Internet Security Days 2018

Angriffe gegen kritische Infrastrukturen

Was haben wir aus KRITIS gelernt?

Daniel Jedecke, Managing Consultant

HISOLUTIONS

Über mich

Daniel Jedecke

- Managing Consultant der HiSolutions AG
- seit 2001 in der Informationssicherheit tätig
- langjährige Erfahrung im Bereich technische IT-Sicherheit und Auditierungen
- berät und begleitet Unternehmen bei der Einführung von ISMS
- Spezialthemen: KRITIS, Netzwerksicherheit und Containersicherheit
- Diplom-Wirtschaftsinformatik, TH Köln
- Master of Science in Applied IT Security, Ruhr-Universität Bochum
- Certified Lead Auditor ISO 27001(inklusive Auditkompetenz für EnWG und zusätzliche Prüfverfahrens-Kompetenz für § 8a BSIG)
- Certified Information Systems Auditor & zertifizierter DSB

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.

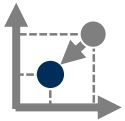
Wirtschafts-
grundschutz

Corporate
Security

Sicherheits-
strategie

Industrial
Security

Kritische
Infrastrukturen

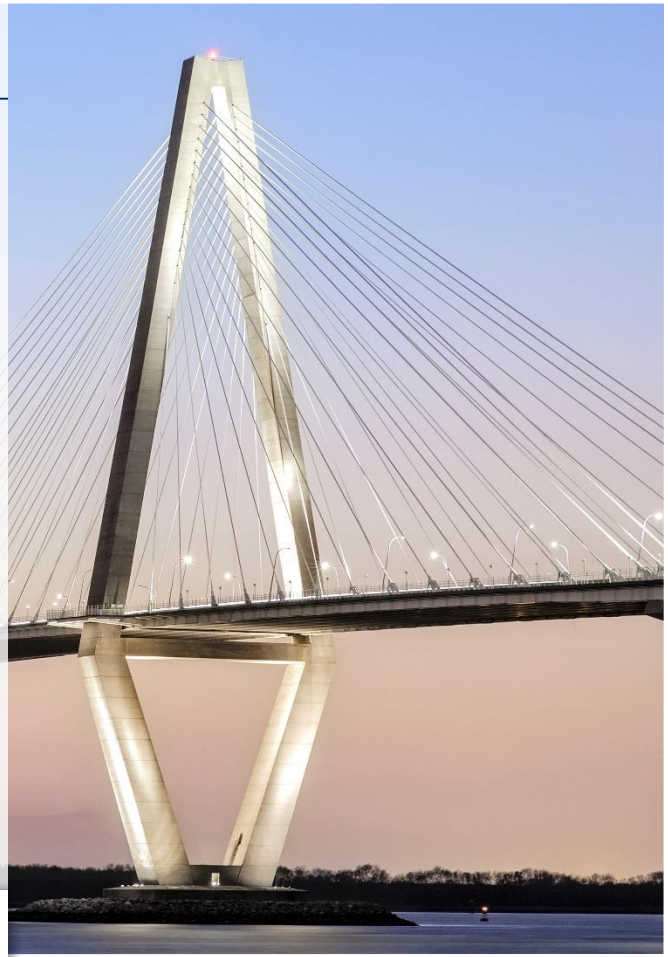


Risk Management

HISOLUTIONS

AGENDA

1 **Erfolgte Angriffe**
2 Regularien
3 Umsetzung von KRITIS
4 Schlussfolgerung



HISOLUTIONS

Attacken auf das Ukrainische Stromnetz

- Dezember 2015
- Wiederholte Attacke im Dezember 2016

- Auswirkungen: ca. 250.000 betroffene Personen in Kiew und dem Umfeld
- Zielgerichtete Angriffe auf die Stromversorgung
- Firmware der Stromunterbrecher wurde gezielt manipuliert

Picture: Wikipedia, CC

HISOLUTIONS

Cyber-Angriffe auf deutsche Energieversorger

- Deutsche Unternehmen aus der Energiebranche waren und sind 2017 und 2018 das Ziel von großangelegten weltweiten Cyber-Angriffskampagnen.

