Internet Security Days 2018

# §8a,b BSIG und BSI- Kritisverordnung für Betreiber Kritischer Infrastruktur

Manuel Atug, Senior Manager

HISOLUTIONS

# Über mich

**Manuel Atug**,

- Senior Manager der HiSolutions AG
- seit über 20 Jahren in der Informationssicherheit tätig
- langjährige Erfahrung im Bereich technische IT-Sicherheit und Auditierungen
- berät und begleitet Unternehmen bei der Einführung von ISMS
- Spezialthemen: KRITIS, Kryptographie und Verschlüsselung, Schutzbedarfsfeststellungen und Risikoanalysen
- Diplom-Informatiker, TH Köln
- Master of Science in Applied IT Security, Ruhr-Universität Bochum

# Leistungsportfolio im Security Consulting

Penetrationstests/
Technische Audits

Cyber-Response/
Forensik


ISMS
ISO


ISMS
Grundschutz

Datenschutz

Auditierung/
Zertifizierung

Business
Continuity

Crisis
Management

IT- Notfall-
management

Konzepte/
Risikoanalysen

Notfall- und
Krisenübungen

Outsourcing/
Auslagerungsmgmt.

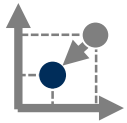
Wirtschafts-
grundschutz

Corporate
Security

Sicherheits-
strategie

Industrial
Security

Kritische
Infrastrukturen



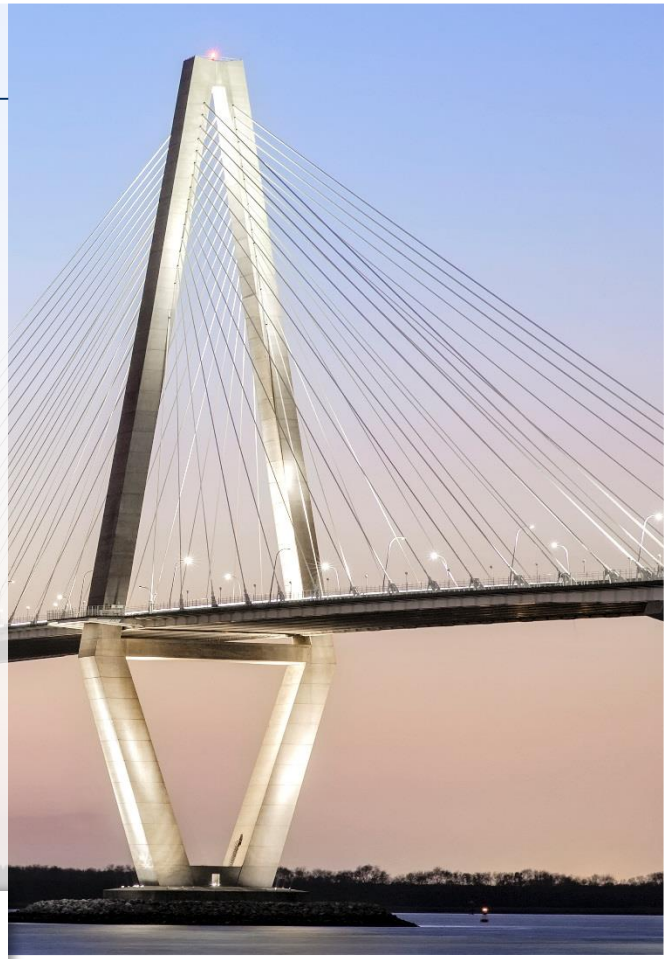
Risk Management



HISOLUTIONS

# AGENDA

1 Motivation
2 Was sind kritische Infrastrukturen
3 Rechtliche Grundlagen für KRITIS-Betreiber
4 Kritis - Sektoren und Fristen
5 Ermittlung des Geltungsbereichs
6 Meldung potenzieller Vorfälle
7 Stand der Technik
8 Prüfung gemäß § 8a BSIG
9 Weitere Zulassungsmöglichkeiten





HISOLUTIONS

# MOTIVATION

*Je besser etwas funktioniert, desto gravierender sind die Folgen, wenn etwas ausfällt.*



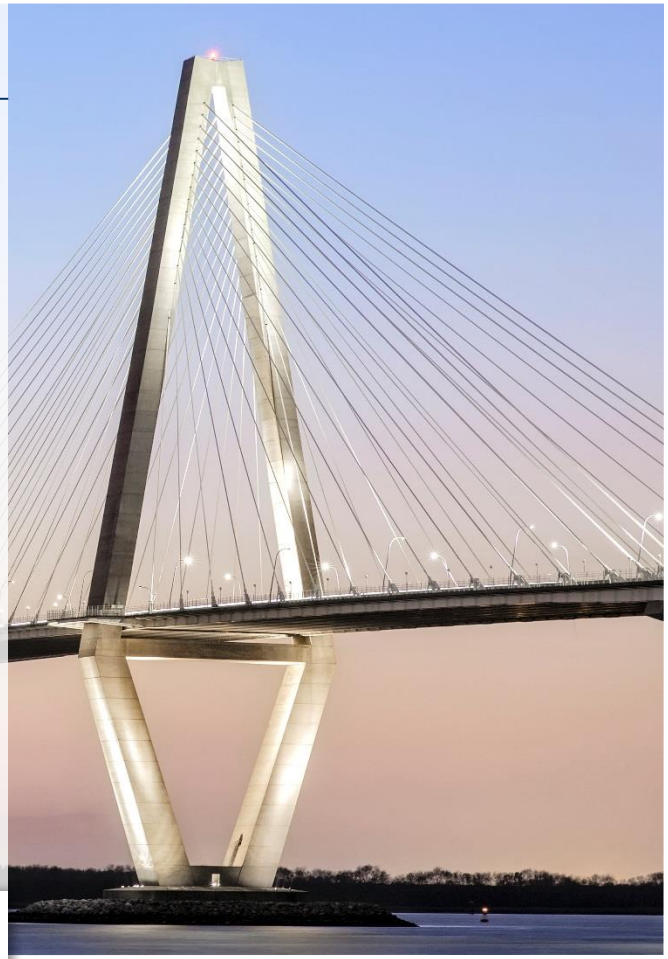

HISOLUTIONS

# Was sind Kritische Infrastrukturen?



HISOLUTIONS

1 Motivation
2 Was sind kritische Infrastrukturen
3 **Rechtliche Grundlagen für KRITIS-Betreiber**
4 Kritis - Sektoren und Fristen
5 Ermittlung des Geltungsbereichs
6 Meldung potenzieller Vorfälle
7 Stand der Technik
8 Prüfung gemäß § 8a BSIG
9 Weitere Zulassungsmöglichkeiten





