Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Herzlich Willkommen

Sicherheit von Anwendungen im Gesundheitswesen

Jeschke, Pascal – DI 24
Kleinmanns, Christian – DI 24

Gliederung

- Vorstellung BSI / Aufgabenbereiche DI 24
- Erfahrungen Sicherheitsanalysen von Gesundheitsanwendungen
- Erfahrungen digitale Pandemiebekämpfung
- Gesetzliche Zuständigkeit
- TR-Zertifizierungsverfahren
- Besonderheiten der TR 03161

Gliederung

- Vorstellung BSI / Aufgabenbereiche DI 24
- Erfahrungen Sicherheitsanalysen von Gesundheitsanwendungen
- Erfahrungen digitale Pandemiebekämpfung
- Gesetzliche Zuständigkeit
- TR-Zertifizierungsverfahren
- Besonderheiten der TR 03161

Das BSI ist die Cyber-Sicherheitsbehörde des Bundes.

Das BSI gestaltet (als zentrales Kompetenzzentrum der Informationssicherheit) die sichere Digitalisierung in Deutschland.

Informationssicherheit und Digitalisierung gehören untrennbar zusammen: Sie sind zwei Seiten einer Medaille und des BSI.

Produkte und Dienstleistungen

Übernahme technischer Schutzmaßnahmen
Sichere mobile Lösungen, Schadsoftware-Prävention, Analysen, DDoS-Mitigation, IT-Notfallmanagement für Regierungsnetze, Angriffserkennung, Nationales IT-Lagezentrum, Technische Richtlinien (TR)

Kooperation
Nationales Verbindungswesen, Cyber-Sicherheitstage, IT-Grundschutztage, Jahrestagung der Informationssicherheitsbeauftragten (ISB), Beirat Digitaler Verbraucherschutz, Cyber-Abwehrzentrum, Allianz für Cybersicherheit, UP KRITIS

Technische Unterstützung und Dienstleistungen
CERT-Bund, Kryptosysteme, Abstrahl-/Lauschabwehrprüfungen, IS-Penetrationstests, Mobile Incident Response Teams (MIRTs), technische Evaluierung, Malware Information Sharing Platform (MISP), Warnungen

Begleitung in der Aus- und Fortbildung
ISB-Ausbildung, Sensibilisierungsvorträge (u. a. Live Hacking), Übungszentrum Netzverteidigung

Beratung
Managementsystem für Informationssicherheit (ISMS), Abhörsicherheit, nach Vorfallsmeldungen, Unterstützung Digitalisierungsprojekte, Digitaler Persönlichkeits- und Verbraucherschutz, Gesellschaftlicher Dialog, Service-Center

Information
IT-Grundschutz, Mindeststandards, Technische Richtlinien (TR), CS-Empfehlungen, Liste zertifizierter und zugelassener Produkte, Lageberichte, Zertifizierungen, IT-Sicherheitskennzeichen (IT-SiK)

Aufgabenbereiche Referat DI 24

Telematik-infrastruktur (TI)

- elektronische Gesundheitskarte
- elektronisches Rezept
- elektronische Patientenakte

Sicherheit von Medizinprodukten

- Schwachstellen-analysen
- Marktsichtung

Sicherheitsvorfälle

- Zusammenarbeit Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM)
- Lagezentrum

IT-Sicherheitsvorgaben

- Technische Richtlinien
- Prüfspezifikationen
- Schutzprofile
- Prüfverfahren

Sicherheit von Bezahlverfahren

- Credit
- Debit

Know Your Customer (KYC)-Verfahren

- Expertengruppen
- Geldwäsche

Anforderungen an anwendungs-spezifische Authentifizierungs-verfahren

- Biometrie-anforderungen
- Multifaktor-Authentifizierung

(Europäische) Arbeitsgruppen

- Secure Element/eUICC
- Hardware-sicherheitsanker

Aufgabenbereiche Referat DI 24

Telematik-infrastruktur (TI)

- elektronische Gesundheitskarte
- elektronisches Rezept
- elektronische Patientenakte

Sicherheit von Medizinprodukten

- Schwachstellen-analysen
- Marktsichtung

Sicherheitsvorfälle

- Zusammenarbeit Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM)
- Lagezentrum

