR mit der Regulatorik und den BSI-Vorgaben.
2. Straffung der Inhalte der TR auf das Wesentliche (bis zu 50% Kürzung wenn möglich)
3. Verbesserung der Nutzbarkeit durch eine Checkliste bzw. eine Arbeitstabelle
4. Konsultation mit späterem Nutzerkreis und Experten

Umsetzung der Aufgaben zur Zielerreichung (1/5)

Abgleich und Straffung der Inhalte

1. Aufgabe (Abgleich): Empfehlungen auf Basis des BSI-Grundschutzes unter Berücksichtigung der regulatorischen Vorgaben (PSD2, RTS, DORA, etc.).

Bestandteile der TR bzw. Dokumente des BSI mit denen ein **Abgleich** erfolgt ist sind insbesondere:

- APP.1.4 Mobile Anwendungen (Apps)
- APP.3.1 Webanwendungen und Webservices
- CON.10 Entwicklung von Webanwendungen
- APP.3.1.A9 Beschaffung von Webanwendungen und Webservices
- Sowie weitere TR und Leitfäden

Umsetzung der Aufgaben zur Zielerreichung (2/5)

Abgleich und Straffung der Inhalte

2. Aufgabe (Straffung der Inhalte): Verkürzung > 50% am Beispiel TR-03174, Teil 1

Inhalt

Einleitung und Erläuterungen zukünftig ca. 7 Seiten (derzeit 10)

Empfehlungen zukünftig ca. 7 Seiten (derzeit 42)

Risikobewertung und Auditierung zukünftig ca. 3 Seiten (derzeit 2)

Anhänge und Verweise zukünftig ca. 6 Seiten (derzeit 6)

Umsetzung der Aufgaben zur Zielerreichung (3/5)

Abgleich und Straffung der Inhalte

ALT

3.1.1 Prüfaspekt (1): Anwendungszweck

O.Purp_1	Der Hersteller MUSS die rechtmäßigen Zwecke der Anwendung und die Verarbeitung von personenbezogenen Daten vor der Installation offenlegen (etwa in der Beschreibung des App-Stores; vgl. Anhang A) und den Nutzer mindestens bei der erstmaligen Inbetriebnahme darüber informieren.
O.Purp_2	Die Anwendung DARF KEINE Daten erheben und verarbeiten, die nicht dem rechtmäßigen Zweck der Anwendung dienen.

Bisher in TR

Kommt in TR

4.3.1 Testcharakteristik zu Prüfaspekt (1): Anwendungszweck

Tabelle 4: Testcharakteristik: Anwendungszweck

Prüfaspekt	Kurzfassung des Prüfaspekts	Prüftiefe	Anmerkungen
O.Purp_1	Informationspflicht des Herstellers zum rechtmäßigen Zweck und Verarbeitung von personenbezogenen Daten.	CHECK	Der Evaluator prüft, ob eine Beschreibung vorhanden ist und diese den rechtmäßigen Zwecken der Anwendung entspricht. Dabei werden die vom Hersteller definierten rechtmäßige Zwecke als Grundlage genutzt. Eine juristische Prüfung der Rechtmäßigkeit ist nicht erforderlich.
O.Purp_2	Zweckgebundene Erhebung und Verarbeitung der Daten.	CHECK	Die Nutzung von Sensordaten ist nur soweit zulässig, wie sie etwa zur Erhebung des Seeds dient. Der Evaluator prüft anhand der

Bisher in TR

Fällt weg

Bisher in TR

Kommt in Anlage

NEU

4.1 Anwendungszweck

Tabelle 1: Anwendungszweck

Kürzel	Empfehlung
O.Purp_1	Der Hersteller **MUSS** die rechtmäßigen Zwecke der Anwendung und die Verarbeitung von personenbezogenen Daten dem Nutzer gegenüber offenlegen (z.B. in den Nutzungsbedingungen).
O.Purp_2	Zur Wahrung der Datensparsamkeit und Zweckbindung **DARF** die Anwendung **KEINE** Daten erheben und verarbeiten, die nicht dem rechtmäßigen Zweck der Anwendung dienen bzw. für diesen notwendig sind.