HISOLUTIONS

# Rechtliche Grundlagen für KRITIS-Betreiber

| Grundlage | Inhalt |
|---|---|
| § 2 Absatz 10 BSIG | Festlegung der KRITIS-Sektoren & Definition Kritische Infrastrukturen |
| § 8a BSIG | IT-Sicherheit in Kritischen Infrastrukturen |
| § 8b BSIG | Melde- und Informationswesen |
| § 1 BSI-KritisV | Begriffsbestimmungen |
| §§ 2-5 BSI-KritisV | Definition der Sektoren aus Korb I |
| §§ 6-8 BSI-KritisV | Definition der Sektoren aus Korb II |
| Anhänge BSI-KritisV | Anlagenkategorien und Schwellenwerte |

# Kritische Infrastrukturen im Sinne des BSIG

## § 2 (10) BSIG

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

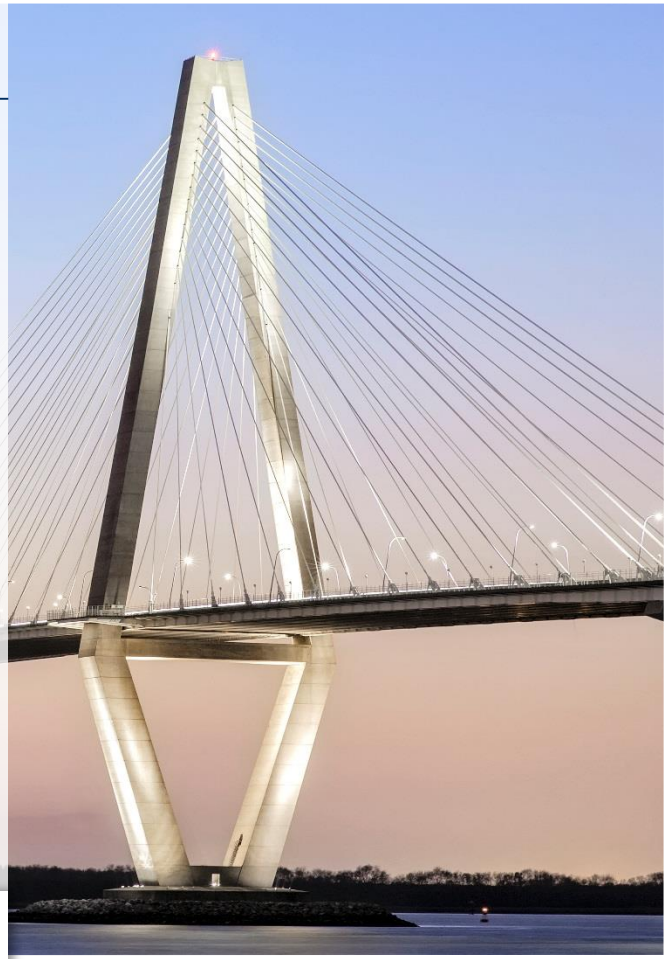
2. von **hoher Bedeutung für das Funktionieren des Gemeinwesens** sind, weil durch ihren Ausfall oder ihre Beeinträchtigung **erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit** eintreten würden.

Die Kritischen Infrastrukturen im Sinne dieses Gesetzes werden durch die Rechtsverordnung nach § 10 Abs. 1 BSIG (BSI-KritisV) näher bestimmt.



HISOLUTIONS

1 Motivation
2 Was sind kritische Infrastrukturen
3 Rechtliche Grundlagen für KRITIS-Betreiber
4 **Kritis - Sektoren und Fristen**
5 Ermittlung des Geltungsbereichs
6 Meldung potenzieller Vorfälle
7 Stand der Technik
8 Prüfung gemäß § 8a BSIG
9 Weitere Zulassungsmöglichkeiten





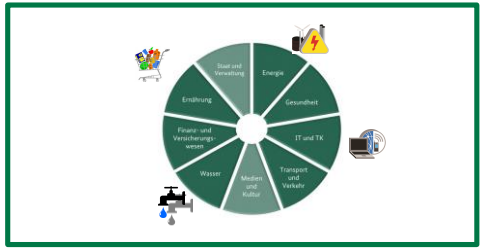
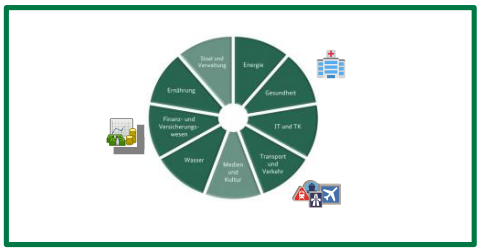
HISOLUTIONS