IT-Sicherheitsvorgaben

- Technische Richtlinien
- Prüfspezifikationen
- Schutzprofile
- Prüfverfahren

Sicherheit von Bezahlverfahren

- Credit
- Debit

Know Your Customer (KYC)-Verfahren

- Expertengruppen
- Geldwäsche

Anforderungen an anwendungs-spezifische Authentifizierungs-verfahren

- Biometrie-anforderungen
- Multifaktor-Authentifizierung

(Europäische) Arbeitsgruppen

- Secure Element/eUICC
- Hardware-sicherheitsanker

Gliederung

- Vorstellung BSI / Aufgabenbereiche DI 24
- Erfahrungen Sicherheitsanalysen von Gesundheitsanwendungen
- Erfahrungen digitale Pandemiebekämpfung
- Gesetzliche Zuständigkeit
- TR-Zertifizierungsverfahren
- Besonderheiten der TR 03161

Erkenntnisse aus Sicherheitsanalysen

- Validierung öffentlicher Schwachstellenmeldungen
- Stichprobenartige Sicherheitsuntersuchungen von mobilen Anwendungen mit Gesundheitsbezug
- Enge Zusammenarbeit mit der Industrie
- Projekte zur Sicherheit von vernetzten Medizin- und Pflegeprodukten (u.A. ManiMed und eCare)

Manipulation von Medizinprodukten (ManiMed)

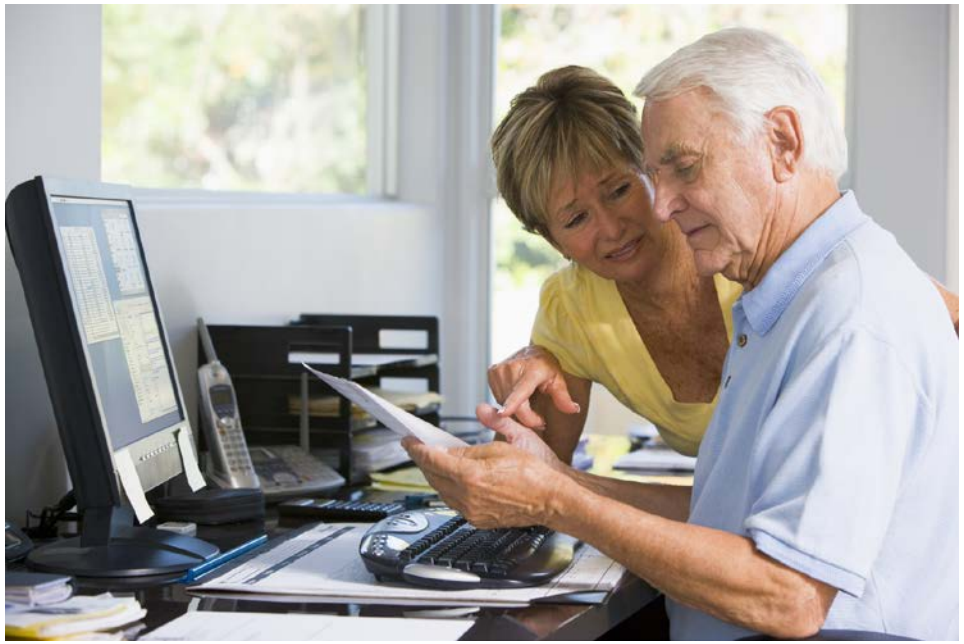
- Marktanalyse von Medizinprodukten
  - Anfragen bei Herstellern und Einrichtungen
  - Insulinpumpen, Herzschrittmacher, Defibrillatoren, Beatmungsgeräte, etc.
- Durchführung von IT-Sicherheitsuntersuchungen
  - Hard- und Software Penetrationstests
- Einleitung von CVD-Prozessen

ManiMed Ergebnisse

- Ergebnisse potentiell durch ausschließlich freiwillige Teilnahme verzerrt
- 150 gemeldete Schwachstellen
  - Häufig in Infrastruktur statt Medizinprodukt
- IT-Sicherheitslage von Hersteller zu Hersteller schwankend
- Projekt deutet auf Verbesserungsmöglichkeiten der IT-Sicherheit von Medizinprodukten hin

