IT-Planungsrat

Digitale Zukunft gestalten

SACHSEN-ANHALT

#moderndenken

Verwaltung digital

Mensch macht´s!

11. Fachkongress des IT-Planungsrats

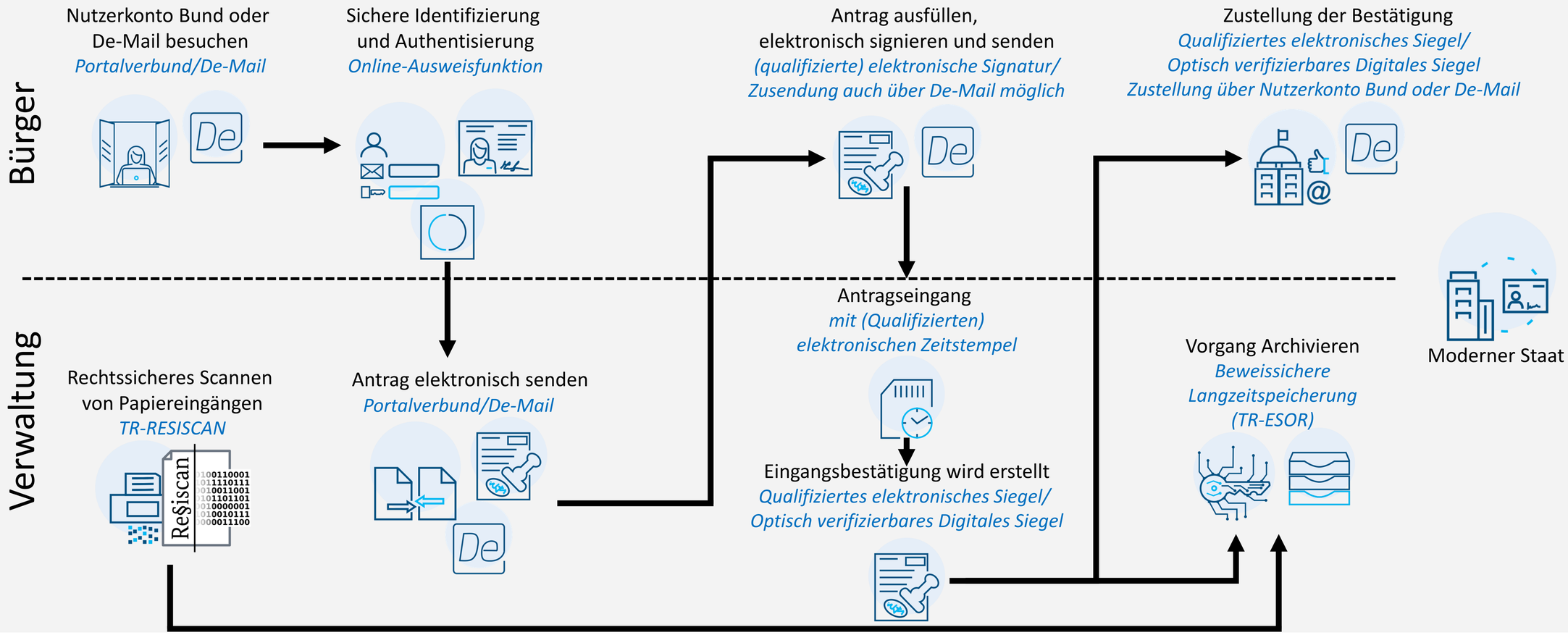
MaSiGov

Markt- und Schwachstellenanalyse zur Sicherheit von E-Government Apps und Webportalen

Sicherheit im Portalverbund

Dr. Thorsten Limböck (BSI)

Referat DI 15
eID-Lösungen für die digitale Verwaltung



Markt- und Schwachstellenanalyse zur Sicherheit von E-Government Apps und Webportalen (MaSiGov)

Hintergrund

- Bund und Länder sind durch das OZG verpflichtet, bis Ende 2022 ihre Verwaltungsleistungen auch ***elektronisch über Verwaltungsportale*** anzubieten (§ 1 Abs. 1 OZG).
- Allerdings enthält das OZG keine näheren Vorgaben im Hinblick auf die Art der ***technischen Umsetzung***.