# KRITIS SEKTOREN

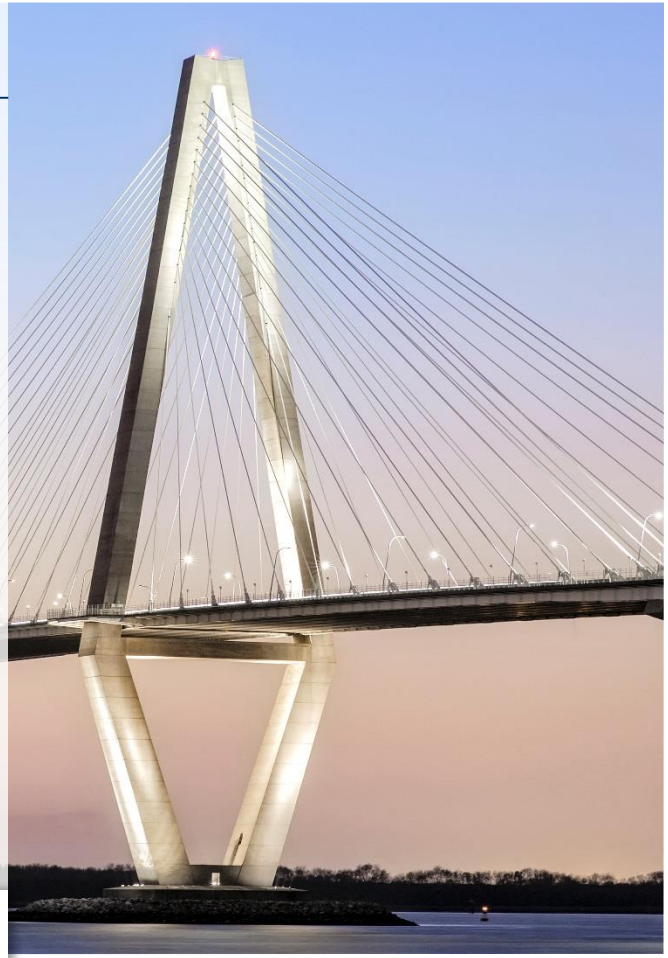



HISOLUTIONS

# KRITIS FRISTEN

| Maßnahmen | Fristen | |
|---|---|---|
| | Korb 1 | Korb 2 |
| |  |  |
| Umsetzung der Maßnahmen nach § 8a BSIG & Durchführung der Prüfung | ab sofort | |
| Lieferung der Nachweise an das BSI | Mai 2018 | Juni 2019 |
| Einrichtung einer Kontaktstelle nach § 8b BSIG | November 2016 | Dezember 2017 |

1 Motivation
2 Was sind kritische Infrastrukturen
3 Rechtliche Grundlagen für KRITIS-Betreiber
4 Kritis - Sektoren und Fristen
**5 Ermittlung des Geltungsbereichs**
6 Meldung potenzieller Vorfälle
7 Stand der Technik
8 Prüfung gemäß § 8a BSIG
9 Weitere Zulassungsmöglichkeiten





HISOLUTIONS

# Ermittlung des Geltungsbereichs

Regelung für Kleinstunternehmen: Mehr als 10 Mitarbeiter oder mehr als 2 Mio € Jahresumsatz? [§ 8c Absatz 1 BSIG]

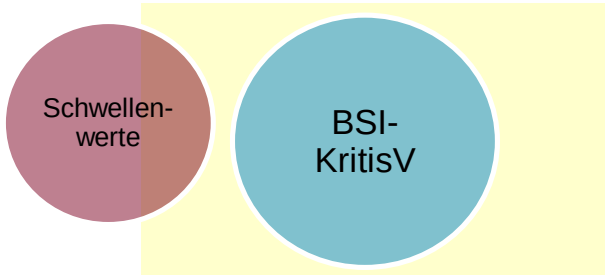
Werden Anlagen zur Erbringung einer kritischen Dienstleistung betrieben? [§ 2 Absatz 10 BSIG]

Werden kritische Dienstleistungen durch externe Dienstleister erbracht, auf deren Beschaffenheit und Betrieb ein bestimmender Einfluss vorliegt? [§ 1 BSI-KritisV]

Liegt der Versorgungsgrad dieser Anlagen über den definierten Schwellenwerten? [Anhänge BSI-KritisV]

# Begriffsbestimmung: Schwellenwert

Ein Wert, bei dessen Erreichen oder dessen Überschreitung der Versorgungsgrad einer Anlage oder Teilen davon als bedeutend im Sinne von § 10 Absatz 1 Satz 1 des BSI-Gesetzes anzusehen ist.