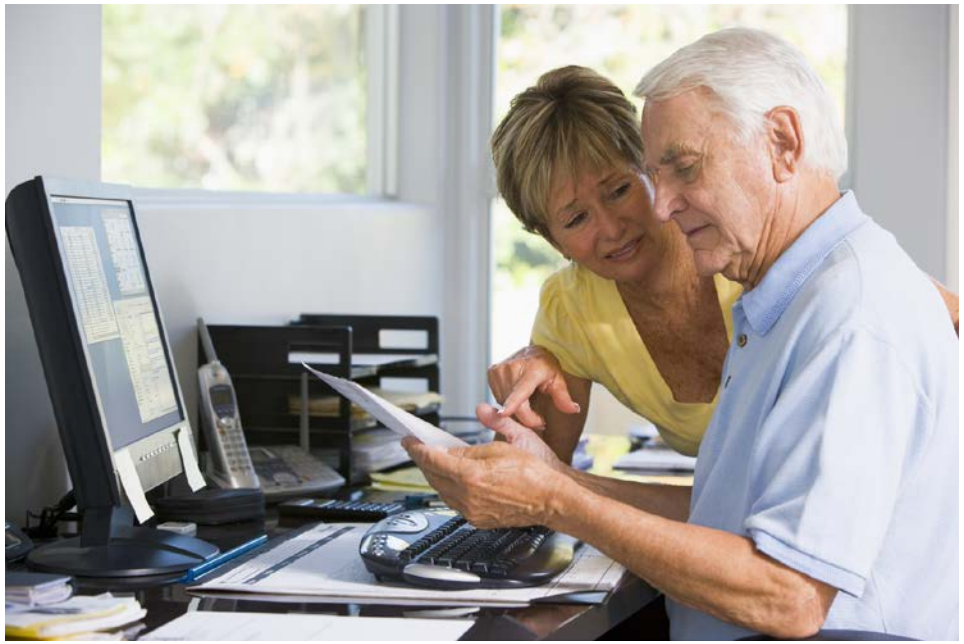
Digitalisierung in der Pflege (eCare)

- Marktanalyse von Pflegeprodukten
  - Anfragen bei Herstellern und Einrichtungen
  - Blutzuckermesssysteme, Smarte-Pillendosen, Seniorentablets, Pulsoximeter
- Durchführung von IT-Sicherheitsuntersuchungen
  - Hard- und Software Penetrationstests
  - Black-Box-Ansatz
- Einleitung von CVD-Prozessen



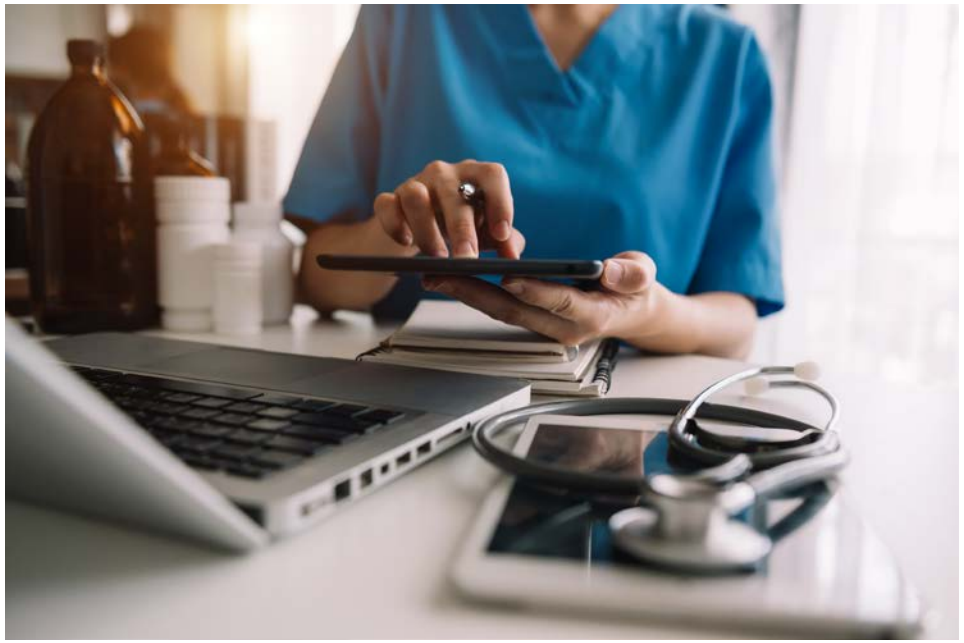
eCare Ergebnisse

- Reduzierte Aussagekraft
  - Fokussierte Testung auf Produkten und Apps
  - Hintergrundsysteme wurden nicht getestet
  - Geringe Prüftiefe
- Mittlere bis schwere Schwachstellen in allen untersuchten Produkten