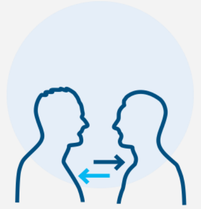
- Bund, Länder und Kommunen haben Umsetzungen oftmals selbstständig entwickelt und ***unterschiedliche Lösungen*** implementiert.
- Ziel des Projekts war es, einen Überblick über die ***Umsetzungslandschaft*** und ihre ***Sicherheit*** zu erhalten um gezielte und sinnvolle ***Unterstützung*** zu leisten.

- Die Betreiber und Entwickler der untersuchten Produkte sollten auf jedem Schritt ***mitgenommen*** werden.

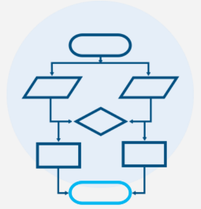
Markt- und Schwachstellenanalyse zur Sicherheit von E-Government Apps und Webportalen (MaSiGov)

Aufbau

- ***Projektlaufzeit:*** Januar 2022 bis Januar 2023
- In einem ersten Schritt wurde die ***Umsetzungslandschaft*** betrachtet (Webportale und Apps für mobile Geräte).
- Auf Basis der Ergebnisse wurden ***Produkte*** ausgewählt und für diese ein ***Katalog mit möglichen Angriffen*** erstellt.



- Im nächsten Schritt wurden Hersteller und Betreiber der ausgewählten Produkte zu einer ***Teilnahme eingeladen***.
- Die Schwachstellenanalyse wurde in ***engem Austausch*** mit den Produktverantwortlichen durchgeführt. (Festlegung des Scopes und Ergebnisbesprechung)

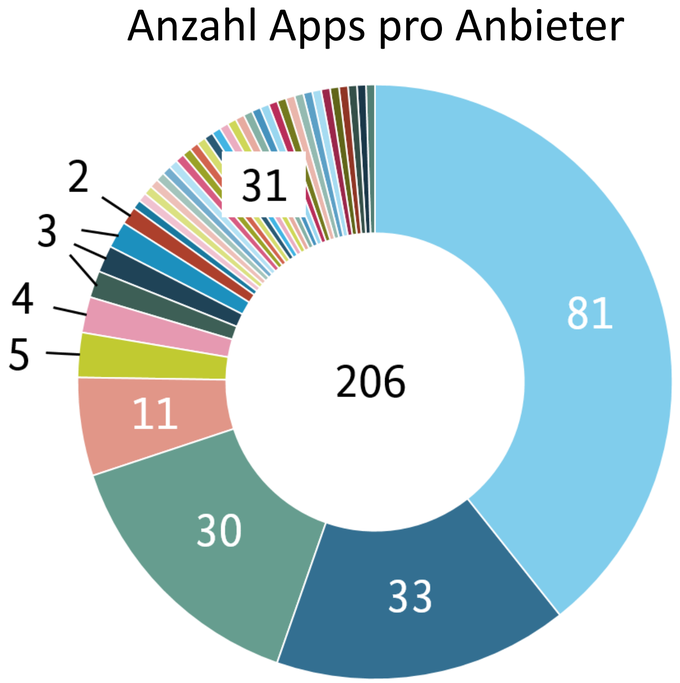


- Übergreifende Erkenntnisse bieten ***Einblick***, wo Unterstützung ***sinnvoll*** ist.

Marktanalyse Apps

Ergebnisse

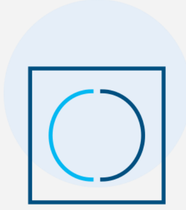
- Insgesamt wurden ***206 Apps*** für mobile Geräte berücksichtigt.
- Apps für mobile Endgeräte lassen sich in verschiedene ***Kategorien*** unterscheiden.
- Eine weitere Kategorie war die ***technische Umsetzung.***
- Bestimmte Funktionen waren überwiegend nativ im ***Programmcode*** der App hinterlegt, andere Funktionen wurden bevorzugt über einen ***integrierten Browser*** ermöglicht.
- Eine letzte Kategorie stellt die ***(Nach-)Nutzung*** der App dar.
- 84 % der Apps basierten auf ***White-Label-Lösungen,***
- 16 % der Apps hatten ***individuelle Anbieter.***
- Nicht abgebildet sind Apps mit ***Viel-Ämter-Lösungen.***