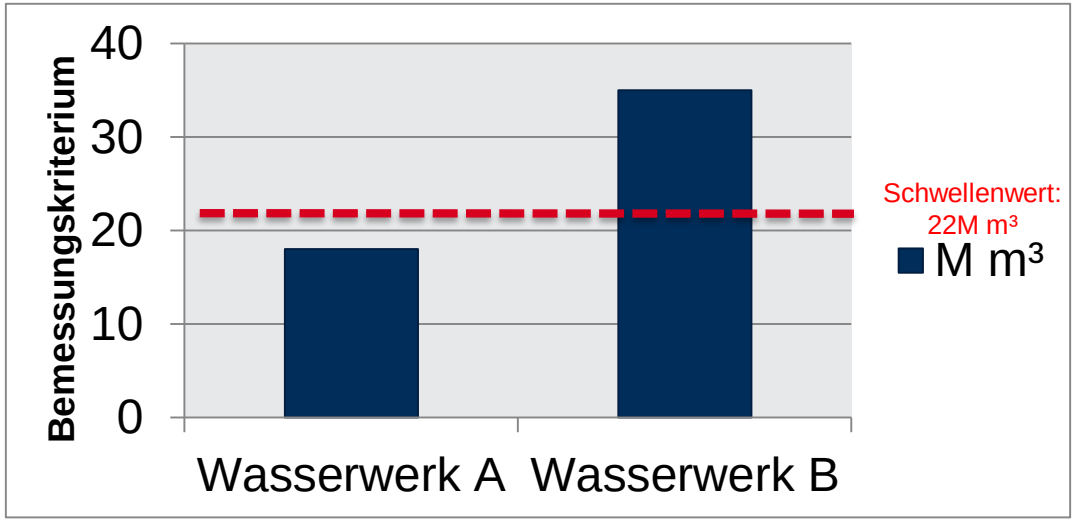

HISOLUTIONS

# Beispiel: Trinkwasserversorgung/-gewinnung (Sektor Wasser)

Wasserwerk A: ~~18M m³~~ **NICHT KRITISCH**

Wasserwerk B: 35M m³ **KRITISCH**

➡ Schwellenwert: **22M m³**





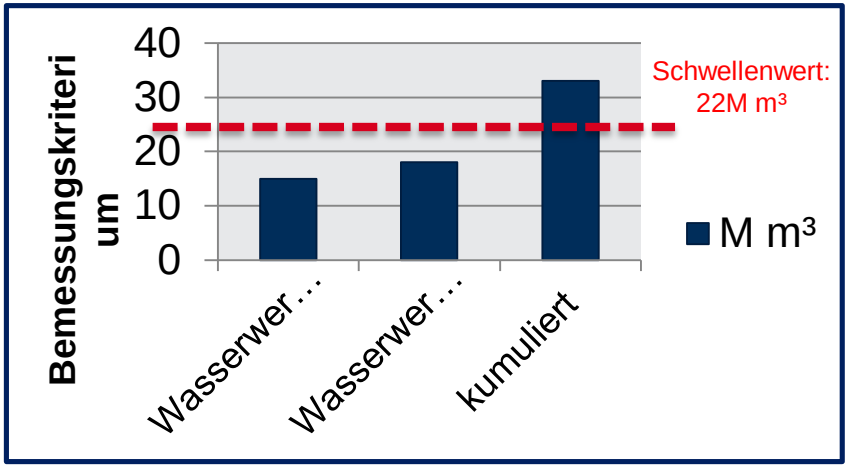

HISOLUTIONS

# Beispiel: Mehrere Anlagen gewertet als eine (Sektor Wasser)

| | | |
|---|---|---|
| Wasserwerk C: | ~~15M m³~~ | NICHT KRITISCH |
| Wasserwerk D: | ~~18M m³~~ | NICHT KRITISCH |
| Kumuliert: | 33M m³ | KRITISCH |

Mehrere Anlagen gelten als eine Anlage, wenn

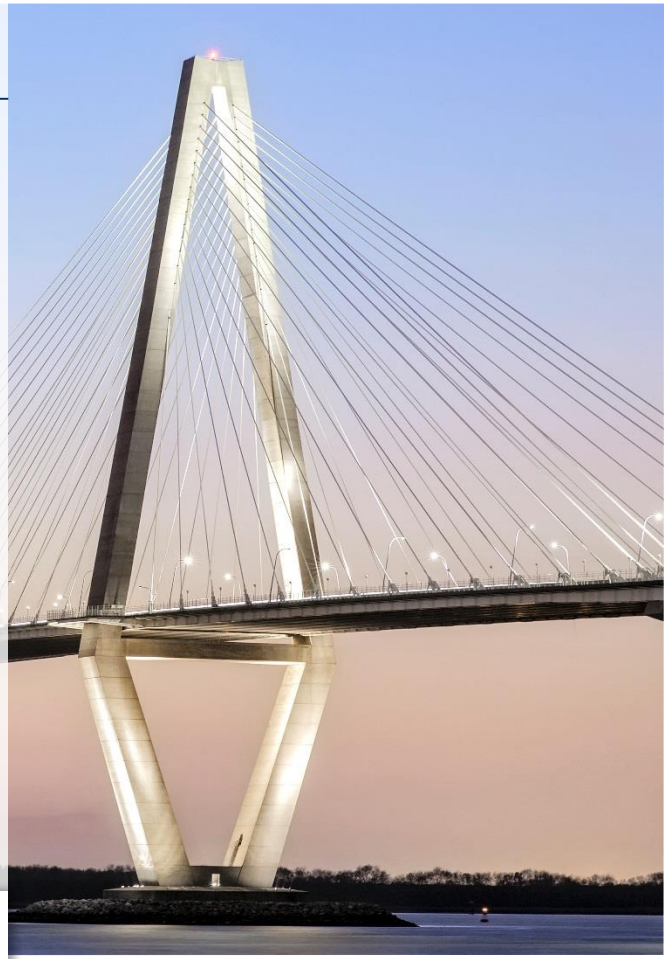
- sie auf demselben Betriebsgelände,
- mit gemeinsamen Betriebseinrichtungen (oder untereinander) verbunden sind,
- einem vergleichbaren technischen Zweck dienen und
- unter gemeinsamer Leitung stehen.






HISOLUTIONS

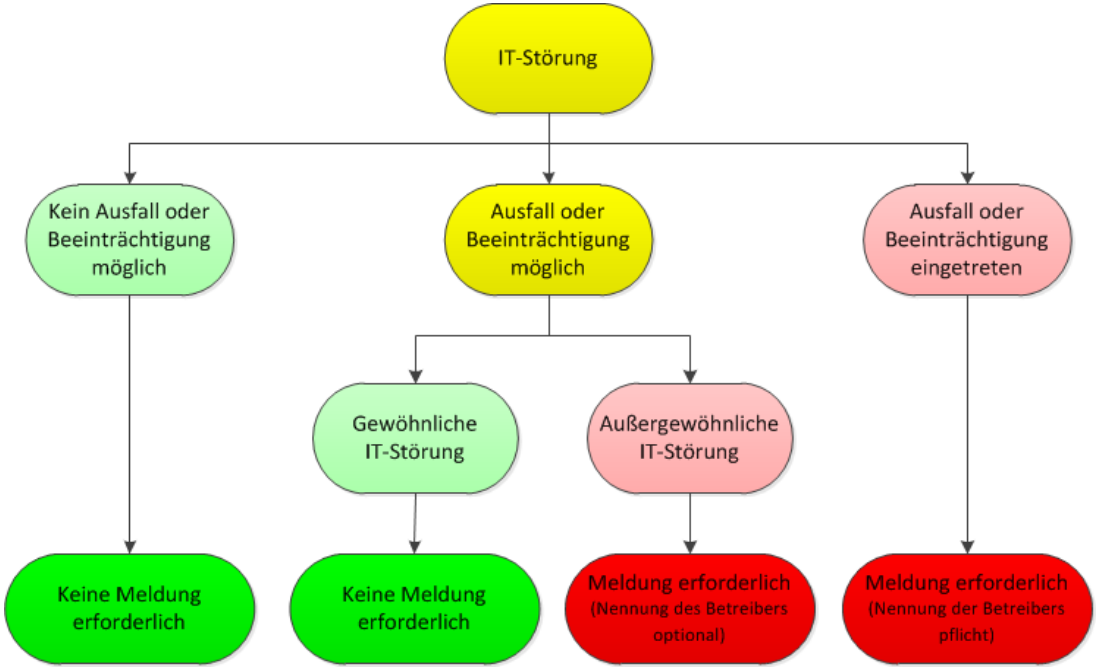
1 Motivation
2 Was sind kritische Infrastrukturen
3 Rechtliche Grundlagen für KRITIS-Betreiber
4 Kritis - Sektoren und Fristen
5 Ermittlung des Geltungsbereichs
6 Meldung potenzieller Vorfälle
7 Stand der Technik
8 Prüfung gemäß § 8a BSIG
9 Weitere Zulassungsmöglichkeiten





