KRITIS – Was ist das?

Azure Ruhrgebiet Meetup

Manuel Atug

Leistungsportfolio im Security Consulting

Penetrationstests/
Technische Audits

Cyber-Response/
Forensik

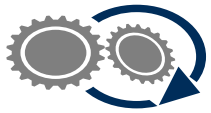
ISMS
ISO

ISMS
Grundschutz

Datenschutz

Auditierung/
Zertifizierung

Sensibilisierung
und Schulung



Business
Continuity

Crisis
Management

IT- Notfall-
management

Konzepte/
Risikoanalysen

Notfall- und
Krisenübungen

Outsourcing/
Auslagerungsmgmt.

Cloud
Security

Wirtschafts-
grundschutz

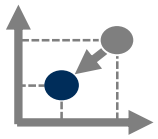
Corporate
Security

Sicherheits-
strategie

Industrial
Security

Medical
Security

Kritische
Infrastrukturen



Risk Management

Über mich

Manuel Atug

- Head of Business Development der HiSolutions AG
- Diplom-Informatiker, Master of Science in Applied IT Security, Ingenieur
- > 23 Jahren in der Informationssicherheit tätig
- langjährige Erfahrung im Bereich technische IT-Sicherheit und Auditierungen
- Themen: KRITIS, Hackback, Ethik, Bevölkerungsschutz
- prägender Berater des BSI für § 8a BSIG

Was ist KRITIS?

Die 10 Kritische Infrastrukturen Sektoren in Deutschland

Quelle https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/Sektoren-Branchen/sektoren-branchen_node.html

§ 2 (10) BSI-Gesetz

Begriffsbestimmungen

Kritische Infrastrukturen im Sinne dieses Gesetzes sind **Einrichtungen, Anlagen oder Teile davon**, die

1. den **Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen** angehören und
2. von **hoher Bedeutung für das Funktionieren des Gemeinwesens** sind, weil durch ihren Ausfall oder ihre Beeinträchtigung **erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit** eintreten würden.

Die **Kritischen Infrastrukturen im Sinne dieses Gesetzes werden durch die Rechtsverordnung** nach § 10 Absatz 1 näher **bestimmt**.

Wann falle ich da drunter?