Fazit der Sicherheitsanalyse von Gesundheitsanwendungen

- Vertrauensvolle Kooperation mit Herstellern
- Ausbaufähiges Gesamtbild der IT-Sicherheit im Gesundheitswesen
- Wachsende Herausforderungen durch Digitalisierung im Gesundheitswesen
- Stärkere Unterstützung durch das BSI



AdobeStock © mrmohock

Anwenden der Erkenntnisse

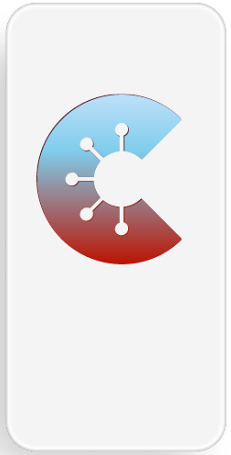
- Weiterentwicklung der Telematikinfrastruktur
- Veröffentlichung von Technischen Richtlinien (TR-03154, TR-03155, TR-03161, etc.)
- Veröffentlichung einer Prüfvorschrift für das Frontend des Versicherten für die elektronische Patientenakte und später für das elektronische Rezept

Gliederung

- Vorstellung BSI / Aufgabenbereiche DI 24
- Erfahrungen Sicherheitsanalysen von Gesundheitsanwendungen
- Erfahrungen digitale Pandemiebekämpfung
- Gesetzliche Zuständigkeit
- TR-Zertifizierungsverfahren
- Besonderheiten der TR 03161

Corona-Warn-App

- Sicherheitsuntersuchungen seit Beginn der Entwicklung im März 2020
- Bisher wurden insgesamt 39 Erweiterungen freigegeben und veröffentlicht.
- Durchführung von siebentägigen Penetrationstests und Code-Reviews in einem zweiwöchigen Rhythmus
- Teilnahme an Threat-Modeling-Workshops zu jeder neuen Version

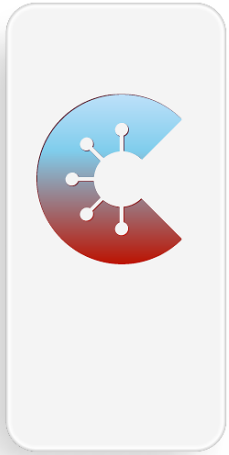


DIE CORONA-WARN-APP:

HIER GIBT'S ANTWORTEN AUF DIE WICHTIGSTEN FRAGEN.

Corona-Warn-App

- Insgesamt über 80 Schwachstellen identifiziert und mitigiert
- Beteiligung der Öffentlichkeit durch verfolgen einer Open-Source Politik
- Enge Zusammenarbeit zwischen BSI, RKI, Deutscher Telekom AG und SAP



DIE CORONA-WARN-APP:

HIER GIBT'S ANTWORTEN AUF DIE WICHTIGSTEN FRAGEN.

Digitaler Impfnachweis

- Sicherheitsuntersuchungen seit Beginn der Entwicklung im April 2021
- Bisher wurden insgesamt 25 Erweiterungen freigegeben und veröffentlicht.
- Durchführung von siebentägigen Penetrationstests und Code-Reviews in einem zweiwöchigen Rhythmus
- Enge Zusammenarbeit zwischen BSI, RKI, BMG und IBM

Zusätzliche Sicherheitsüberprüfungen

- CovBot
- Deutscher Elektronischer Sequenzdaten-Hub (DESH)
- Digitales Impfquotenmonitoring (DIM)
- European Federal Gateway Service (EFGS)
- Surveillance, Outbreak Response Management and Analysis System (SORMAS)

Gliederung

- Vorstellung BSI / Aufgabenbereiche DI 24
- Erfahrungen Sicherheitsanalysen von Gesundheitsanwendungen
- Erfahrungen digitale Pandemiebekämpfung
- Gesetzliche Zuständigkeit
- TR-Zertifizierungsverfahren
- Besonderheiten der TR 03161