Marktanalyse Apps

Ergebnisse

- Bei 80 % der Apps lag der Schwerpunkt in der ***Aufgabe*** vornehmlich der ***Informationsprovision***. Dies Umfasste vornehmlich aktuelle Informationen, Bekanntmachungen, Veranstaltungskalender, Points of Interest, Abfallkalender, ÖPNV.
- Eine ***Nutzereingabe*** (Kommunikation Richtung Verwaltung) war nachrangig (Kontaktformular, Terminbuchung, Mängelmelder).
- In vereinzelten Fällen war ein Zugriff ***OZG-Leistungen*** möglich, hierbei handelte es sich um browserbasierten Zugriff auf das Webportal.
- Für die Schwachstellenanalyse im Rahmen des Projekts konnte ***keine geeignete App*** identifiziert werden.
- Allerdings: Die App-Landschaft ***wächst*** an Umfang und Inhalten.



Marktanalyse Webportale

Ergebnisse

- Webportale sind stark ***unterschiedlich***, individuell und ***komplex*** in Umfang, Komponenten und Stakeholdern.
- ***Mehrstufiges*** Vorgehen: Recherche, Fragebogen
- ***Kriterien*** waren umfangreiche Funktionalitäten auf OZG-Antragsstrecken und ***Interesse*** an Teilnahme.
- Es wurden ***fünf*** Portale ausgewählt:
  - Zwei Serviceportale von ***Ländern***
  - Zwei Portale von ***Kommunen***
  - Ein ***Kommunalportal*** eines ***Landes***