HISOLUTIONS

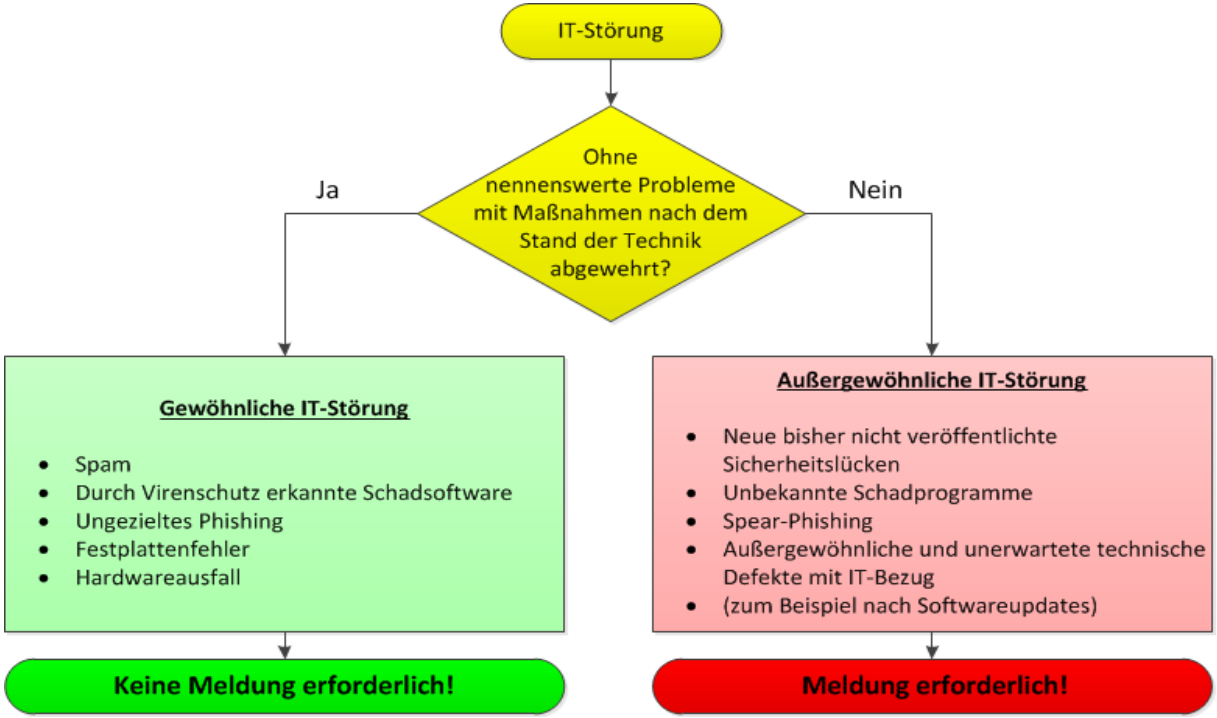
# MELDEKRITERIEN UND –SCHWELLEN






HISOLUTIONS

# Gewöhnliche vs. außergewöhnliche IT-Störungen






HISOLUTIONS

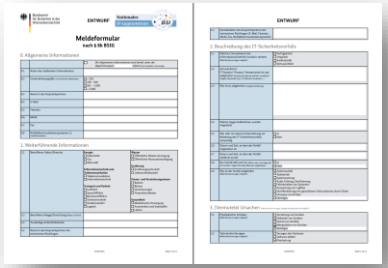
# Melde- und Informationsvorgaben gemäß § 8b BSIG

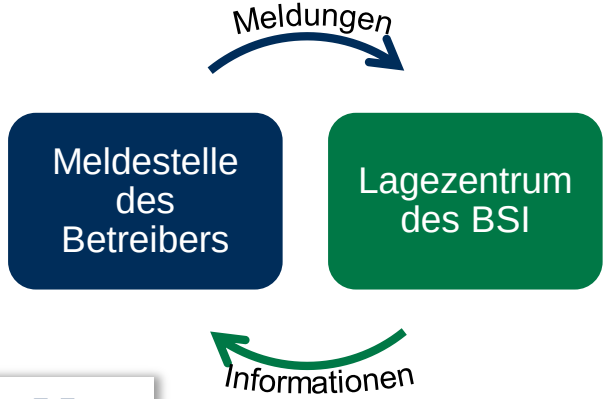
Einrichtung einer **24/7 Kontaktstelle** zur Kommunikation mit dem BSI

- Erfüllen der **Meldepflicht**
  ➔ Melden von **erheblichen IT-Sicherheitsvorfällen** an das BSI

- Erfüllen der **Informationspflicht**
  ➔ **Einrichten** eines **Prozesses** zur geeigneten **Entgegennahme** und **Reaktion** auf die vom BSI **erhaltenen** Lageprodukte und **Warnungen**