Digitale Gesundheitsanwendungen (DiGA)

§ 33a SGB V

(1) Versicherte haben Anspruch auf **Versorgung mit Medizinprodukten** niedriger Risikoklasse, deren Hauptfunktion wesentlich auf digitalen Technologien beruht und die dazu bestimmt sind, bei den Versicherten oder in der Versorgung durch Leistungserbringer die Erkennung, Überwachung, Behandlung oder Linderung von Krankheiten oder die Erkennung, Behandlung, Linderung oder Kompensierung von Verletzungen oder Behinderungen zu unterstützen (digitale Gesundheitsanwendungen). Der Anspruch umfasst nur solche digitalen Gesundheitsanwendungen, die

1.vom Bundesinstitut für Arzneimittel und Medizinprodukte **[BfArM]** in das Verzeichnis für digitale Gesundheitsanwendungen nach **§ 139e** aufgenommen wurden und

2.entweder nach Verordnung des behandelnden Arztes oder des behandelnden Psychotherapeuten oder mit Genehmigung der Krankenkasse angewendet werden.

Für die Genehmigung nach Satz 2 Nummer 2 ist das Vorliegen der **medizinischen Indikation nachzuweisen**, für die die digitale Gesundheitsanwendung bestimmt ist. Wählen Versicherte Medizinprodukte, deren Funktionen oder Anwendungsbereiche über die in das Verzeichnis für digitale Gesundheitsanwendungen nach § 139e aufgenommenen digitalen Gesundheitsanwendungen hinausgehen oder deren Kosten die Vergütungsbeträge nach § 134 übersteigen, haben sie die Mehrkosten selbst zu tragen.

Digitale Gesundheitsanwendungen (DiGA)

§ 139e SGB V

(10) Das Bundesamt für Sicherheit in der Informationstechnik **[BSI]** legt im **Einvernehmen** mit dem Bundesinstitut für Arzneimittel und Medizinprodukte **[BfArM]** und im **Benehmen** mit der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit **[BfDI]** erstmals bis zum **31. Dezember 2021** und dann in der Regel jährlich die von digitalen Gesundheitsanwendungen nachzuweisenden **Anforderungen** an die **Datensicherheit** nach Absatz 2 Satz 2 Nummer 2 fest. Das Bundesamt für Sicherheit in der Informationstechnik bietet ab dem **1. Juni 2022 Verfahren** zur Prüfung der Einhaltung der Anforderungen nach Satz 1 sowie Verfahren zur Bestätigung der Einhaltung der Anforderungen nach Satz 1 durch **entsprechende Zertifikate** an. Der Nachweis der Erfüllung der Anforderungen an die Datensicherheit durch den Hersteller ist spätestens ab dem 1. Januar 2023 unter Vorlage eines Zertifikates nach Satz 2 zu führen.

Digitale Pflegeanwendungen (DiPA)

§ 40a SGB XI

(1) Pflegebedürftige haben Anspruch auf Versorgung mit **Anwendungen**, die **wesentlich auf digitalen Technologien** beruhen und von den Pflegebedürftigen oder in der Interaktion von Pflegebedürftigen, Angehörigen und zugelassenen ambulanten Pflegeeinrichtungen genutzt werden, um Beeinträchtigungen der **Selbständigkeit** oder der Fähigkeiten des Pflegebedürftigen zu mindern und einer Verschlimmerung der Pflegebedürftigkeit entgegenzuwirken, soweit die Anwendung **nicht wegen Krankheit oder Behinderung** von der Krankenversicherung oder anderen zuständigen Leistungsträgern zu leisten ist (digitale Pflegeanwendungen).