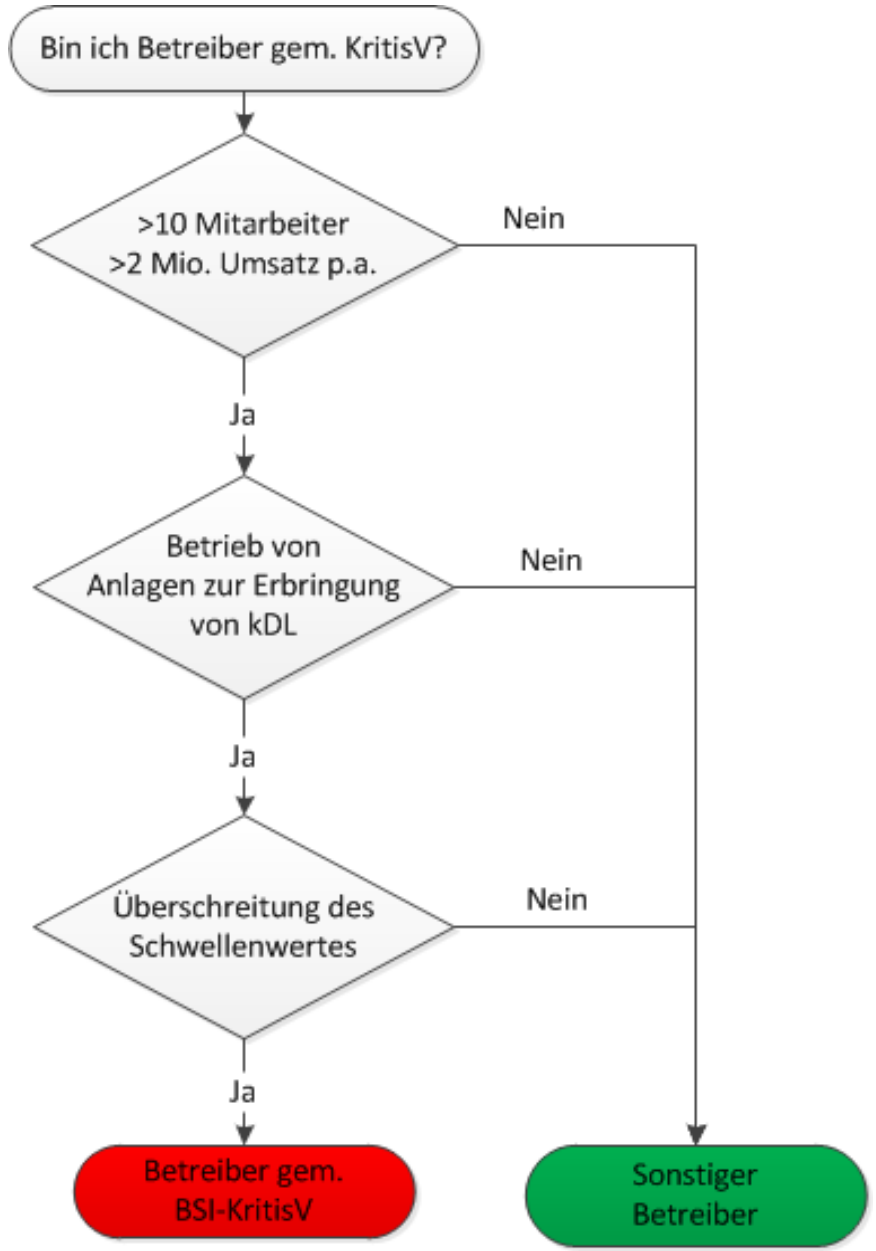
Vorgehensweise zur Bestimmung von kritischen Dienstleitungen

Bin ich Betreiber gemäß BSI-KritisV?

- Habe ich mehr als 10 Mitarbeiter oder mehr als 2 Mio. EUR Jahresumsatz
  (kein Kleinstunternehmen gemäß § 8d (1) BSIG)?

- Betreibe ich Anlagen zur Erbringung einer kDL?

- Liegt der Versorgungsgrad dieser Anlagen über dem jeweiligen Schwellenwert?



Auszug aus der BSI-KritisV

(Beispiel: Sektor Wasser)

Teil 1 - Grundsätze und Fristen

1. Für die in Teil 3 Spalte B Nummer 1 genannten Anlagenkategorien gelten vorrangig die Begriffsbestimmungen nach den technischen Regeln der Deutschen Vereinigung für Wasserwirtschaft, Abwasser und Abfall e. V. (DIN EN 16323) in der jeweils geltenden Fassung. Für die in Teil 3 Spalte B Nummer 2 genannten Anlagenkategorien gelten vorrangig die Begriffsbestimmungen nach den technischen Regeln der Deutschen Vereinigung des Gas- und Wasserfachs e. V. (DIN 4046) in der jeweils geltenden Fassung. (…)

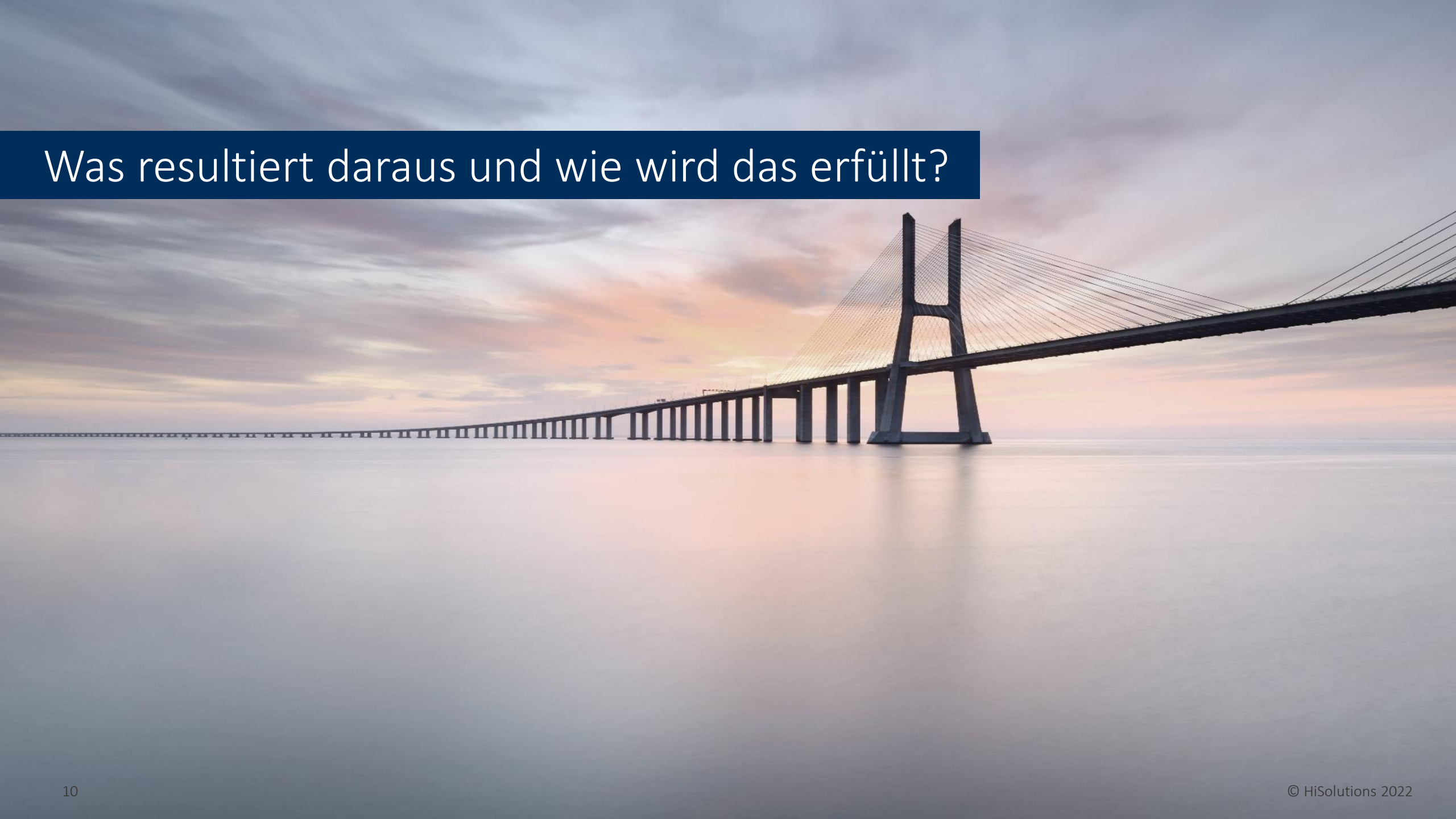
Teil 3 - Anlagenkategorien und Schwellenwerte

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Anlagenkategorie	Bemessungskriterium	Schwellenwert
1.	**Abwasserbeseitigung**		
1.1	Siedlungsentwässerung		
1.1.1	Kanalisation	Angeschlossene Einwohner	500 000
1.2	Abwasserbehandlung und Gewässereinleitung		
1.2.1	Kläranlage	Ausbaugröße in Einwohnerwerten	500 000

Teil 2 - Berechnungsformeln zur Ermittlung der Schwellenwerte

7. Der für die Anlagenkategorien des Teils 3 Nummer 2.1.1 bis 2.4.1 genannte Schwellenwert ist unter Annahme eines Durchschnittsverbrauchs von 44 m3 pro versorgter Person pro Jahr und eines Regelschwellenwertes von 500 000 versorgten Personen wie folgt berechnet: 22 Millionen m3/Jahr = 44 m3/Jahr × 500 000

Was resultiert daraus und wie wird das erfüllt?



§ 8a (1) BSI-Gesetz

Sicherheit in der Informationstechnik Kritischer Infrastrukturen

Betreiber Kritischer Infrastrukturen sind verpflichtet, **spätestens zwei Jahre nach Inkrafttreten** der Rechtsverordnung nach § 10 Absatz 1 **angemessene organisatorische und technische Vorkehrungen** zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei soll der **Stand der Technik** eingehalten werden. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.

§ 8a (3) BSI-Gesetz

Sicherheit in der Informationstechnik Kritischer Infrastrukturen

Die **Betreiber Kritischer Infrastrukturen** haben mindestens **alle zwei Jahre die Erfüllung der Anforderungen** nach Absatz 1 auf **geeignete Weise nachzuweisen**.

Der Nachweis kann durch **Sicherheitsaudits, Prüfungen oder Zertifizierungen** erfolgen.

Die **Betreiber übermitteln dem Bundesamt die Ergebnisse** der durchgeführten Audits, Prüfungen oder Zertifizierungen **einschließlich** der dabei **aufgedeckten Sicherheitsmängel**. Das Bundesamt kann die Vorlage der Dokumentation, die der Überprüfung zugrunde gelegt wurde, verlangen. Es kann bei Sicherheitsmängeln im **Einvernehmen** mit der zuständigen Aufsichtsbehörde des Bundes oder im **Benehmen** mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel verlangen.

Quellen zur Entwicklung einer Prüfgrundlage

Integration von / Verweis auf bestehende Standards

Bestehende Branchenstandards, ISO 27001, BSI-IT-Grundschutzkompendium, Publikationen der Branchenverbände etc. können als Bestandteile verwendet werden.

Orientierungshilfe B3S

Eine Anlehnung an die Orientierungshilfe B3S und deren Struktur ist hilfreich, da sie die Mindestqualität an eine Umsetzung von § 8a (1) BSIG zusammenfasst.

Die Orientierungshilfe enthält keine harten Anforderungen, qualitativ gleichwertige Alternativen sind möglich.

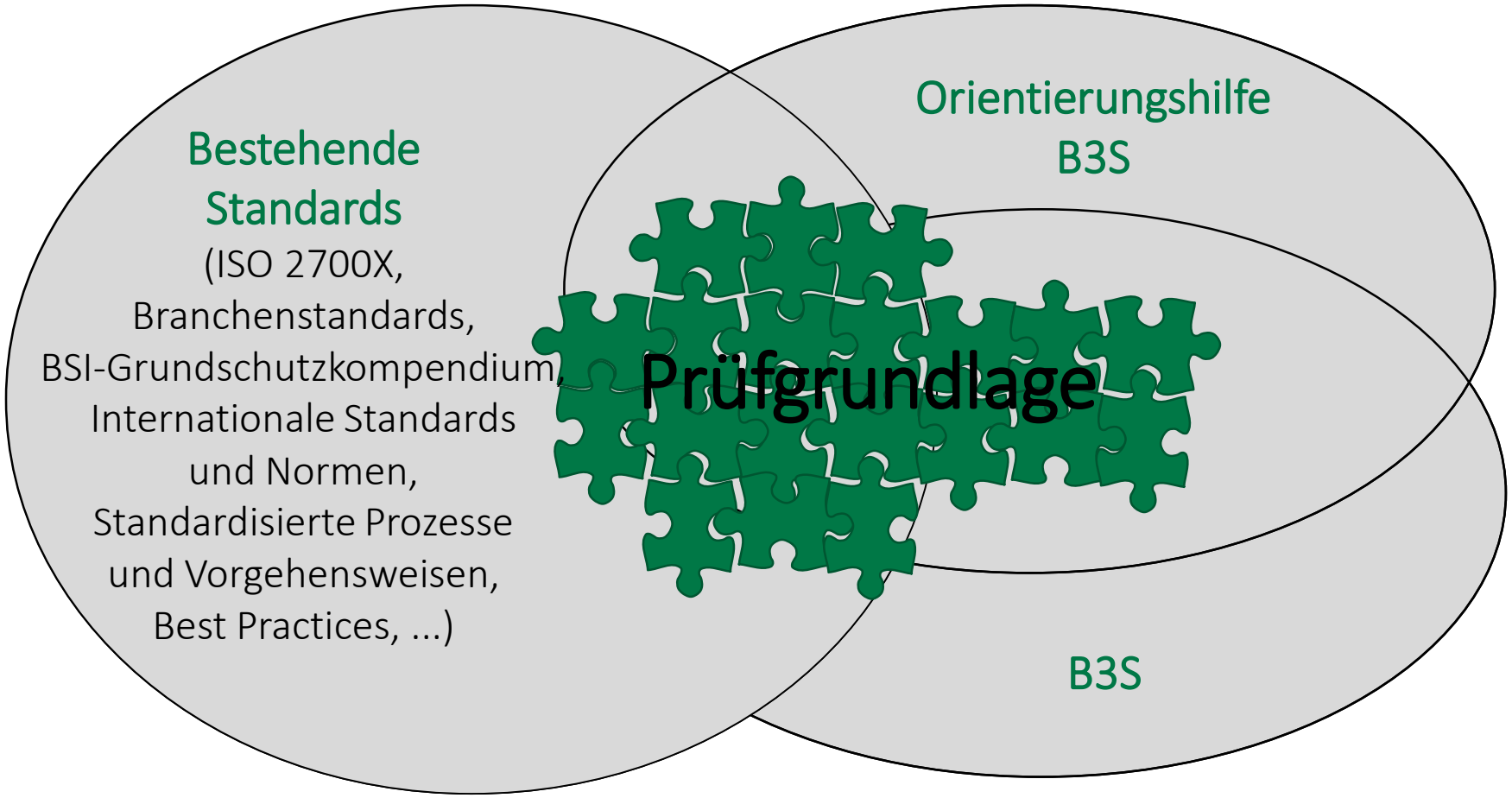
B3S

Eine Anlehnung an einen B3S ist ebenfalls hilfreich, da er branchentypische Sicherheitsaspekte zur Umsetzung von § 8a (1) BSIG zusammenfasst.

Branchenspezifische Sicherheitsstandards (B3S)

- Branchen können **branchenspezifische Sicherheitsstandards (B3S)** erstellen, um den „Stand der Technik“ in ihrer Branche zu konkretisieren.
- Das BSI hat eine **Orientierungshilfe (OH)** mit Inhalten und Anforderungen an B3S herausgegeben.
- Die Erarbeitung der B3S erfolgt im Allgemeinen in **Branchenarbeitskreisen** des UP KRITIS.
- B3S können als **Grundlage** für **Prüfungen und Audits** verwendet werden.

Quellen zur Entwicklung einer Prüfgrundlage



Nachweiserbringung

Allgemeines zur Nachweisführung

Nachweisintervall

Alle 2 Jahre

Nachweismöglichkeiten

Audits, Prüfungen oder Zertifizierungen

Besonderheiten

- Übersendung der Liste der bereits bekannten und in der Prüfung festgestellten Sicherheitsmängel an das BSI.
- Das BSI kann die Vorlage der Dokumentation, die der Überprüfung zugrunde gelegt wurde, verlangen.
- BSI kann im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel verlangen.

Nachweis- und Bewertungsprozess

Prüfung der Anlage alle 2 Jahre

Betreiber übersendet dem BSI die Nachweise (Formulare mit Anlagen)

Auswertung des Nachweisdokumentes und ggf. Anforderung des vollständigen Prüfberichts/Unterlagen durch das BSI.

Nach Sichtung des Prüfberichtes kann das BSI nach Abstimmung mit der Aufsichtsbehörden die Beseitigung der Mängel fordern.

Schloßstraße 1 | 12163 Berlin

info@hisolutions.com | +49 30 533 289 0

www.hisolutions.com