**Meldeformular**

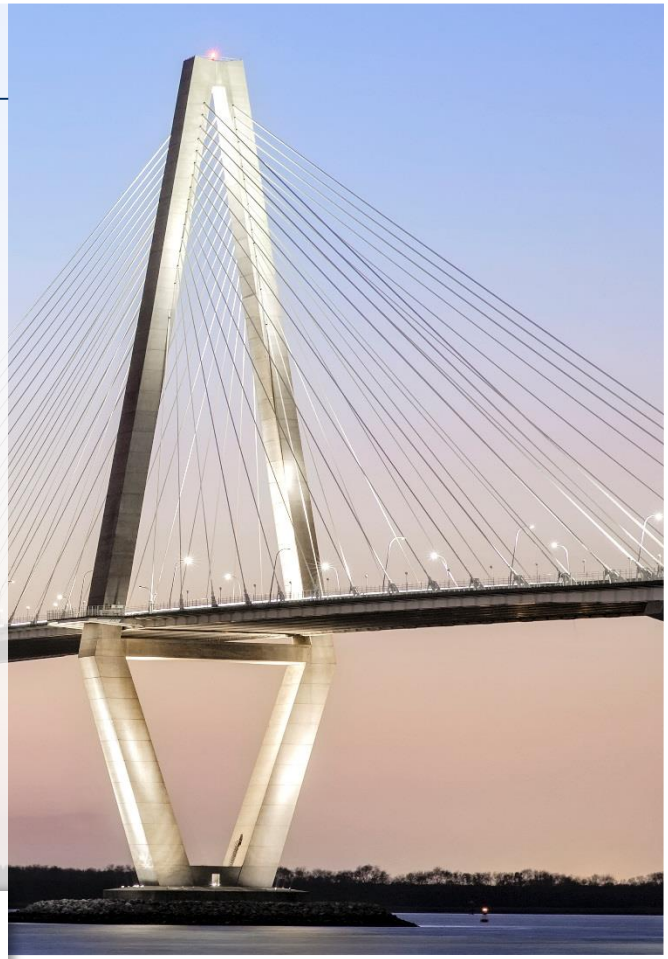







HISOLUTIONS

1 Motivation
2 Was sind kritische Infrastrukturen
3 Rechtliche Grundlagen für KRITIS-Betreiber
4 Kritis - Sektoren und Fristen
5 Ermittlung des Geltungsbereichs
6 Meldung potenzieller Vorfälle
7 **Stand der Technik**
8 Prüfung gemäß § 8a BSIG
9 Weitere Zulassungsmöglichkeiten





HISOLUTIONS

# Gesetzesbegründung des IT-Sicherheitsgesetzes zum „Stand der Technik“

„Auf Grund der weitreichenden gesellschaftlichen Auswirkungen ist bei den technischen und organisatorischen Vorkehrungen der „Stand der Technik“ zu berücksichtigen [BSIG: „einzuhalten“].

- „Stand der Technik“ in diesem Sinne ist der **Entwicklungsstand** fortschrittlicher
  - Verfahren, Einrichtungen oder Betriebsweisen,
- der die **praktische Eignung einer Maßnahme zum Schutz der Funktionsfähigkeit** von informationstechnischen
  - Systemen, Komponenten oder Prozessen
- gegen **Beeinträchtigungen** der
  - Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit gesichert erscheinen lässt.“



HISOLUTIONS

# Gesetzesbegründung des IT-Sicherheitsgesetzes zum „Stand der Technik“

„Bei der Bestimmung des „Standes der Technik“ sind insbesondere einschlägige

- internationale, europäische und nationale Normen und Standards heranzuziehen,

aber auch vergleichbare

- Verfahren, Einrichtungen und Betriebsweisen,

die mit **Erfolg in der Praxis erprobt** wurden.

Die Verpflichtung zur Berücksichtigung des „Standes der Technik“ schließt die Möglichkeit zum Einsatz solcher Vorkehrungen nicht aus, die einen **ebenso effektiven Schutz** wie die anerkannten Vorkehrungen nach dem „Stand der Technik“ bieten.“

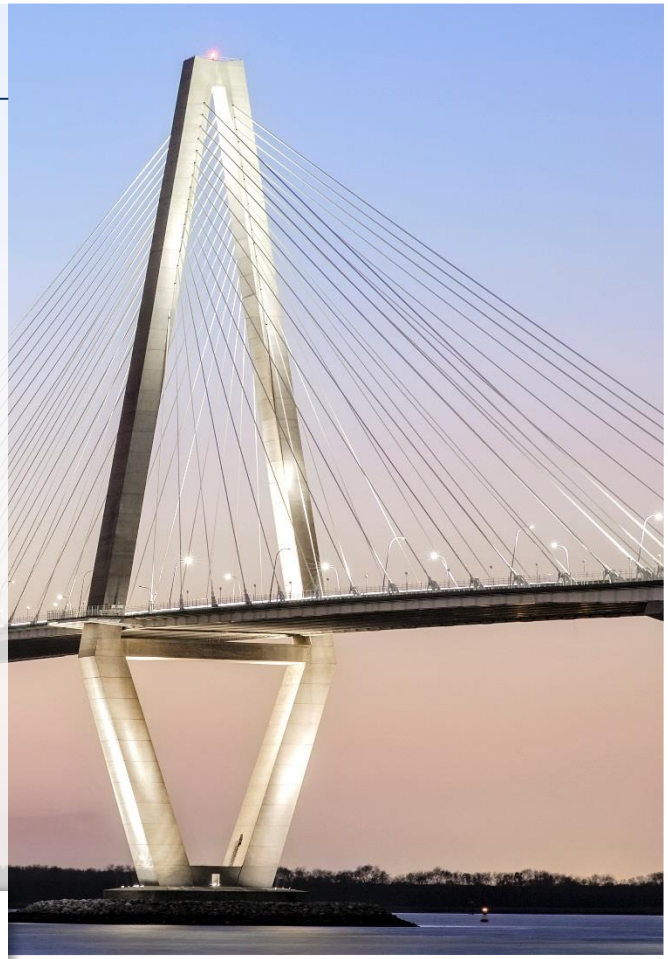
# Branchenspezifische Sicherheitsstandards (B3S)

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



HISOLUTIONS

1 Motivation
2 Was sind kritische Infrastrukturen
3 Rechtliche Grundlagen für KRITIS-Betreiber
4 Kritis - Sektoren und Fristen
5 Ermittlung des Geltungsbereichs
6 Meldung potenzieller Vorfälle
7 Stand der Technik
**8 Prüfung gemäß § 8a BSIG**
9 Weitere Zulassungsmöglichkeiten





HISOLUTIONS

# Prüfung gemäß § 8a BSIG

Der **Fokus der Prüfung** gemäß § 8a BS … der IT-Systeme von **kritischen Dien…**

**Risikoakzeptanz** oder **Risikoübernahme** für **Verfügbarkeit nicht** ausreichend!

**Entwicklung** einer **Prüfgrundlage**, welche die **branchenspezifischen Beson…** berücksichtigt

Prüfung der **Umsetzung angemessener** organisatorischer und technischer **Vorkehrungen** zur **Vermeidung** von IT-Störungen durch Maßnahmen nach **Stand der Technik** auf Basis der **Prüfgrundlage**

Nach erfolgter Prüfung: Auslieferung der **Nachweise** zur Umsetzung & Liste der aufgedeckten Sicherheitsmängel an das BSI

Prüfung **zwei Jahre** nach **Inkrafttreten** der **BSI-KritisV** und ab dann **alle zwei Jahre**



HISOLUTIONS

# BESONDERHEITEN

**Schutzbedarf:**

- Der Fokus liegt auf der **Verfügbarkeit der kritischen Dienstleistung** bzw. der Vermeidung von Versorgungsengpässen, **nicht auf wirtschaftlichen Aspekten**.