- Laut BSI liegen derzeit keine Hinweise auf erfolgreiche Zugriffe auf Produktions- oder Steuerungsnetzwerke vor. Es sei nur eine Frage der Zeit, bis neue, erfolgreiche Angriffe ausgeübt würden. Daher müsse man das IT-Sicherheitsgesetz fortschreiben.

HISOLUTIONS

Hacken der Bundesregierung

- Das Datennetzwerk der Bundesregierung wurde von unbekannten Angreifern attackiert.
- Die Bundesregierung sagt hierzu:
  „…es wurden bereits geeignete Maßnahmen zur Aufklärung und zum Schutz getroffen…An dem Vorfall wird mit hoher Priorität und erheblichen Ressourcen gearbeitet…“
- Es wurden Daten exfiltriert und eine Schadsoftware wurde eingeschleust.
- Die Attacke wurde erst im Dezember 2017 erkannt, obwohl der Angriff bereits seit einem Jahr lief.

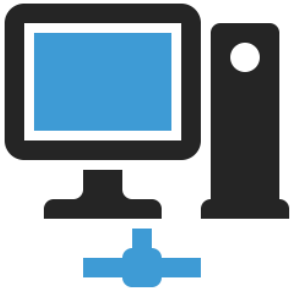
Weitere Angriffe und Ausfälle in 2018

Angriffe:

- US-Krankenhaus von Ransomware teilweise lahmgelegt

Ausfälle:

- Schwere Computerpanne am Frankfurter Flughafen
- USV Ausfall bei einem deutschen Hoster
- Computerausfall der europäischen Flugsicherung Eurocontrol
- Belgischer Luftraum durch technische Probleme gesperrt
- Kfz-Zulassung in ganz Deutschland ausgefallen
- Flugbetrieb in Hamburg nach Stromausfall eingestellt