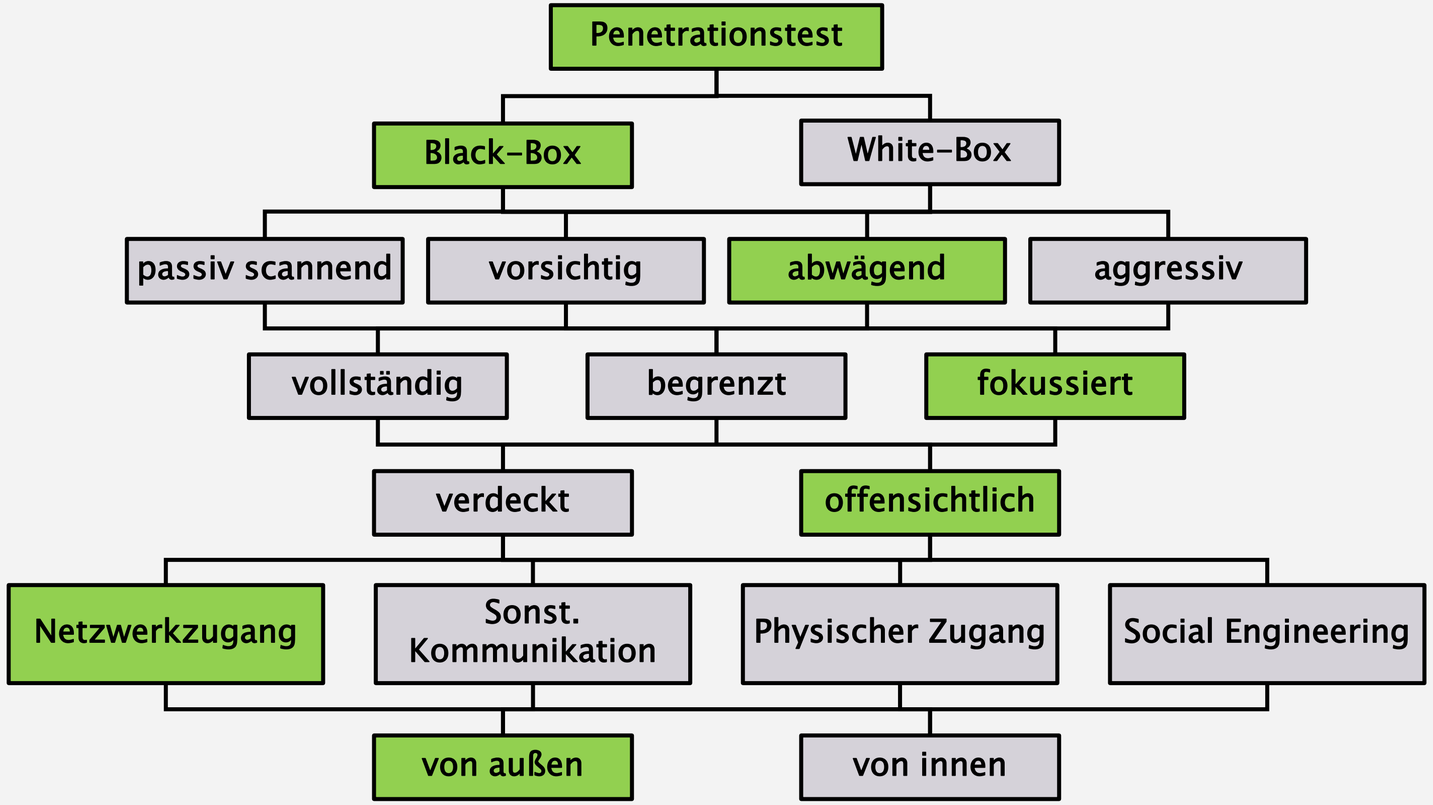
Schwachstellenanalyse Webportale

Durchführungskonzept

- Für die Schwachstellenanalyse wurde ein ***Angriffskatalog*** auf Basis ***etablierter Standards*** (OWASP Testing Guide, ASVS) erstellt.
- Für jedes Produkt wurde ein ***individueller Durchführungskatalog*** erstellt, welcher Eigenschaften und Funktionen berücksichtigt.
- Die Schwachstellenanalyse bestand aus zwei Teilen: ***Systemebene*** und ***Anwendungsebene***
- Die Durchführung wurde auf Basis gängiger und bewährter ***Konzepte*** gewählt.

Schwachstellenanalyse Webportale

1. Informationsbasis
2. Aggressivität
3. Umfang
4. Vorgehensweise
5. Zugang
6. Ausgangspunkt



„Studie: Durchführungskonzept für Penetrationstests“, BSI

Analyseergebnisse

Systemebene

- Grundsätzlich ist zu unterscheiden zwischen ***Schwachstelle*** (direkte Angreifbarkeit) und ***Hinweis*** (begünstigender Faktor).
- Auf der ***Systemebene*** wurden bei allen getesteten Portalen Schwachstellen od. Hinweise im Kontext mit ***Transportverschlüsselung*** identifiziert.
- Schwachstelle, bei der der Web-Server mit geringem Aufwand des Angreifers viel ***Rechenleistung*** erzeugt wird (***D(He)ater-Angriff***) (4/5)
- Denial-of-Service durch Secure Client-Initiated Renegotiation (Neuaushandeln der TLS-Parameter) möglich (1/5)
- Hinweise umfassen Verwendung von nicht-empfohlenen ***TLS-Konfigurationen*** (4/5) und ***Auffälligkeiten*** in den Konfigurationen der verwendeten TLS-Zertifikate (3/5)

Analyseergebnisse

Anwendungsebene

- Einsatz älterer ***Skript-Bibliotheken*** mit bekannten Schwachstellen (3/5)
- Verwundbare ***Uploadfunktionen***, welche eine Vielzahl an möglichen Angriffen zulassen (Schadcode, Dateitypen, -größen, Anzahl) (4/5)
- Verwundbarkeit bei ***Zwischenspeicherung*** von Anträgen (1/5)
- Unsichere Weiterleitung, welche einen ***Phishing-Angriff*** erlaubt (1/5)
- Schwachstellen im Umgang mit ***sensiblen Informationen*** (Rechtschreibprüfung, Autovervollständigung) (3/5)
- Schwachstelle im Umgang mit ***Cookies*** (1/5)
- Hinweise umfassen ***Session Handling***, ***HTTP-Security Header*** und ***HTTP-Methoden***

Fazit

Erkenntnisse

- Die Portallandschaft ist ***aktiv, vielfältig und komplex***.
- Einige der gefundenen Schwachstellen waren über ***alle*** Portale hinweg vergleichbar. Sie basieren auf ***gleichen Funktionalitäten***.
- Zentrale Funktionen sind ***Eingabefelder*** und ***Dateiupload.***
- Schwerpunkte für ***Unterstützungen*** sind identifiziert.
- Die Erkenntnisse werden berücksichtigt und fließen u.a. in eine ***Technische Richtlinie*** zum ***Portalverbund*** ein.
- Bei ***keinem Portal*** wurden Schwachstellen mit ***kritischem*** oder ***hohem*** Risikograd gefunden.
- Allerdings: Es wurden nur Portale untersucht, die einer Teilnahme ***zugestimmt*** hatten. Sämtliche teilnehmenden Portale hatten ***Erfahrung*** mit Schwachstellenanalysen. Das Ergebnis ist nicht repräsentativ.

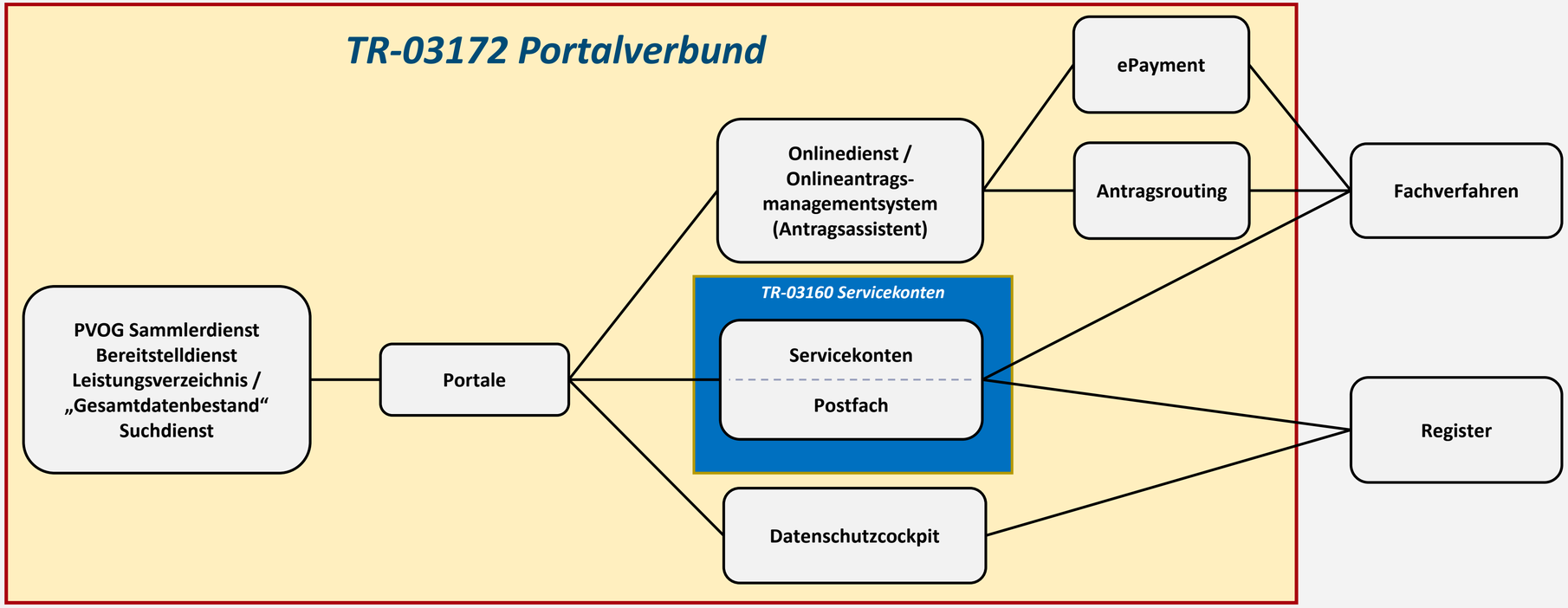
Technische Richtlinie Portalverbund

BSI TR-03172 Portalverbund

- Ziel ist es, die Umsetzenden dabei zu ***unterstützen***, einen ***sicheren*** Portalverbund zu gestalten.
- ***Bestehende*** Lösungen werden ebenso berücksichtigt, wie künftige.
- Die Empfehlungen sind an die ***unterschiedlichen Komponenten*** angepasst.
- Ein ***modularer Aufbau*** bietet die Struktur, gesuchte Informationen jederzeit ***schnell*** zu finden.
- ***Bestehende*** Technische Richtlinien werden berücksichtigt.
- Die TR Portalverbund ***wächst*** und verändert sich ***mit*** dem Portalverbund selbst.

Technische Richtlinie Portalverbund

Der Portalverbund



Vielen Dank für Ihre Aufmerksamkeit!

Kontakt

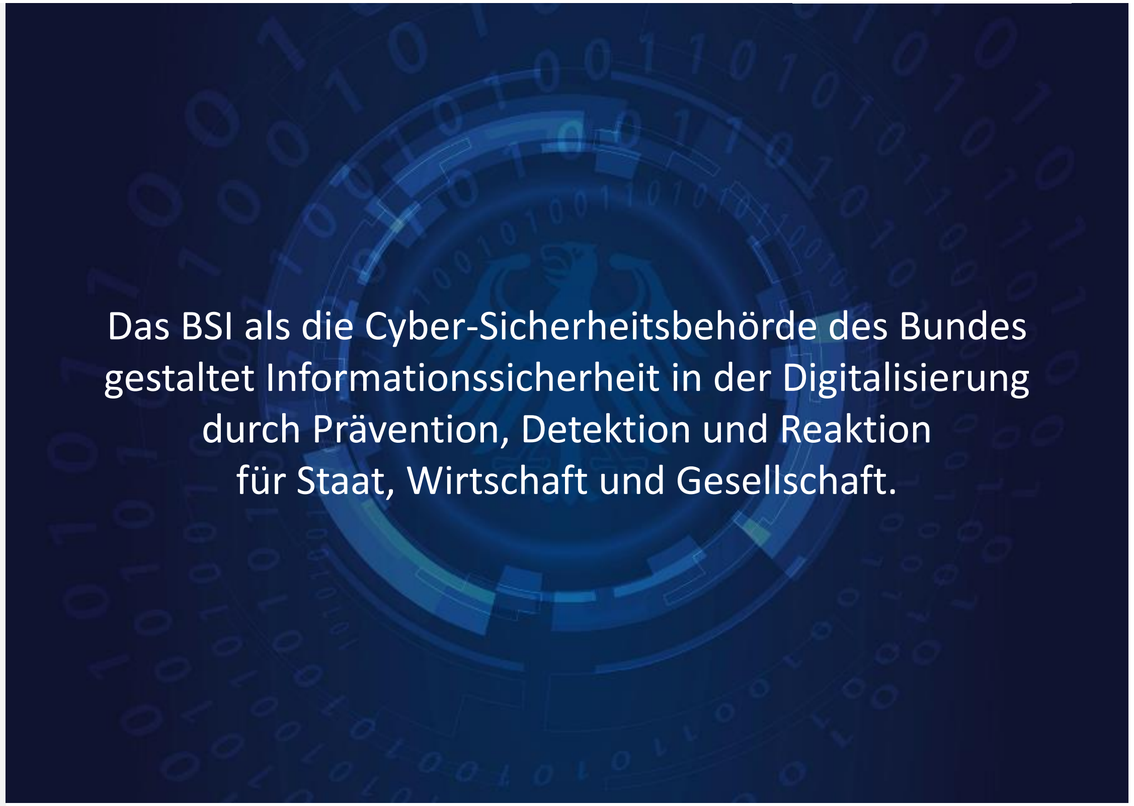
Dr. Thorsten Limböck
E-Mail: thorsten.limboeck@bsi.bund.de

Referat DI 15 – eID-Lösungen für die digitale Verwaltung
E-Mail: referat-di15@bsi.bund.de

Projekt MaSiGov
E-Mail: MaSiGov@bsi.bund.de

BSI TR-03172 Portalverbund
E-Mail: Portalverbund@bsi.bund.de

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



Link zum Abschlussbericht:

https://bsi.bund.de/dok/MaSiGov

Vielen Dank!

Fragen?