(2) Der Anspruch umfasst nur solche digitale Pflegeanwendungen, die vom Bundesinstitut für Arzneimittel und Medizinprodukte **[BfArM]** in das **Verzeichnis für digitale Pflegeanwendungen** nach **§ 78a Absatz 3** aufgenommen sind. Die **Pflegekasse** entscheidet auf **Antrag** des Pflegebedürftigen über die **Notwendigkeit** der Versorgung des Pflegebedürftigen mit einer digitalen Pflegeanwendung. Entscheiden sich Pflegebedürftige für eine digitale Pflegeanwendung, deren Funktionen oder Anwendungsbereiche über die in das Verzeichnis für digitale Pflegeanwendungen nach § 78a Absatz 3 aufgenommenen digitalen Pflegeanwendungen hinausgehen oder deren Kosten die Vergütungsbeträge nach § 78a Absatz 1 Satz 1 übersteigen, haben sie die **Mehrkosten selbst zu tragen**. Über die von ihnen zu tragenden Mehrkosten sind die Pflegebedürftigen von den Pflegekassen vorab in schriftlicher Form oder elektronisch zu informieren.

Digitale Pflegeanwendungen (DiPA)

§ 78a SGB XI

(7) Das Bundesamt für Sicherheit in der Informationstechnik **[BSI]** legt im **Einvernehmen** mit dem Bundesinstitut für Arzneimittel und Medizinprodukte **[BfArM]** und im **Benehmen** mit der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit **[BfDI]** erstmals bis zum **31. Dezember 2021** und dann in der Regel jährlich die von digitalen Pflegeanwendungen nach Absatz 4 Satz 3 Nummer 2 zu **gewährleistenden Anforderungen an die Datensicherheit** fest. **§ 139e Absatz 10 Satz 2 und 3 des Fünften Buches** gilt entsprechend.

§ 139e Absatz 10 Satz 2 und 3 SGB V

Das Bundesamt für Sicherheit in der Informationstechnik bietet ab dem **1. Juni 2022 Verfahren** zur Prüfung der Einhaltung der Anforderungen nach Satz 1 sowie Verfahren zur Bestätigung der Einhaltung der Anforderungen nach Satz 1 durch **entsprechende Zertifikate** an. Der Nachweis der Erfüllung der Anforderungen an die Datensicherheit durch den Hersteller ist spätestens ab dem 1. Januar 2023 unter Vorlage eines Zertifikates nach Satz 2 zu führen.

Gesundheitsdaten

- Das Verständnis des BSI beruht auf der Legaldefinition in Art. 4 Abs. 15 DSGVO und dem Erwägungsgrund 35 der DSGVO.
- Das BSI teilt das daraus resultierende weite Begriffsverständnis der Literatur: **alle Informationen**, welche die **Gesundheit** einer Person unter **allen Aspekten** - körperlichen wie psychischen – beschreiben als Gesundheitsdaten.
- Aus dem grundsätzlichen Verarbeitungsverbot nach Art 9 Abs. 1 DSGVO und den allgemeinen Anforderungen an die Rechtmäßigkeit der Datenverarbeitung nach Art 6 DSGVO leitet das BSI einen **hohen** bis **sehr hohen Schutzbedarf** nach BSI 200-2 ab.

Gliederung

- Vorstellung BSI / Aufgabenbereiche DI 24
- Erfahrungen Sicherheitsanalysen von Gesundheitsanwendungen
- Erfahrungen digitale Pandemiebekämpfung
- Gesetzliche Zuständigkeit
- TR-Zertifizierungsverfahren
- Besonderheiten der TR 03161

TR-Familie: Anforderungen an Anwendungen im Gesundheitswesen

- Erweiterung der bestehenden TR-03161 auf TR-Familie bestehend aus Anforderungen für:
  - mobile Anwendungen (TR-03161-1)
  - Web-Anwendungen (TR-03161-2)
  - Hintergrundsysteme (TR-03161-3)
- Jährlicher Review der Anforderungen an die Datensicherheit
- TR-Familie wurde am 03.06.2022 veröffentlicht

Prüfprozess des BSI

- Zertifizierung nach TR stellt einen DAkkS akkreditierten Zertifizierungsprozess dar.
- Die Konformitätsprüfung wird durch, vom BSI anerkannte neutrale Prüfstellen durchgeführt.
- Die Prüfung wird von der zuständigen Zertifizierungsstelle überwacht und vom zuständigen Fachreferat inhaltlich geprüft.

Zulassung Prüfstelle: TR-03161-X

- Fachliche Anforderungen an die Prüfstelle durch das Fachreferat definiert.
- Prüfstelle muss mindestens zwei kompetente TR-Prüfer für die jeweilige TR 03161-X bereitstellen.
- BSI veröffentlicht alle zugelassenen Prüfstellen auf seiner Homepage*.

(*) https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Listen/Technische-Richtlinien-TR/Liste-TR-Pruefstellen/liste-tr-pruefstellen_node.html

Zulassung Prüfer: TR-03161-X

- Fachliche Anforderungen an die Prüfstelle durch das Fachreferat definiert.
- Abgeschlossener informationstechnischer Bildungsabschluss oder fünf Jahre einschlägige Berufserfahrung
- Mind. zwei Jahre Berufserfahrung in technischen Bereichen der TR
- Nachweis der Fachkenntnis in 60 minütigem Interview

(*) https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Listen/Technische-Richtlinien-TR/Liste-TR-Pruefstellen/liste-tr-pruefstellen_node.html

Gliederung

- Vorstellung BSI / Aufgabenbereiche DI 24
- Erfahrungen Sicherheitsanalysen von Gesundheitsanwendungen
- Erfahrungen digitale Pandemiebekämpfung
- Gesetzliche Zuständigkeit
- TR-Zertifizierungsverfahren
- Besonderheiten der TR 03161

Methodik TR-03161-X

- Zertifizierung basierend auf Restrisikobewertung nach anerkannten Standards, bspw.:
  - BSI Standard 200-3
  - ISO 27005
  - Common Criteria Evaluation Methodology
- Es müssen nicht alle Anforderungen erfüllt werden

Beispiel 1: Anwendbarkeit von Prüfanforderungen in TR-03161-X

O.Resi_7	Die Anwendung SOLL Härtungsmaßnahmen, wie etwa eine Integritätsprüfung vor jeder Verarbeitung sensibler Daten innerhalb des Programmablaufs, realisieren.
O.Resi_8	Die Anwendung MUSS starke Maßnahmen gegen Reverse Engineering umsetzen.
O.Resi_9	Die Anwendung MUSS Zugriffskontrollmechanismen unter der Berücksichtigung von unterschiedlichen Plattformen und Plattformversionen implementieren, so dass ein

- Entwicklung einer OpenSource-Anwendung
- Prüflabor analysiert die Situation und die Abwägungen des Herstellers
- Prüflabor bewertet die Anforderung als „NOT APPLICABLE“

Methodik TR-03161-X

- Erfüllen von Prüfanforderungen kann Einzelfallentscheidungen erfordern.
- Einzellfallentscheidungen werden vom Prüflabor getroffen.
- Mindestens die folgenden Aspekte werden berücksichtigt
  - Schutzbedarf der Daten
  - Abwägungen der Hersteller
  - Auswirkungen auf das Restrisiko

Beispiel 2: Einzelfallentscheidungen in TR-03161-X

O.Auth_8	Die Anwendung MUSS nach einer angemessenen Zeit in der sie nicht aktiv verwendet wurde (idle time) eine erneute Authentisierung fordern.
O.Auth_9	Die Anwendung MUSS nach einer angemessenen Zeit in der sie aktiv verwendet wurde (active time) eine erneute Authentisierung fordern.
O.Auth_10	Die Authentisierungsdaten DÜRFEN NICHT ohne eine ausreichende Authentifizierung des Nutzers geändert werden.

- Die Angemessenheit kann zwischen unterschiedlichen Use-Cases variieren
  - Beispiel 1: Anwendungen zum Abspielen von Videoanleitungen (z.B.: Sportübungen)
  - Beispiel 2: Tagebuchanwendungen

Methodik TR-03161-X

- Nicht alle Prüfaspekte können auf jede Anwendung angewandt werden.
- Nicht anwendbare Prüfaspekte werden mit „NOT APPLICABLE“ gekennzeichnet.

Beispiel 1: Anwendbarkeit von Prüfaspekten in TR-03161-X

3.1.6.2	Authentifizierung über Biometrie
O.Biom_1	Die Verwendung biometrischer Systeme DARF NICHT als alleiniger Authentifizierungsmechanismus eingesetzt werden. Sie ist lediglich als Teil einer Zwei-Faktor-Authentifizierung zulässig.