Kürzel	Empfehlungen	Prüftiefe	Erläuterung Prüfung
O.Purp_1	Der Hersteller **MUSS** die rechtmäßigen Zwecke der Anwendung und die Verarbeitung von personenbezogenen Daten dem Nutzer gegenüber offenlegen (z.B. in den Nutzungsbedingungen).	CHECK	Der Evaluator prüft, ob eine Beschreibung vorhanden ist und diese den rechtmäßigen Zwecken der Anwendung entspricht. Dabei werden die vom Hersteller definierten rechtmäßigen Zwecke als Grundlage genutzt. Hierbei ist auch augenmerk darauf zu legen, ob ggf. Daten in einem Drittland verarbeitet werden und ob auf entsprechende Datenschutzvorgaben hingewiesen wird. Eine juristische Prüfung der Rechtmäßigkeit ist nicht erforderlich.
O.Purp_2	Zur Wahrung der Datensparsamkeit und Zweckbindung **DARF** die Anwendung **KEINE** Daten erheben und verarbeiten, die nicht dem rechtmäßigen Zweck der	CHECK	Die Nutzung von Sensordaten ist nur soweit zulässig, wie sie etwa zur Erhebung des Seeds dient. Der Evaluator prüft anhand der Permisson-Policy, welche Daten in der

Umsetzung der Aufgaben zur Zielerreichung (4/5)

Die Inhalte der TR werden in einer Tabelle zusammengefasst

3. Aufgabe (Verbesserung der Nutzbarkeit): Die TR bekommt einen tabellarischen Anhang mit allen Empfehlungen und zusätzlichen Informationen => Planungs-, Arbeits- und Auditierungsgrundlage

Empfehlungen **Auditierung** **Ergänzende Informationen** **Bemerkungen / Bewertung**

Kürzel	Empfehlungen	Prüftiefe	Erläuterung Prüfung	BSI GS-Katalog/TR	PSD 2 (Richtlinie)	DORA / RTS RMF	Erläuterung Ergebnisse Prüfung	Kritikalität	Bewertung
O.Resi_1	Die Anwendung **MUSS** eigene Prüfmechanismen implementieren, die beim Start der Anwendung feststellen, ob sie in einer Entwicklungs-/Debug-Umgebung ausgeführt wird. Wenn die Anwendung feststellt, dass sie in einer Entwicklungs-/Debug-Umgebung ausgeführt wird, **MUSS** sie sich sofort beenden.	CHECK	Der Evaluator prüft die Wirksamkeit der Debug-Erkennung durch praktische Tests (vergleiche O.Resi_5).	**CON.8.A7** 7 Durchführung von entwicklungsbegleitenden Software-Tests (B)		**Delegierte Verordnung (EU) 2024/1774, Artikel 8 (2) b) v)**		Bitte auswählen	Bitte auswählen
O.Resi_2	Die Anwendung **MUSS** eigene Prüfmechanismen implementieren, die beim Start der Anwendung feststellen, ob sie	CHECK	Der Evaluator prüft die Wirksamkeit der Erkennung durch praktische Tests (vergleiche	**CON.8.A5** Sicheres Systemdesign (B)					

Die Software MUSS in einer Test- und Entwicklungsumgebung getestet werden, die getrennt von der Produktionsumgebung ist.

Die Finanzunternehmen entwickeln, dokumentieren und implementieren … Anforderungen an die Trennung von IKT-Produktionsumgebungen von Entwicklungs-, Test- und anderen Nicht Produktionsumgebungen, …

Umsetzung der Aufgaben zur Zielerreichung (5/5)

Abstimmung mit den späteren Nutzern der TR

4. Aufgabe (Konsultation Nutzerkreis): Hauptkritikpunkte an bestehender TR-03174 sind

- Der mangelnde Bezug zum Finanzwesen und
- Die fehlende Abstimmung im Vorfeld der Veröffentlichung.

Dem soll bei der Überarbeitung durch ein frühzeitiges Einbeziehen möglicher Nutzer und einer transparenten Vorgehensweise vorgesorgt werden.

=> Hierzu zählt u.a. auch dieser Vortrag!

Bestehende Arbeitspakete und weitere Zukunft

Zeitliche Planung der Umsetzung aus Mitte 2025

- **Erstellung eines ersten Entwurfs der TR** (bis Ende September 2025)
- **Beginn Abstimmung ab Oktober**

Paket 1 (Okt. 2025)

- **Erneuerung der drei TR nach Abstimmung inkl. Arbeitstabellen**
- **Weitere Abstimmung** (in Q4 2025)
- **Veröffentlichung** der überarbeiteten Technischen Richtline 03174 Ende Januar 2026

Paket 2 (Januar 2026)

- **Vorstellung und Diskussion** => kontinuierliche Verbesserungen

Mögliche Zukunft

Bundesamt
für Sicherheit in der
Informationstechnik

Vielen Dank für Ihre Aufmerksamkeit!

Andreas Schwiemann
Referent

Andreas.schwiemann@bsi.bund.de
Tel.: +49 (0) 228 9582 6930
Mobil: +49 151 – 564 933 29

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 87
53175 Bonn

www.bsi.bund.de

Follow us: