Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Sichere KI-Anwendungen für Deutschland

Arne Schönbohm
Präsident
Bundesamt für Sicherheit in der Informationstechnik

Innovationssymposium Künstliche Intelligenz
Berlin, 29.06.2021

Digitalisierung

Sichtbare Chancen, unsichtbare Bedrohungen

Anwendungsbeispiele für KI:

- Industrie 4.0
- Mobilität und Logistik
- Medizin
- Smart Cities
- Smart Homes

Bundesamt für Sicherheit in der Informationstechnik

Künstliche Intelligenz

Wissenschaftliche Disziplin und Technologie

Inferenzsysteme

überwachtes/unüberwachtes/verstärkendes
Maschinelles Lernen

Tiefe Neuronale Netze

Expertensysteme

Logisches Schließen

Wissensrepräsentation

Bayessche Netze

Statistische Methoden

Deduktionssysteme

Hybride Systeme

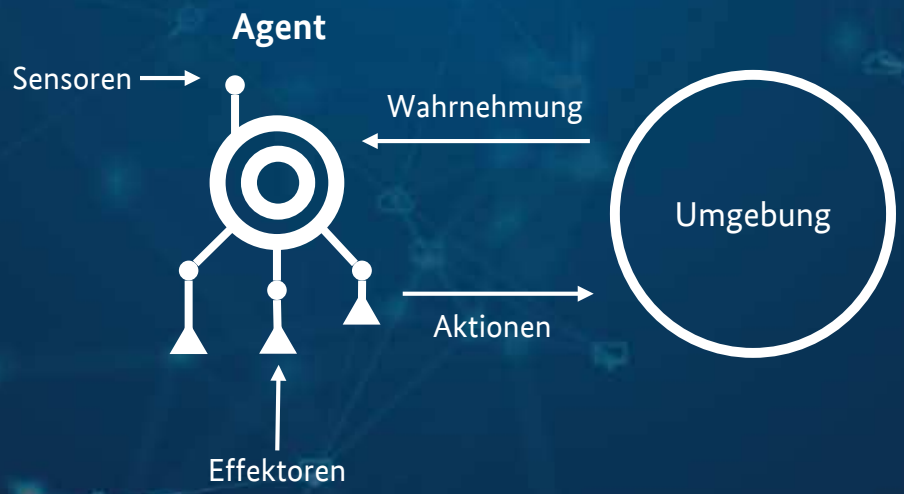
Suchen und Optimieren

Bundesamt
für Sicherheit in der
Informationstechnik

Eine Definition für KI-Systeme

KI-Systeme sind Software- und Hardwaresysteme, die Künstliche Intelligenz nutzen, um in der physischen oder digitalen Welt "rational" zu handeln. Auf Grundlage von Wahrnehmung und Analyse ihrer Umgebung agieren sie mit einem gewissen Grad an Autonomie, um bestimmte Ziele zu erreichen.

- ***BSI***



Bundesamt für Sicherheit in der Informationstechnik

Künstliche Intelligenz beim BSI

IT-Sicherheit für KI

Wir untersuchen neuartige Bedrohungen für KI-Systeme und entwickeln geeignete Gegenmaßnahmen

Angriffe durch KI

Wir verfolgen neue KI-gesteuerte und KI-unterstützte Angriffsmethoden gegen IT-Systeme und Infrastrukturen und entwickeln geeignete Gegenmaßnahmen

IT-Sicherheit durch KI

Wir ermöglichen die Nutzung von KI-Methoden zur Verbesserung der IT-Sicherheit, z. B. zur Prävention, Detektion und Reaktion bei Cyber-Angriffen

KI und digitaler Verbraucherschutz

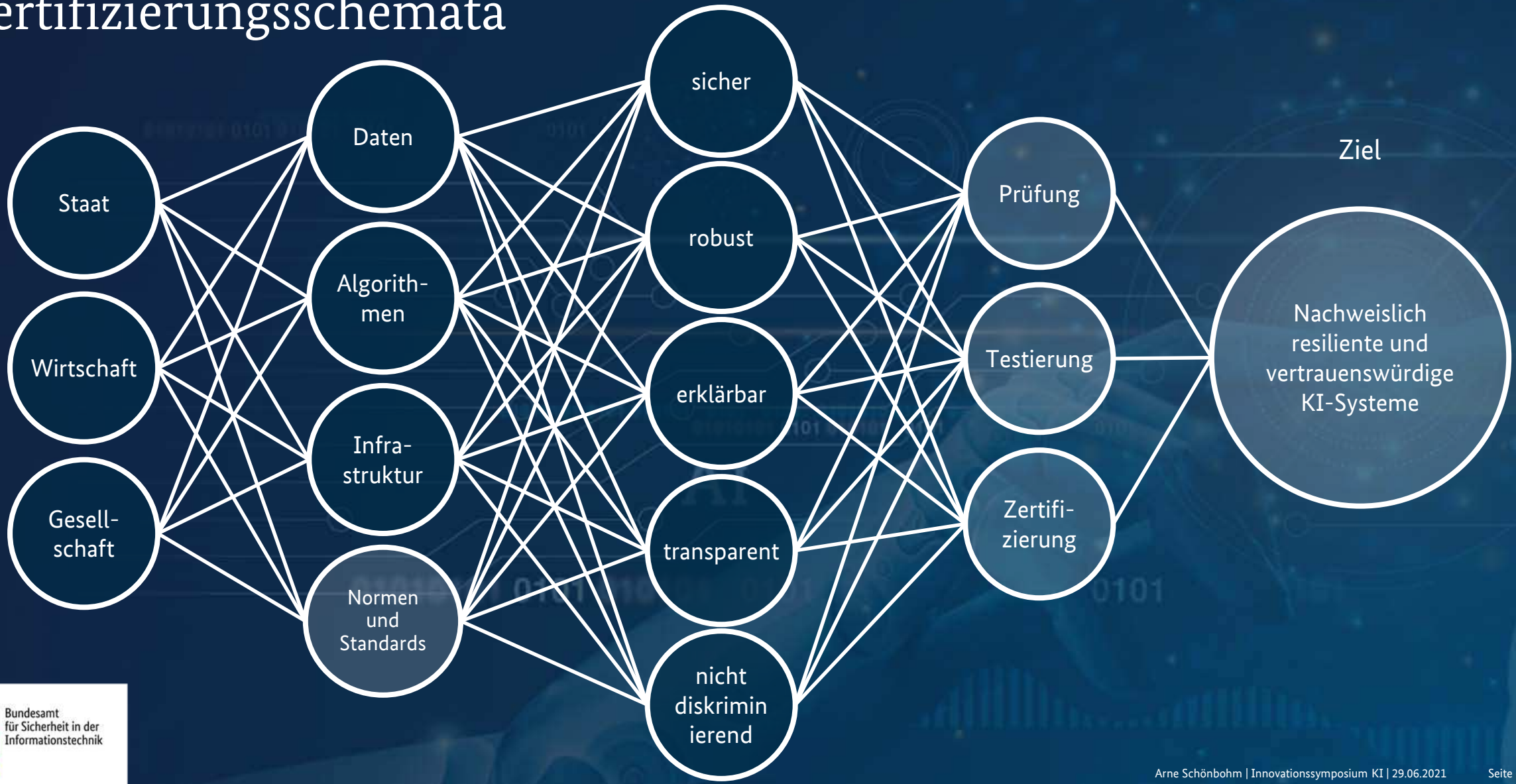
Wir fördern den sicheren und transparenten Einsatz von KI-Methoden in Verbraucherprodukten und steigern die Beurteilungsfähigkeit der Verbraucherinnen und Verbraucher für KI-basierte Systeme

Normen und Standards für KI

Wir entwickeln und bewerten Prüfkriterien, Prüfmethoden und Prüfwerkzeuge für nachweisbar sichere und vertrauenswürdige KI-Systeme mit dem Ziel, Normen und Standards für diese Systeme zu entwickeln

Bundesamt für Sicherheit in der Informationstechnik

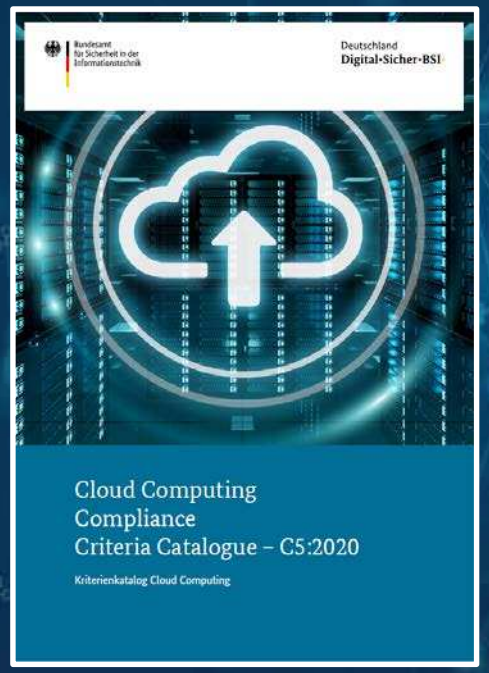
Von Technischen Richtlinien über Normen und Standards zu Zertifizierungsschemata



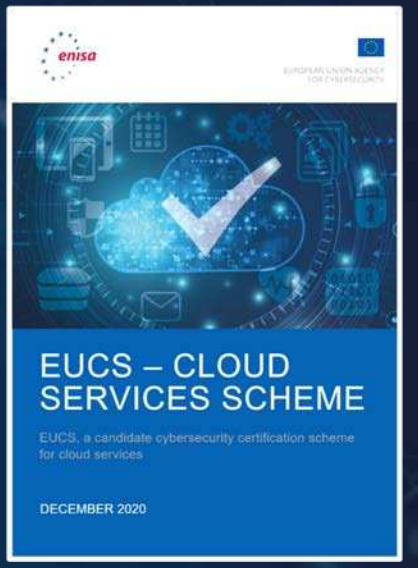
Bundesamt
für Sicherheit in der
Informationstechnik

Cloud Computing Compliance Criteria Catalogue C5:2020

- Vorgaben zum Audit nach ISAE
- Rahmenbedingungen zur Schaffung von Transparenz
- 121 Sicherheitskriterien, gegliedert in 17 Bereiche, holistische Betrachtung der Informationssicherheit



Basis für Level „Substantial“ Audit-Anforderungen



Sicherheitsnachweise

gaia-x

Bundesamt für Sicherheit in der Informationstechnik

AI Cloud Service Compliance Criteria Catalogue (AIC4)

- Erweiterung von C5
- 47 Sicherheitskriterien, gegliedert in 7 Bereiche
- Kombination der beiden Audits ermöglicht eine umfassende Bewertung von KI-Diensten in einer Cloud

Bundesamt
für Sicherheit in der
Informationstechnik

KI in den Nationalen Koordinierungszentren – Europa

- **Europäisches Kompetenzzentrum (ECCC)**
  mit Sitz in Bukarest
- **Nationale Koordinierungs-zentren** in allen EU-Mitgliedstaaten

NKCS in allen EU-Mitgliedstaaten

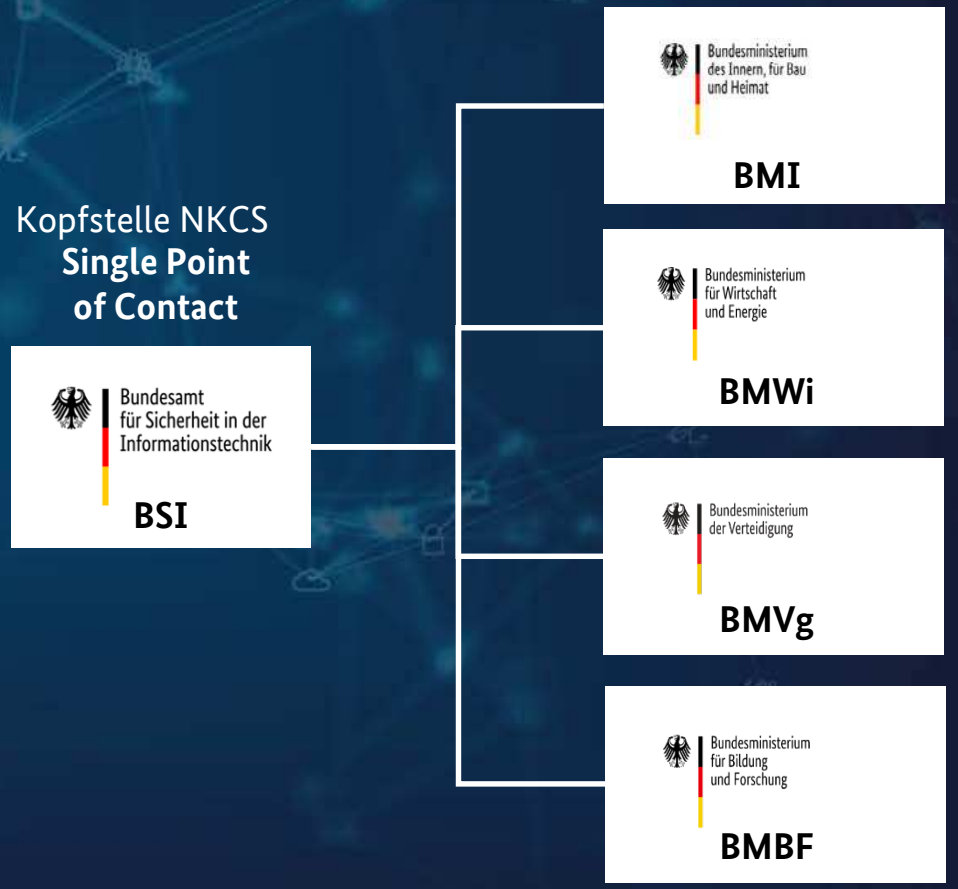
- **EU-Förderprogramm „Digital Europe“ (2021-2027)**
  - **EU-Fördermittel** in Höhe von **über 2 Mrd. EUR** für die Themen KI, Cloud und Dateninfrastruktur
  - **KI Test- und Experimentiereinrichtungen**
    Ziel: Vertrauenswürdige KI
  - **KI On Demand Plattform**
    Ziel: EU KI-Infrastruktur für Entwickler*innen, Integrator*innen und Anwender*innen

Bundesamt für Sicherheit in der Informationstechnik

KI in den Nationalen Koordinierungszentren (NKCS) – Deutschland

- **Nationales Koordinierungszentrum Cybersicherheit**
  - **Koordination der Cybersicherheitsforschung** in **Deutschland, Europa und internationa**l
  - **KI** elementarer Bestandteil der **EU-Förderprogramme** („Digital Europe“ und „Horizon Europe“)
  - Mitgestaltung der Digitalisierung in Deutschland und Europa

NKCS-Aufbau



Bundesamt für Sicherheit in der Informationstechnik

Gemeinsam Informationssicherheit stärken

Regional, National, International

Bundesamt für Sicherheit in der Informationstechnik

Das BSI als die Cyber-Sicherheitsbehörde des Bundes gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft

Vielen Dank
für Ihre Aufmerksamkeit!

Kontakt

Arne Schönbohm
Präsident

[redacted]@bsi.bund.de
Tel. +49 (0) 228 9582[redacted]
Fax +49 (0) 228 10 9582 5[redacted]

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

Bundesamt
für Sicherheit in der
Informationstechnik