- Verwendet die Anwendung keine biometrischen Systeme, kann das komplette Kapitel 3.1.6.2 im Rahmen der Zertifizierung mit „NOT APPLICABLE“ gewertet werden.
- Die Bewertung erfolgt durch das für die Zertifizierung beauftragte Prüflabor in Zusammenarbeit mit dem Hersteller.

Fazit

- Jährlicher Review der Anforderungen an die Datensicherheit
- Starke Beteiligung der Industrie
- Einzelbetrachtung der Anwendungen
- Einheitlicher Zertifizierungsprozess mit vergleichbaren Ergebnissen

Vielen Dank für Ihre Aufmerksamkeit!

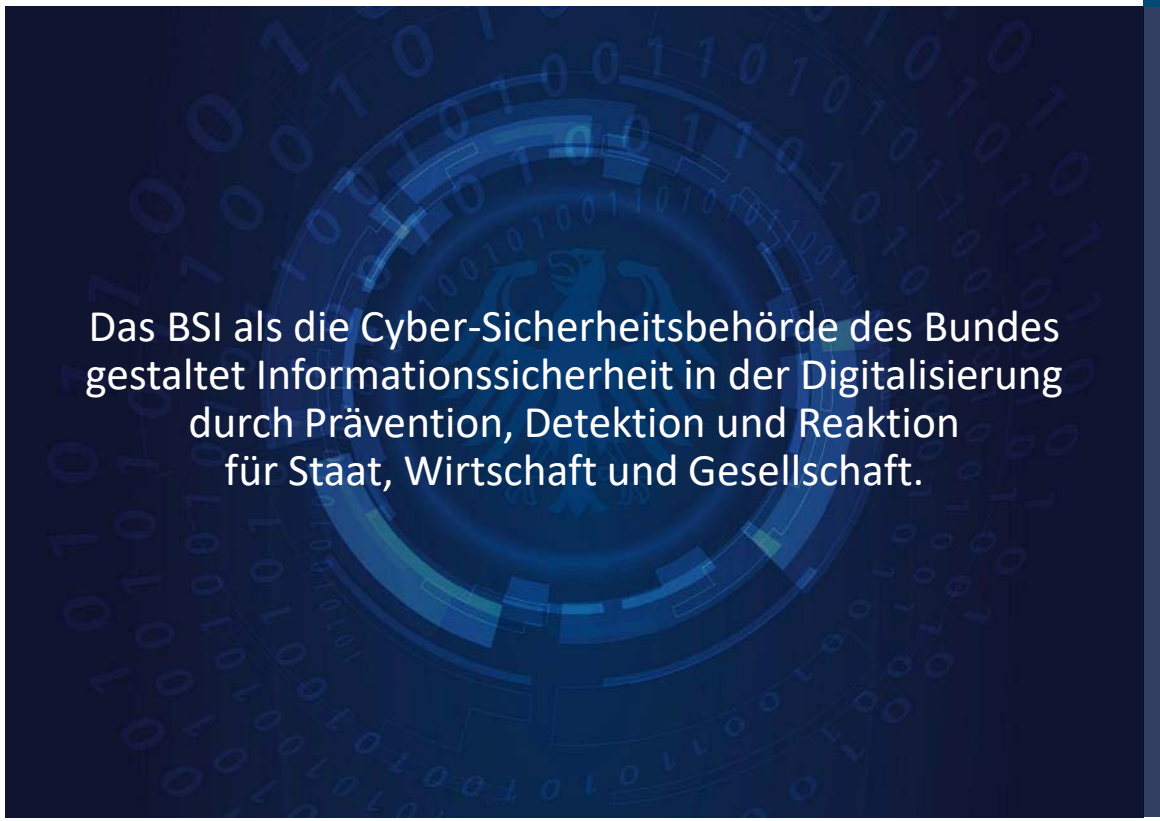
Deutschland
Digital•Sicher•BSI•

Kontakt

Christian Kleinmanns
Referat DI 24 - Cyber-Sicherheit im Gesundheits- und Finanzwesen
Tel.: +49 228 99 9582-6872
Mail: christian.kleinmanns@bsi.bund.de

Pascal Jeschke
Referat DI 24 - Cyber-Sicherheit im Gesundheits- und Finanzwesen
Tel.: +49 228 99 9582-4160
Mail: pascal.jeschke@bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de



Bundesamt
für Sicherheit in der
Informationstechnik