HISOLUTIONS

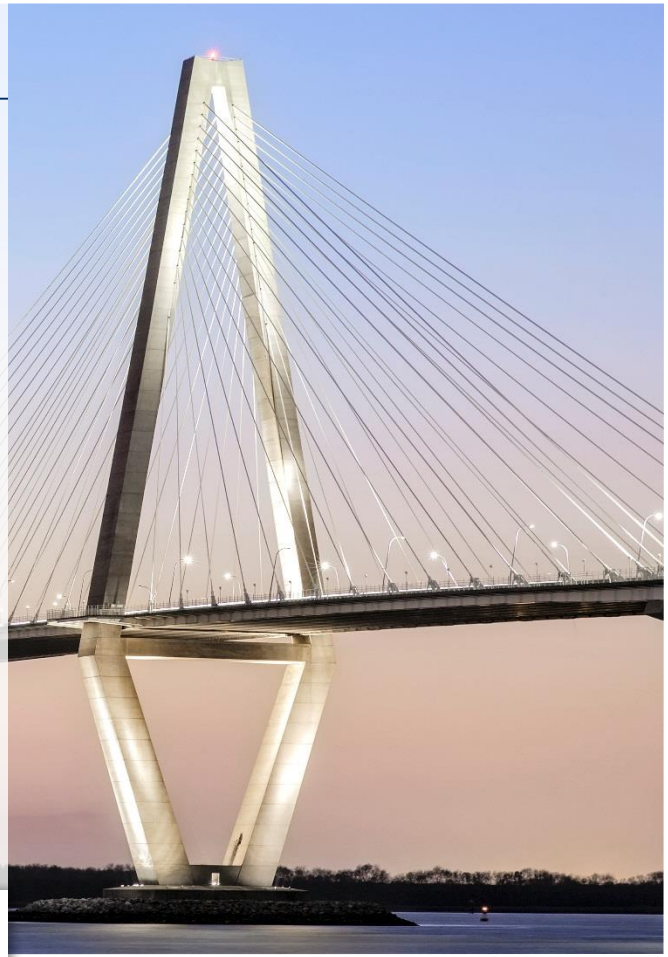
AGENDA

1 Erfolgte Angriffe

2 Regularien

3 Umsetzung von KRITIS

4 Schlussfolgerung



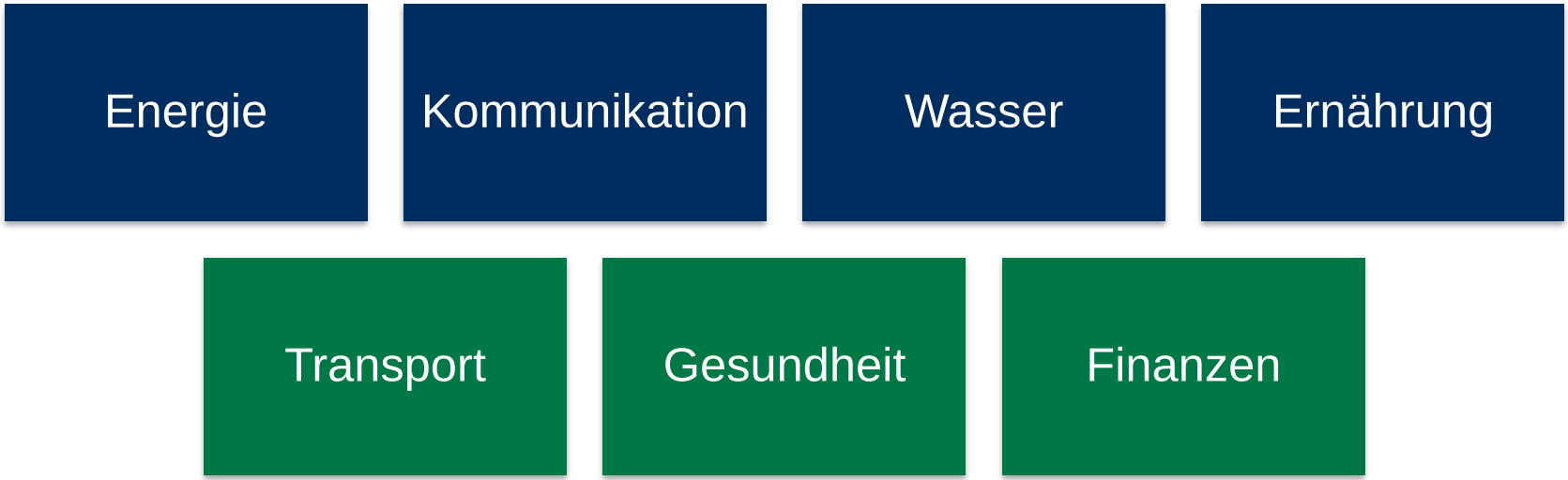
HISOLUTIONS

Regularien in Deutschland

- Regulierung für kritische Infrastrukturen begann 2015
- Ziel: Sicherheit der IT-Komponenten von kritischen Infrastrukturen
- Rechtlich verbindlich ab einer Versorgung von mindestens 500.000 Bürgern
- Betreiber in sieben Sektoren müssen ihre IT-Sicherheit nachweisen

HISOLUTIONS

KRITIS Sektoren



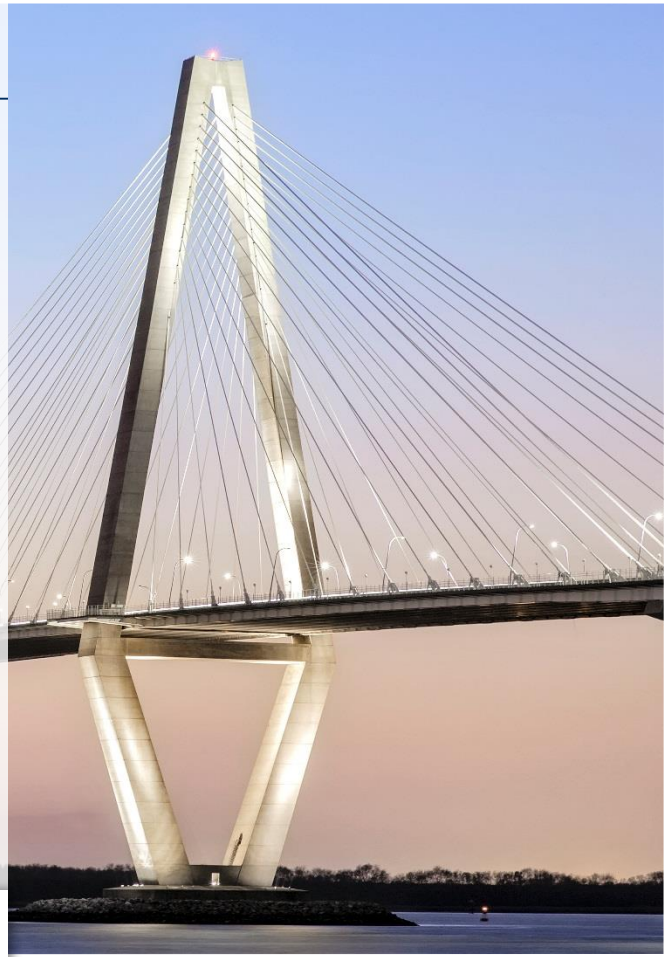
Korb 1: Deadline Mai 2018 (Energie im Januar 2018)