**All-Gefahren-Ansatz:**

- Behandlung aller relevanten Bedrohungen und Schwachstellen der maßgeblichen Informationstechnik d. h. Systeme, Komponenten oder Prozesse zur Erbringung der kDL.

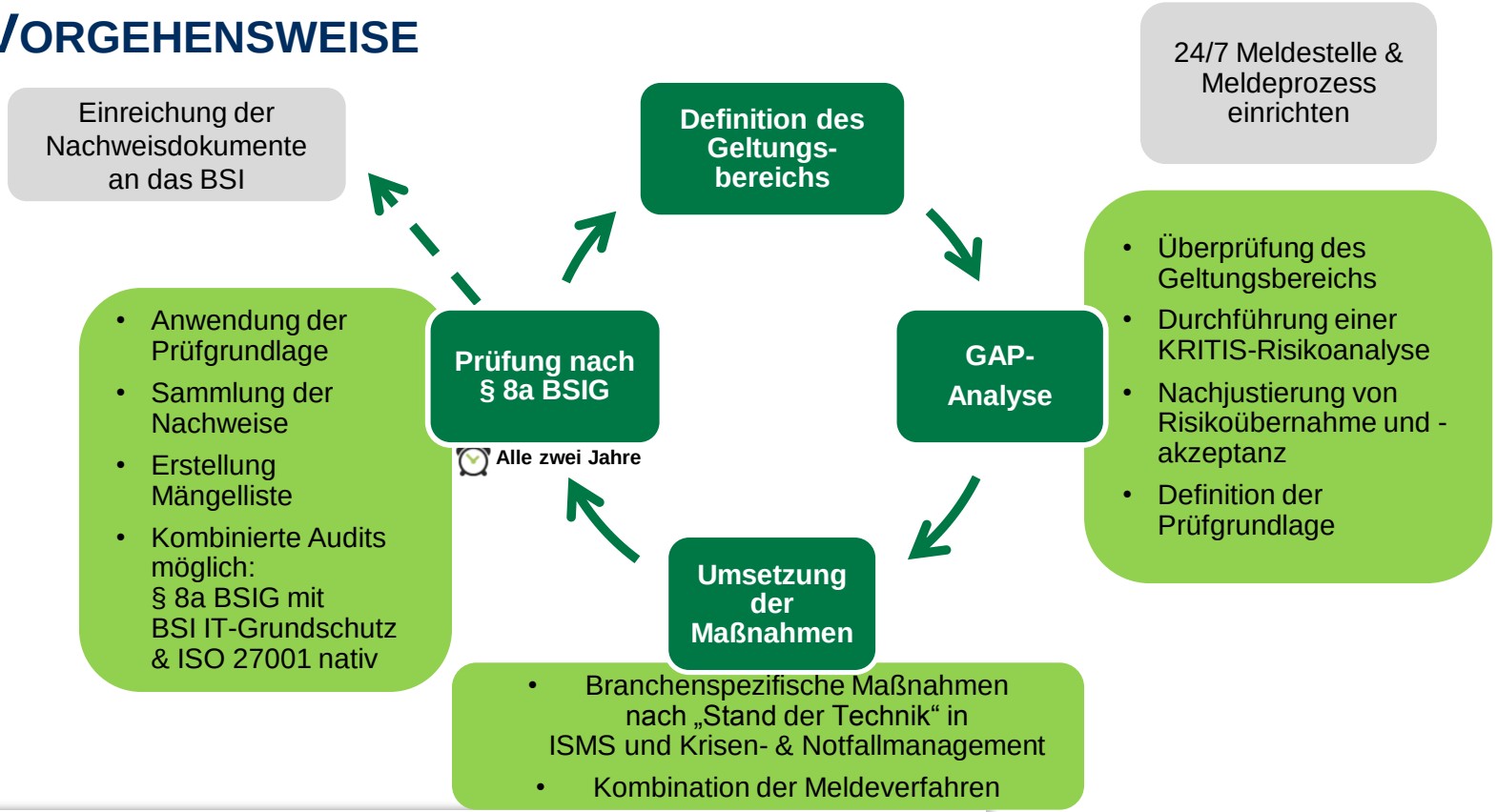
**Risikoakzeptanz:**

- nur eingeschränkte Akzeptanz / Verlagerung von Risiken:
- Risikoakzeptanz muss mögliche Versorgungsausfälle betrachten (nicht allein betriebswirtschaftliches Risiko!)
- Versicherungen sind zur Vermeidung von Versorgungsengpässen nicht ausreichend



HISOLUTIONS

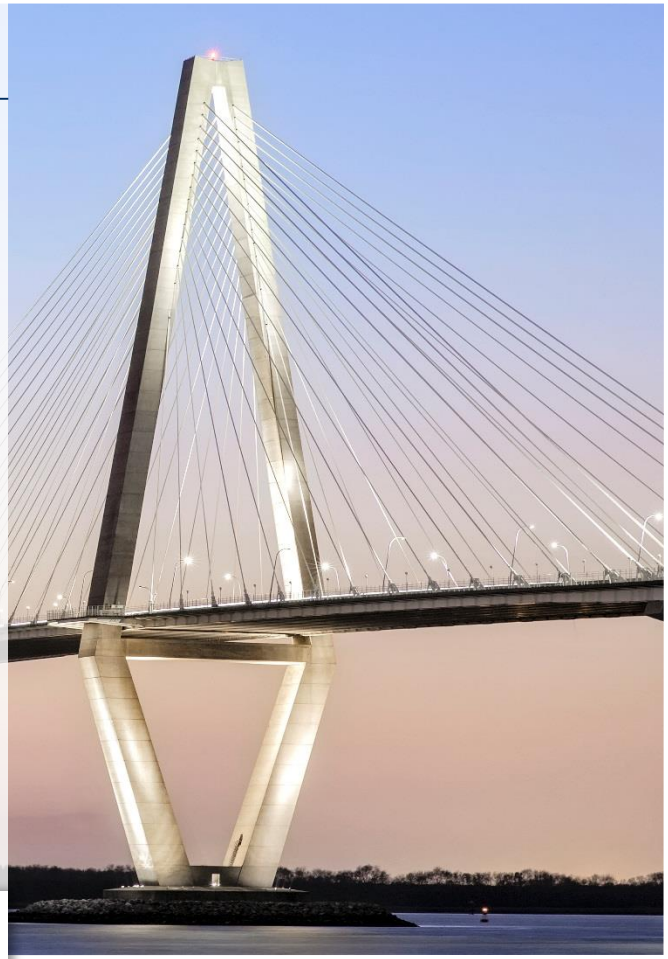
# VORGEHENSWEISE






HISOLUTIONS

1 Motivation
2 Was sind kritische Infrastrukturen
3 Rechtliche Grundlagen für KRITIS-Betreiber
4 Kritis - Sektoren und Fristen
5 Ermittlung des Geltungsbereichs
6 Meldung potenzieller Vorfälle
7 Stand der Technik
8 Prüfung gemäß § 8a BSIG
**9 Weitere Zulassungsmöglichkeiten**





HISOLUTIONS

# Alternative Zulassungsmöglichkeiten

**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**

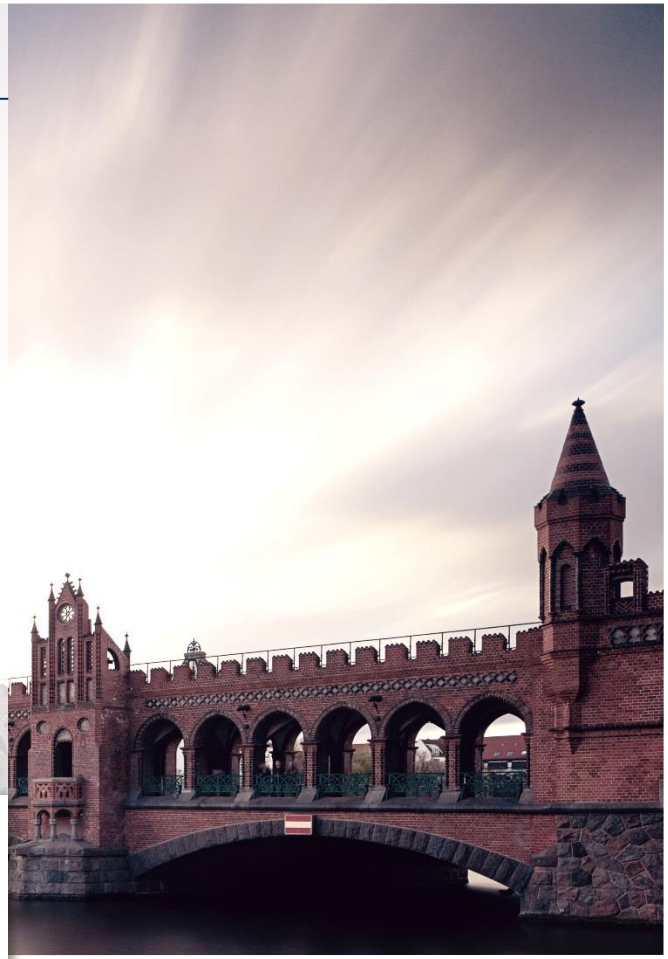
Eine Anlehnung an einen B3S ist ebenfalls hilfreich, da er branchentypische Sicherheitsaspekte zur Umsetzung von § 8a (1) BSIG zusammenfasst.

# Was Sie aus dieser Präsentation mitnehmen sollten:

**KRITIS ist ein sinnvoller Ansatz um die IT-Sicherheit in Unternehmen zu stärken**

**Er bietet gute Integrationsmöglichkeiten in andere Standards und Normen**

**KRITIS dient primär dem Schutz der Bevölkerung, nicht der Unternehmen**

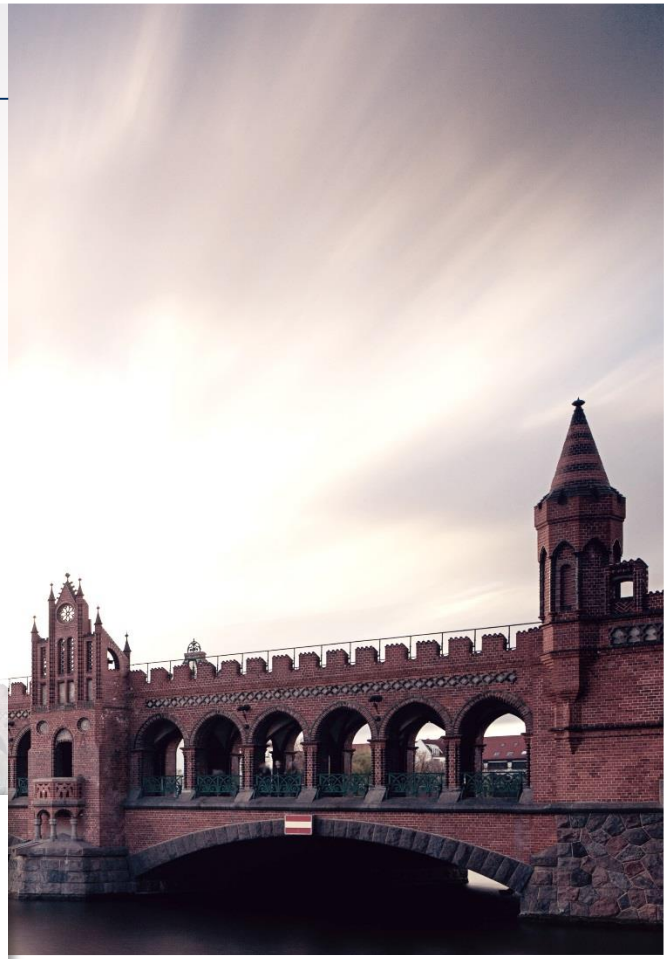


HISOLUTIONS

# HISOLUTIONS BEDANKT SICH FÜR IHRE AUFMERKSAMKEIT

**HiSolutions AG**

Bouchéstraße 12
12435 Berlin
info@hisolutions.de
www.hisolutions.de
+49 30 533 289 0



HISOLUTIONS