Korb 2: Deadline Juni 2019

HISOLUTIONS

AGENDA

1 Erfolgte Angriffe
2 Regularien
3 Umsetzung von KRITIS
4 Schlussfolgerung



HISOLUTIONS

KRITIS – Unterschiede zu anderen Sicherheitsstandards

- KRITIS dient primär dem **Schutz der Bevölkerung**, nicht des Betreibers.
- Ergebnis der KRITIS Prüfung ist **kein Zertifikat**, sondern eine Mängelliste mit Sicherheitsmängeln, die zu beheben sind.
- KRITIS prüft die **Umsetzung** von Sicherheitsanforderungen, nicht deren Planung.

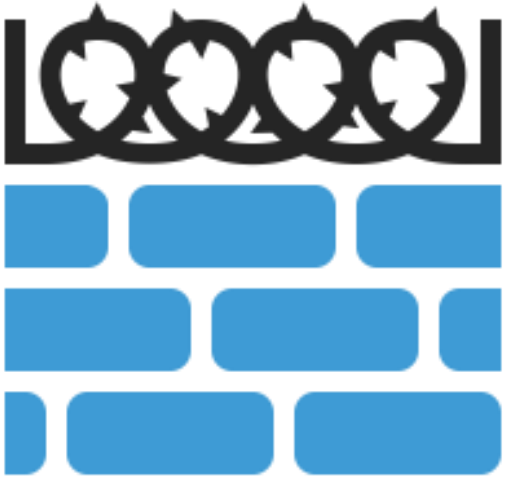
KRITIS – Unterschiede zu anderen Sicherheitsstandards

- KRITIS setzt **kein** zertifiziertes ISMS voraus! Es **muss** ein geeignetes ISMS Managementsystem verwendet werden, welches auch ein gemeinsames Management System sein kann.

- Es kann je nach Anlagentyp spezielle Anforderungen geben, welche die oben genannte Aussage aufhebt. So können einzelne Aufsichtsbehörden weitere Anforderungen, wie ein zertifiziertes ISMS nach ISO 27001, aufstellen.

„Stand der Technik“

- „Stand der Technik“ ist nicht juristisch definiert:
  - Sollte mehr als „nur übliche“ Maßnahmen sein
  - Aber weniger als die aktuellen wissenschaftlichen Standards
  - Als gute Basis dienen bewährte Industriestandards. Die Umsetzung muss auf Grundlage des zu minimierenden Risikos bewertet werden.



Ist alles sicher nach der Umsetzung (1/3)?

- Einige Unternehmen aus Korb 1 haben erst ab 2018 mit der Umsetzung begonnen und wurden bis zum Ende der Frist nicht fertig.

- Es zeigten sich oft Mängel in industriellen Steuerungssystemen oder Automatisierungssystemen.
  - Diese Mängel können meist erst nach umfangreichen Umbaumaßnahmen behoben werden.

HISOLUTIONS

Ist alles sicher nach der Umsetzung (2/3)?

- Teilweise haben wir schnell eingeführte ISMS Systeme erlebt, welche nur auf dem Papier existierten und keinen Mehrwert für das Unternehmen hatten.
  - IT-Sicherheit erfordert ein Umdenken bei den beteiligten Personen. Dies kann aber nicht von heute auf morgen passieren.

HISOLUTIONS

Ist alles sicher nach der Umsetzung (3/3)?

- Systeme müssen durch Regularien immer mehr vernetzt werden.
- Die Anforderungen an die Sicherheit werden nur langsam nachgezogen.

- **Beispiel Stromversorgung**:
  - Neue Automationssysteme haben oft WLAN und Bluetooth Unterstützung, welche unzureichend abgesichert ist.

HISOLUTIONS

Und was erwartet uns bei Korb 2?

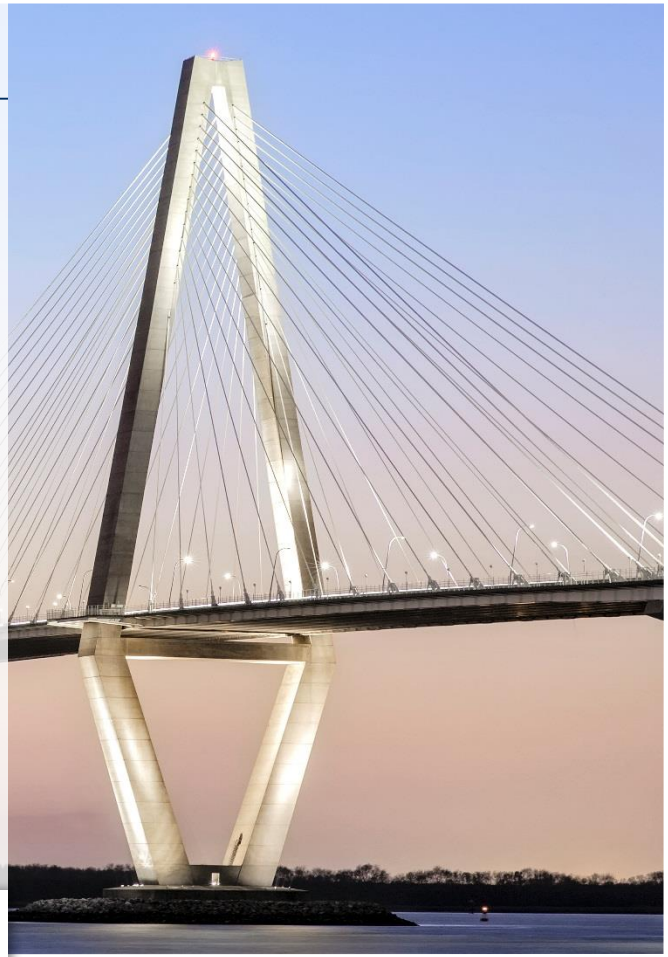
- Auch bei Korb 2 starten einige Unternehmen erst in 2019. Das Budget wurde in 2018 nicht eingeplant.
  - **Beispiel Hessen**:
    Den Krankenhäusern fehlen Gelder für die Umsetzung der Anforderungen. Eine kleine Anfrage an die Regierung hat gezeigt, dass nur ein Bruchteil für IT-Sicherheit geplant wurde.

- Die uns bekannten Projekte in den Sektoren Finanzen und Gesundheit starten langsam.

HISOLUTIONS

AGENDA

1 Erfolgte Angriffe
2 Regularien
3 Umsetzung von KRITIS
4 Schlussfolgerung



HISOLUTIONS

Schlussfolgerung (1/2)

- KRITIS eröffnet eine gute Ausgangsposition, um IT-Sicherheit zu verbessern.

- Es ist kein „Folge der Checkliste“ – Prinzip.
  - Eigenverantwortung der Betreiber ist gefordert.

Schlussfolgerung (2/2)

- KRITIS deckt nur den IT-gestützten Teil der kritischen Infrastrukturen ab!

- Beispiel: Wenn die Industrie in Folge von Umwelteinflüssen nicht mehr arbeiten kann, dann fällt dies nicht unter KRITIS!
  - Temperaturobergrenzen von 28 Grad für Kühlwasser wurden 2018 vielerorts überschritten. Kraftwerke mussten drosseln oder abgeschaltet werden.

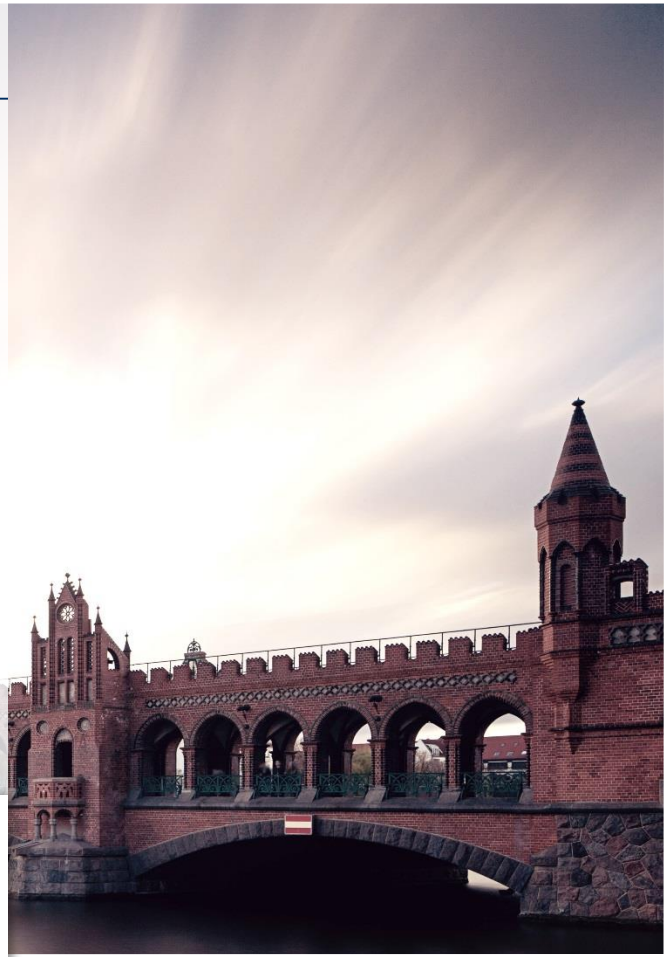
HISOLUTIONS

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.

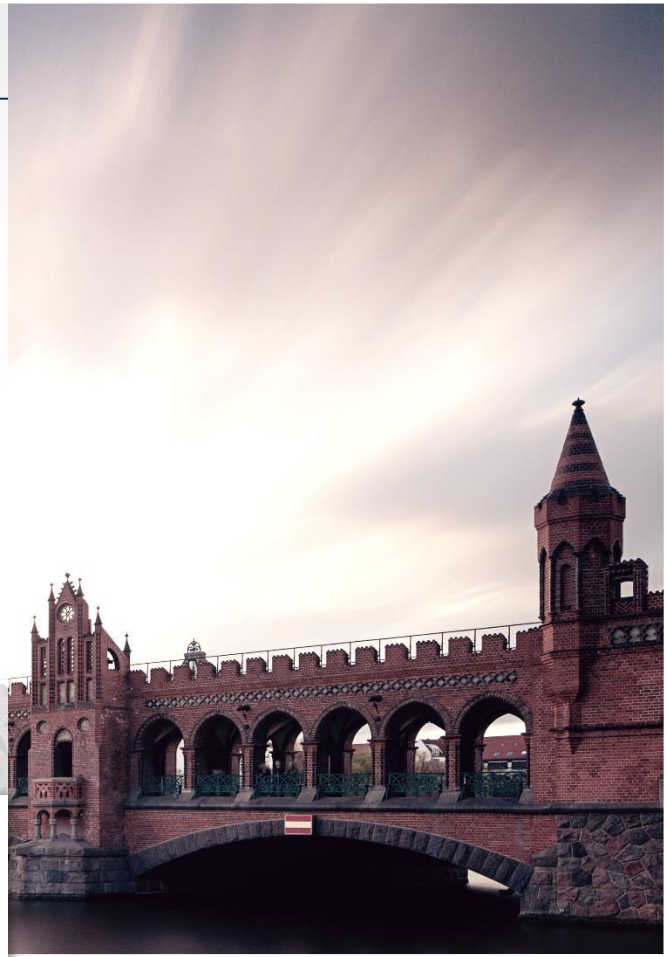


HISOLUTIONS

HISOLUTIONS BEDANKT SICH FÜR IHRE AUFMERKSAMKEIT

HiSolutions AG

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



HISOLUTIONS